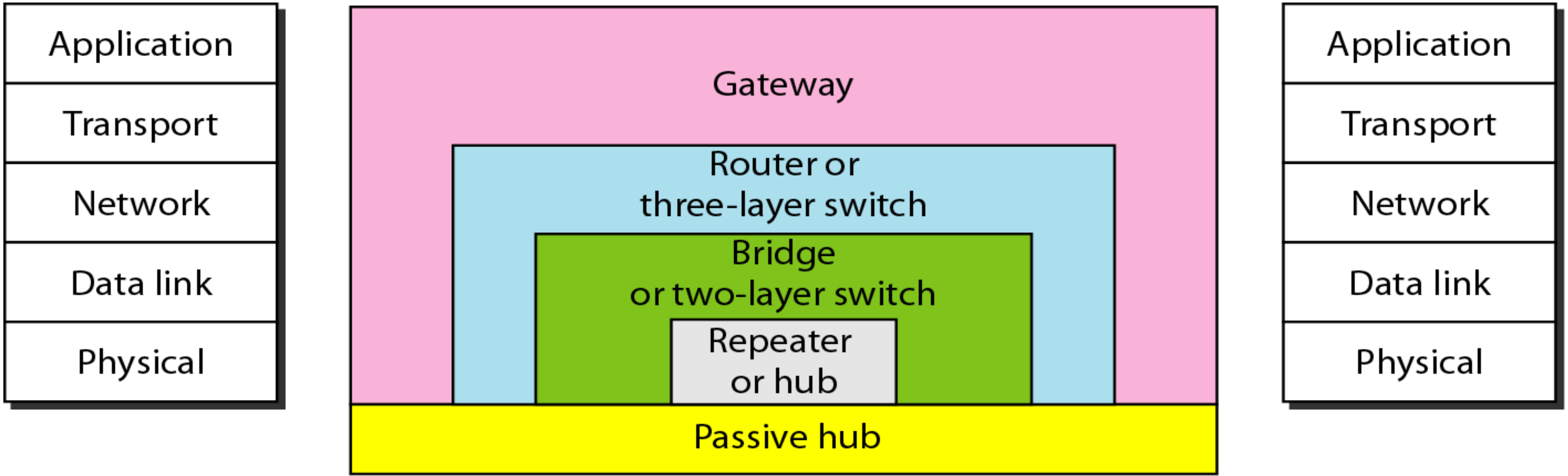
CHAPTER 5

LAN and WAN Technologies

LAN Devices: Repeater, Hub, Bridge and Switch

- LANs do not normally operate in isolation.
- They are connected to one another or to the Internet.
- To connect LANs, or segments of LANs, we use connecting devices.
- Connecting devices can operate in different layers of the Internet model.



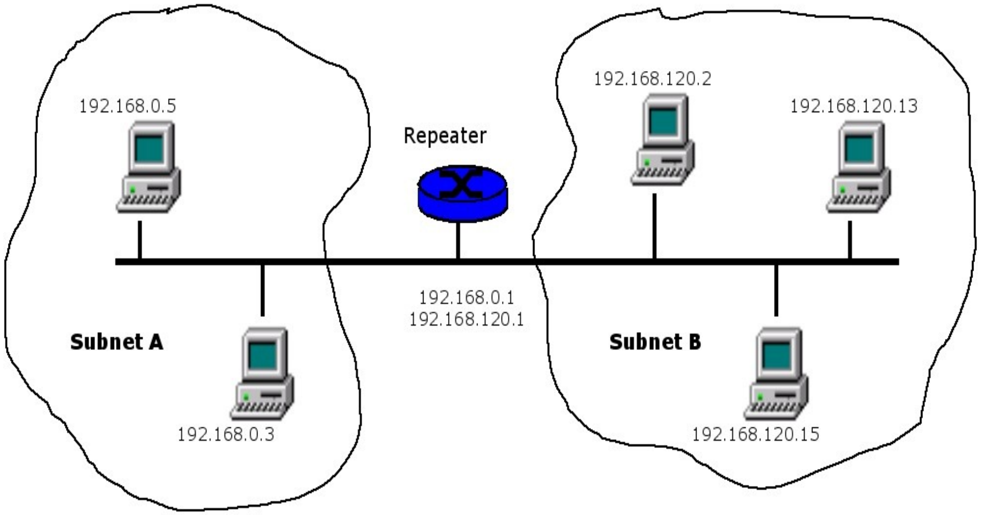
1. Repeater

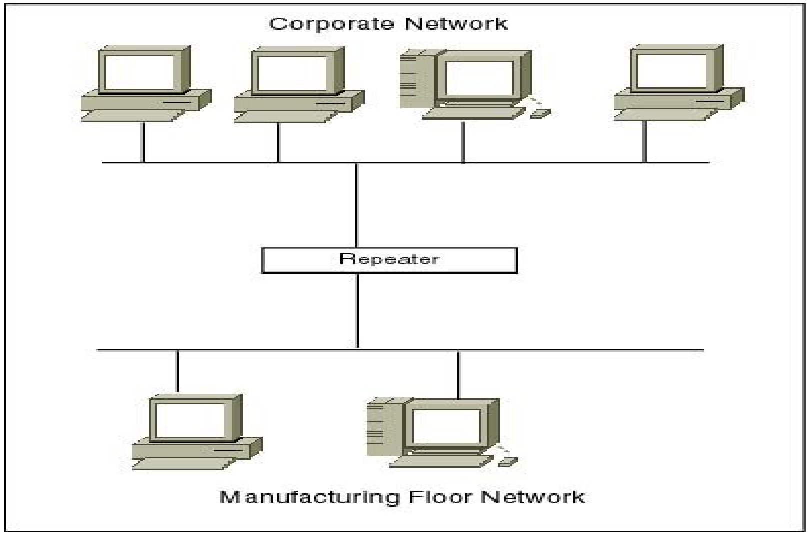
- A repeater receives a signal, regenerates it, and passes it on.
- It can regenerate signals at the bit level to allow them to travel a longer distance on the media.
- It operates at Physical Layer of OSI
- The Four Repeater Rule for 10-Mbps Ethernet should be used as a standard when extending LAN segments.
- This rule states that no more than four repeaters can be used between hosts on a LAN.

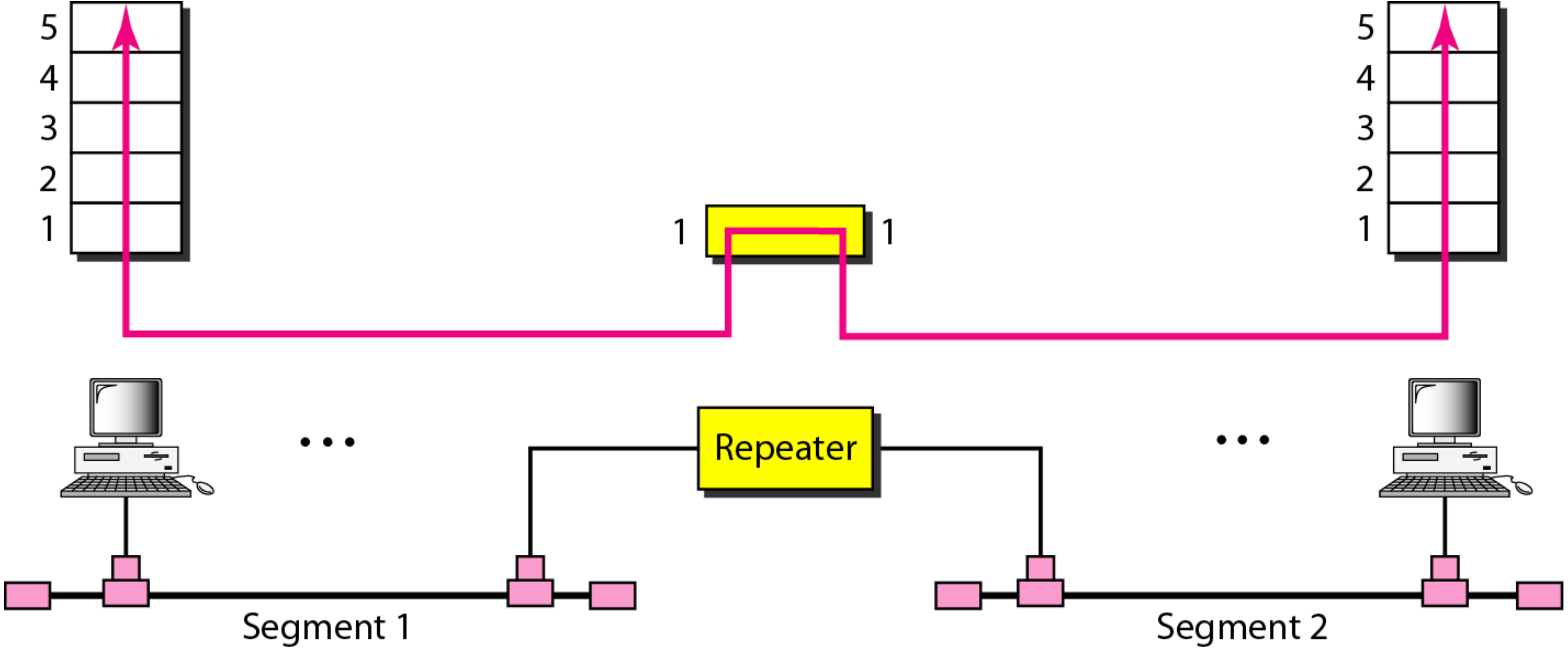
1. Repeater-----

- This rule is used to limit latency added to frame travel by each repeater.
- A repeater does not actually connect two LANs; it connects two segments of the same LAN.
- The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.
- A repeater is used to lengthen Ethernet network distance limitation by creating network segments
- A repeater forwards every frame; it has no filtering capability.

Repeater in action

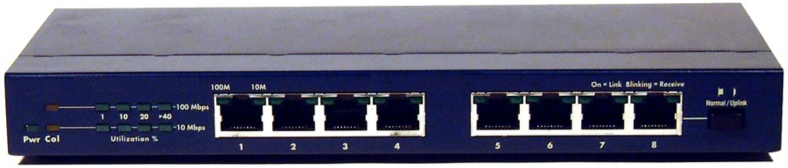


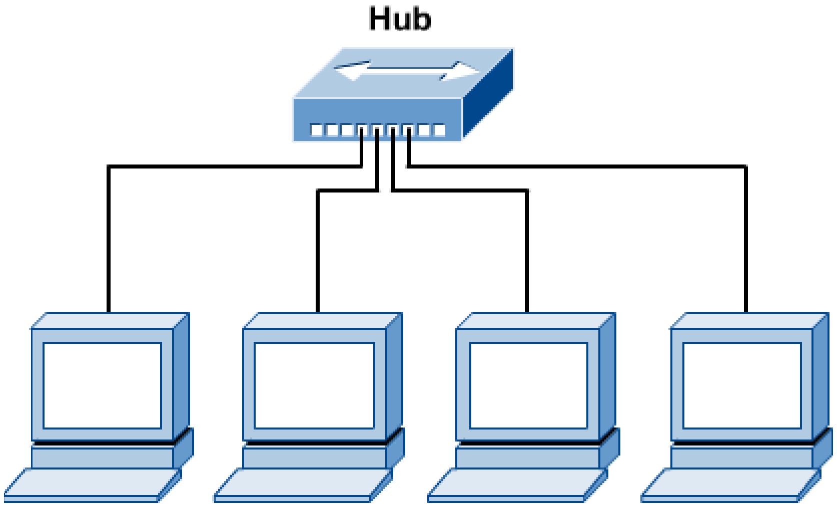




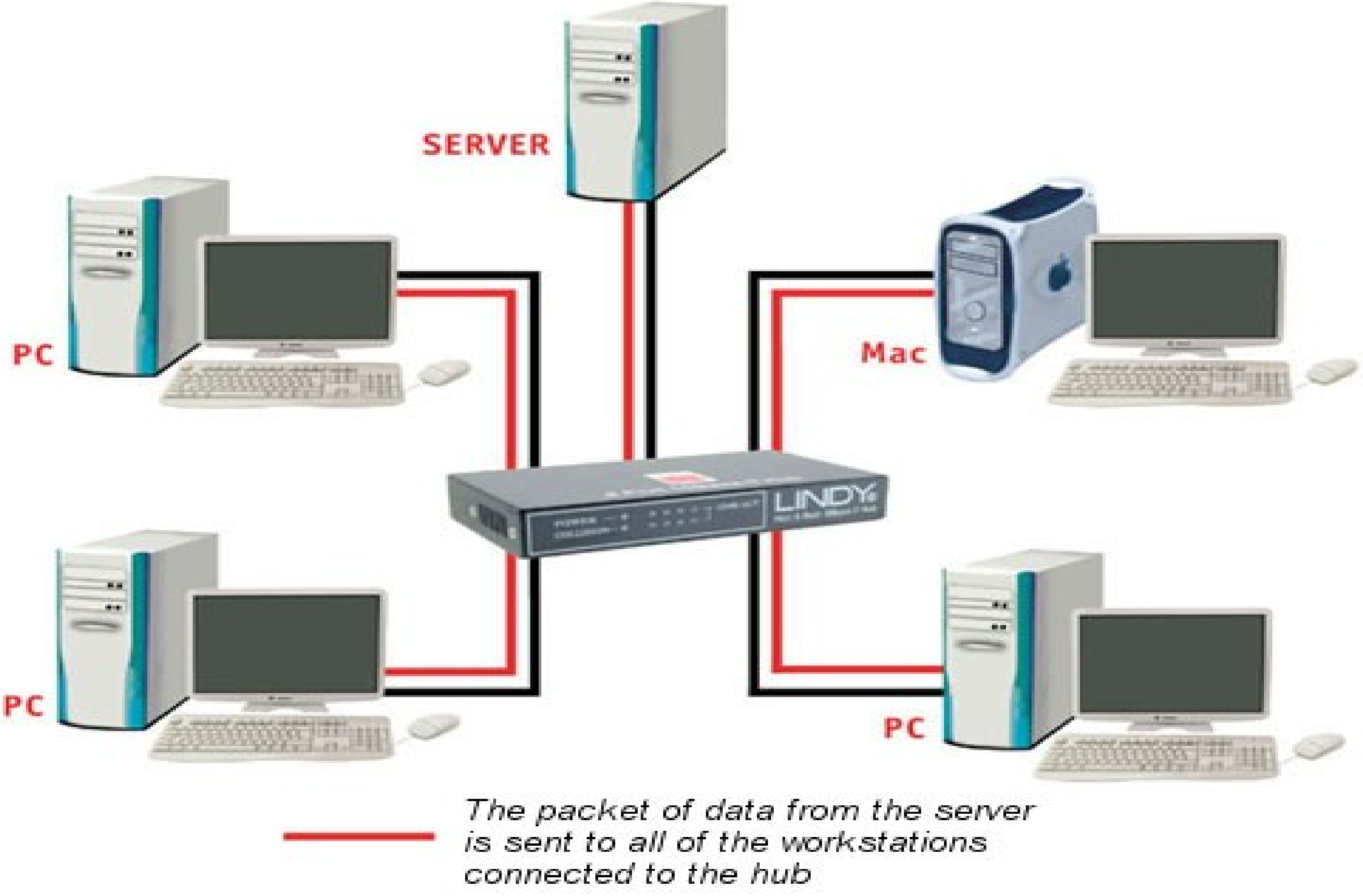
2. Hub

- Hubs are used to connect multiple nodes to a single physical device, which connects to the network.
- Hubs are actually multiport repeaters.
- Using a hub changes the network topology from a linear bus, to a star.
- With hubs, data arriving over the cables to a hub port is electrically repeated on all the other ports connected to the same network segment.





2.Hub----



━ The packet of data from the server is sent to all of the workstations connected to the hub

Types of Hubs

1. Passive hubs

- do not amplify the electrical signal of incoming packets before broadcasting them out to the network.
- It is just a connector.
- It connects the wires coming from different branches.
- In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point.
- This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Types of Hubs---

2. Active hubs,

- a type of hub that can perform amplification, as does a repeater.
- Some people use the terms concentrator when referring to a passive hub and multiport repeater when referring to an active hub.

3. Intelligent hubs

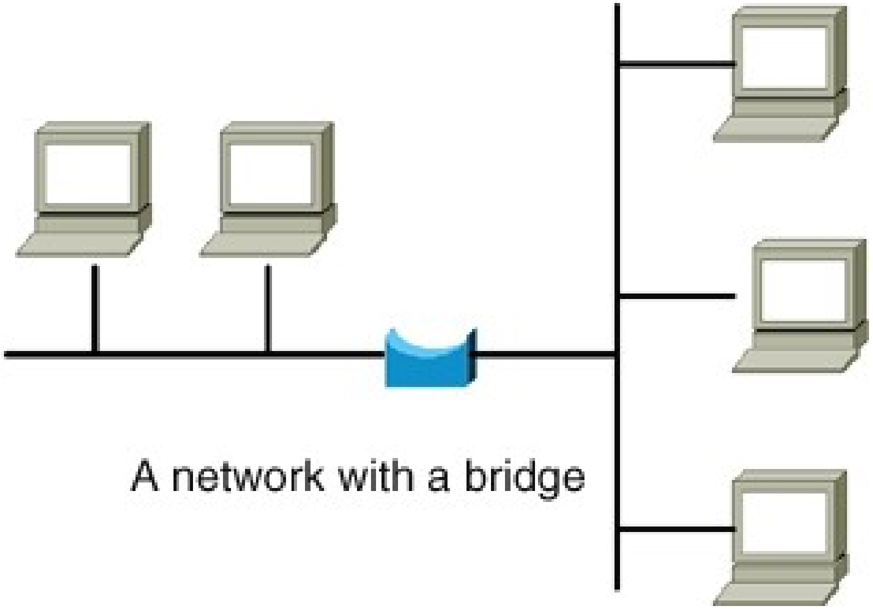
- add extra features to an active hub that are of particular importance to businesses.
- An intelligent hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space).
- It also typically includes remote management capabilities via SNMP and virtual LAN (VLAN) support

3. Bridge

- **Bridges are used to logically separate network segments within the same network.**
- **They operate at the OSI physical and data link layer and are independent of higher-layer protocols.**
- **As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.**
- **The function of the bridge is to make intelligent decisions about whether or not to pass signals on to the next segment of a network.**

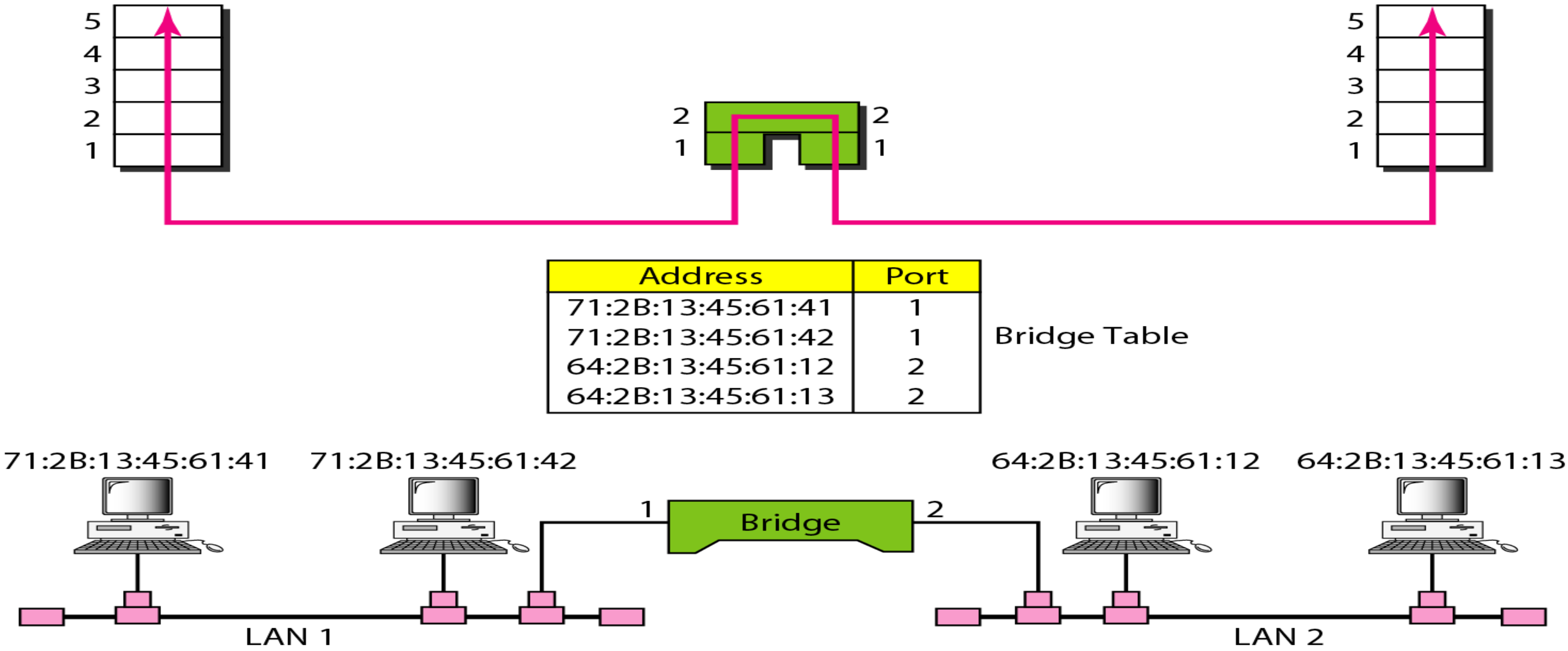
3. Bridge----

- When a bridge receives a frame on the network, the destination MAC address is looked up in the bridge table to determine whether to filter, flood, or copy the frame onto another segment
- Broadcast Packets are forwarded to all directions



➢ **Filtering**: A bridge has filtering capability.

- It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports.



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table

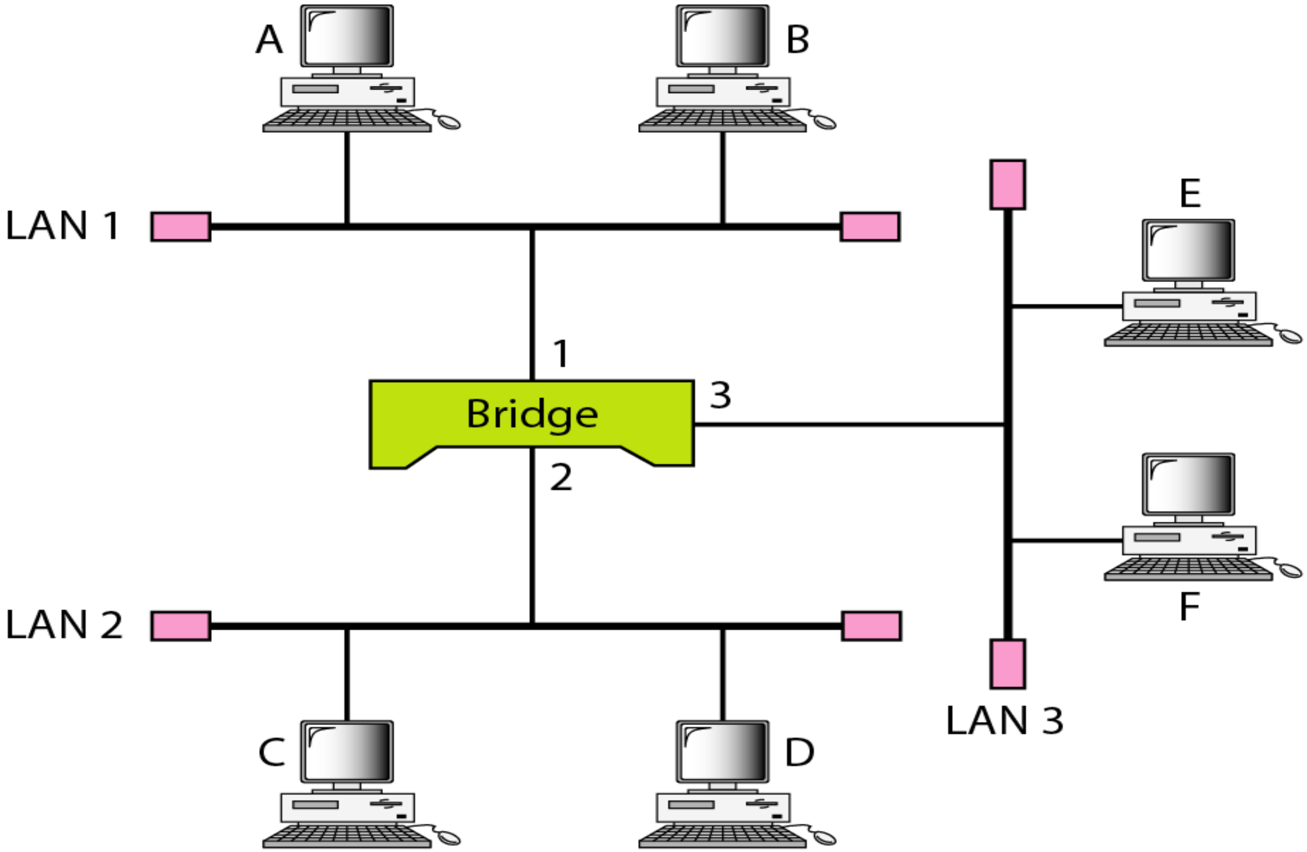
Cont...

- In the previous figure, if a frame destined for station 712B13456142 arrives at port 1, the bridge consults its table to find the departing port.
- According to its table, frames for 712B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped.
- On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded.
- In the first case, LAN 2 remains free of traffic; in the second case, both LANs have traffic.

MAC Address Learning

- Bridges MAC table can be static or dynamic.
- To make a table dynamic, we need a bridge that gradually learns from the frame movements.
- To do this, the bridge inspects both the destination and the source addresses.
- The destination address is used for the forwarding decision (table lookup); the source address is used for adding entries to the table and for updating purposes.

Learning Process – Example



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

1. When station A sends a frame to station D, the bridge does not have an entry for either D or A.

- The frame goes out from all three ports; the frame floods the network.
- However, by looking at the source address, the bridge learns that station A must be located on the LAN connected to port 1.

✓ This means that frames destined for A, in the future, must be sent out through port 1.

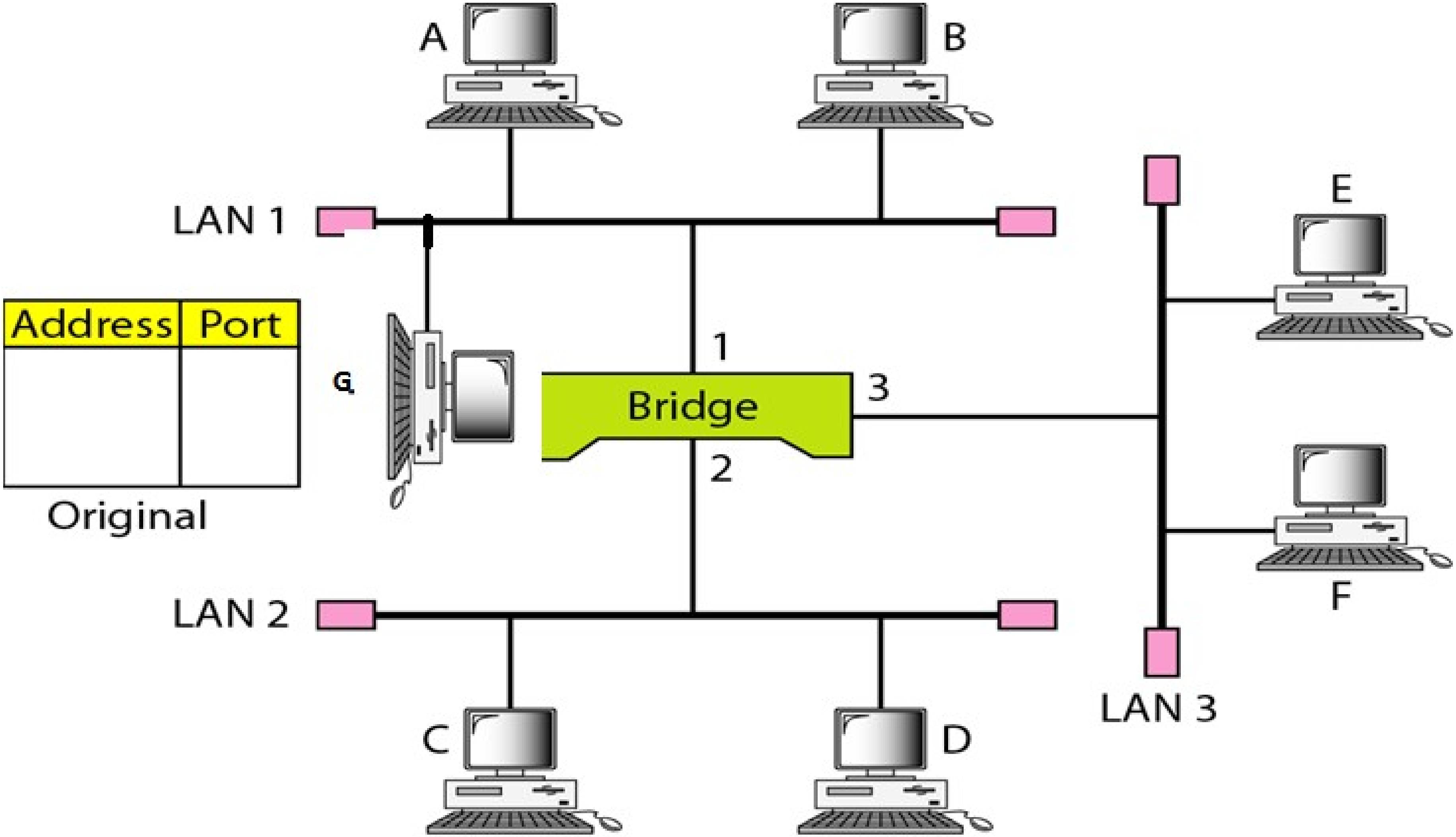
✓ The bridge adds this entry to its table. The table has its first entry now.

2. When station E sends a frame to station A, the bridge has an entry for A, so it forwards the frame only to port 1.

- There is no flooding.
- In addition, it uses the source address of the frame, E, to add a second entry to the table.

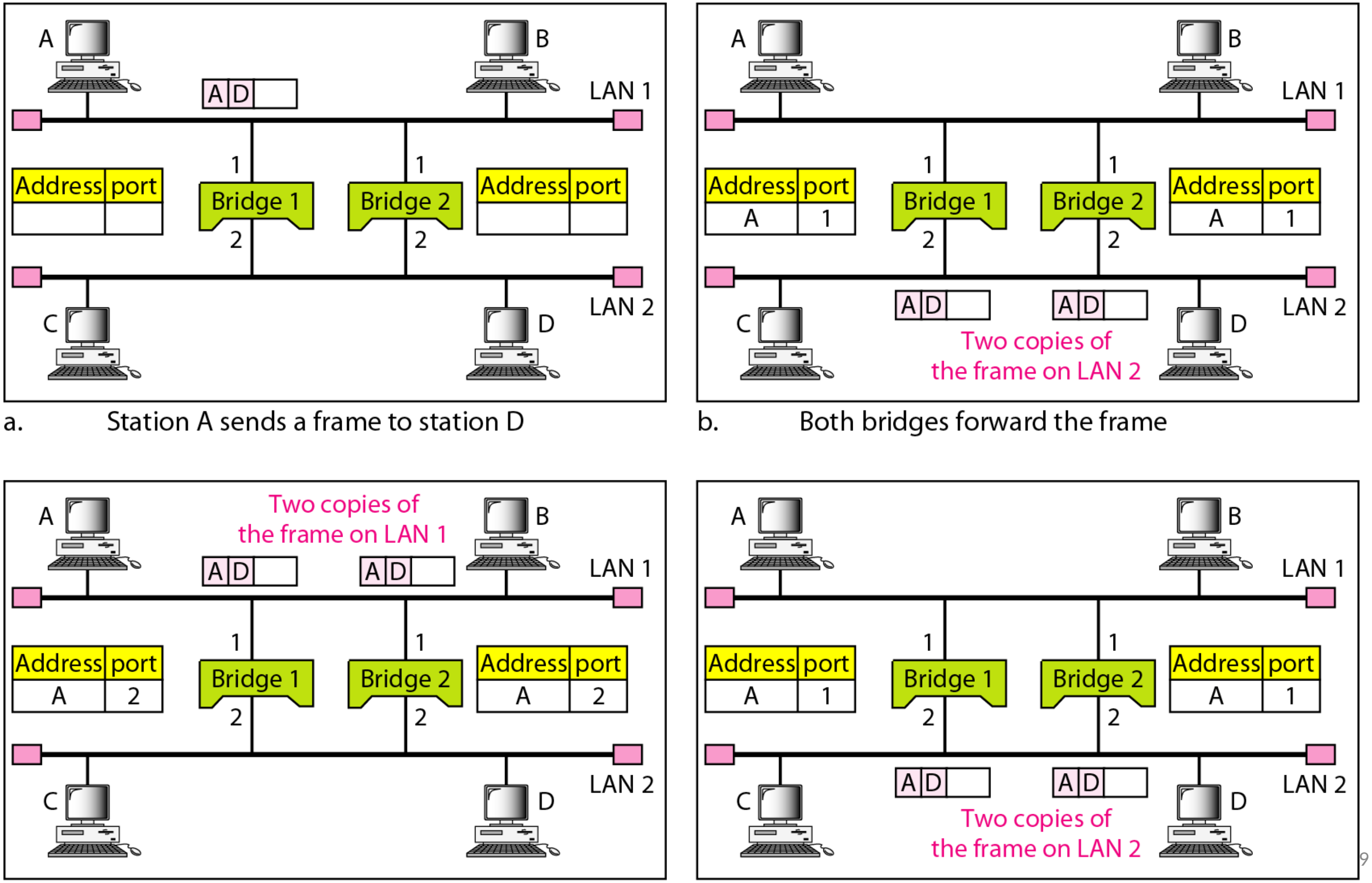
3. When station B sends a frame to C, the bridge has no entry for C, so once again it floods the network and adds one more entry to the table.
4. The process of learning continues as the bridge forwards frames.

- Quiz3 (g9-10): in the following diagram, if the following series of data transmission occurs, show how the Bridge table is built and tell if filtering or flooding is done in every step. Use A,B,C.. As MAC addresses and 1,2,3 as port numbers: A-G; G-D; C-D; F-G



Looping Problem in bridges

- A transparent bridge works fine as far as no redundant bridge in the network



Two copies of the frame on LAN 2

Two copies of the frame on LAN 1

a. Station A sends a frame to station D

b. Both bridges forward the frame

c. Both bridges forward the frame

d. Both bridges forward the frame

Cont...

1. Station A sends a frame to station D.

- The tables of both bridges are empty. Both forward the frame and update their tables based on the source address A.

2. Now there are two copies of the frame on LAN 2.

- The copy sent out by bridge 1 is received by bridge 2, which does not have any information about the destination address D; it floods the bridge.
- The copy sent out by bridge 2 is received by bridge 1 and is sent out for lack of information about D.

Cont…

- Note that each frame is handled separately because bridges, as two nodes on a network sharing the medium, use an access method such as CSMA/CD.
- The tables of both bridges are updated, but still there is no information for destination D.

3. Now there are two copies of the frame on LAN 1. Step 2 is repeated, and both copies flood the network.
4. The process continues on and on.

- Note that bridges are also repeaters and regenerate frames.
- So in each iteration, there are newly generated fresh copies of the frames

Reading Assignment:

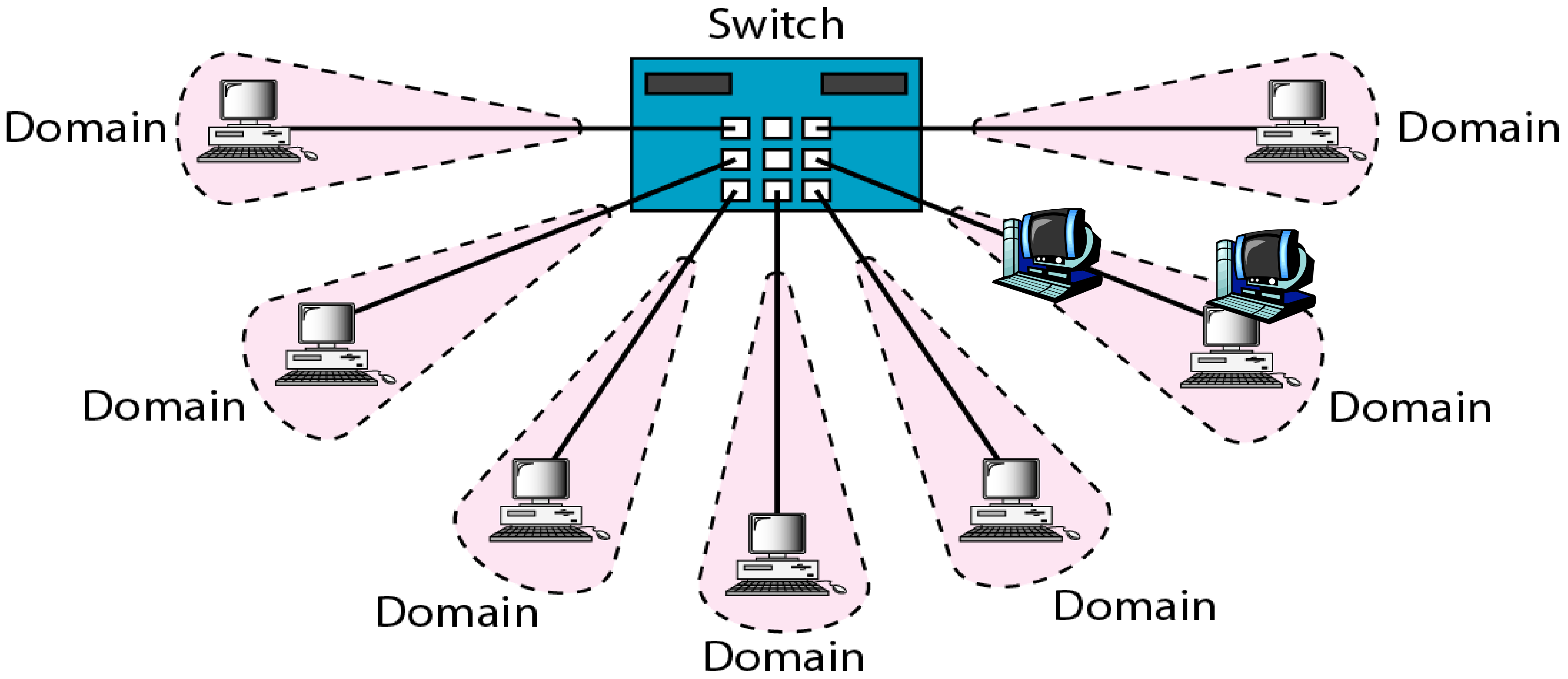
- To solve the looping problem, the IEEE specification requires that bridges use the spanning tree algorithm to create a loopless topology. Read About spanning tree algorithm

4. Switch

- Switches are Multiport Bridges.
- Switches provide a unique network segment on each port, thereby separating collision domains.
- Today, network designers are replacing hubs in their wiring closets with switches to increase their network performance and bandwidth while protecting their existing wiring investments.
- Like bridges, switches learn certain information about the data packets that are received from various computers on the network.
- Switches use this information to build forwarding tables to determine the destination of data being sent by one computer to another computer on the network.

Switches: Dedicated Access

- Hosts have direct connection to switch
- Full Duplex: No collisions
- Switching: A-to-A’ and B-to-B’ simultaneously, no collisions
- Switches can be cascaded to expand the network



Two/three-layer switches

- When we use the term switch, we must be careful because a switch can mean two different things. We must clarify the term by adding the level at which the device operates.
- We can have a two-layer switch or a three-layer switch.
- A three-layer switch is used at the network layer; it is a kind of router.
- The two-layer switch performs at the physical and data link layers.
- A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance.
- A bridge with a few ports can connect a few LANs together.
- A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.
- ✓ This means no competing traffic (no Collision)

Types of Switches

1.Cut-through switch

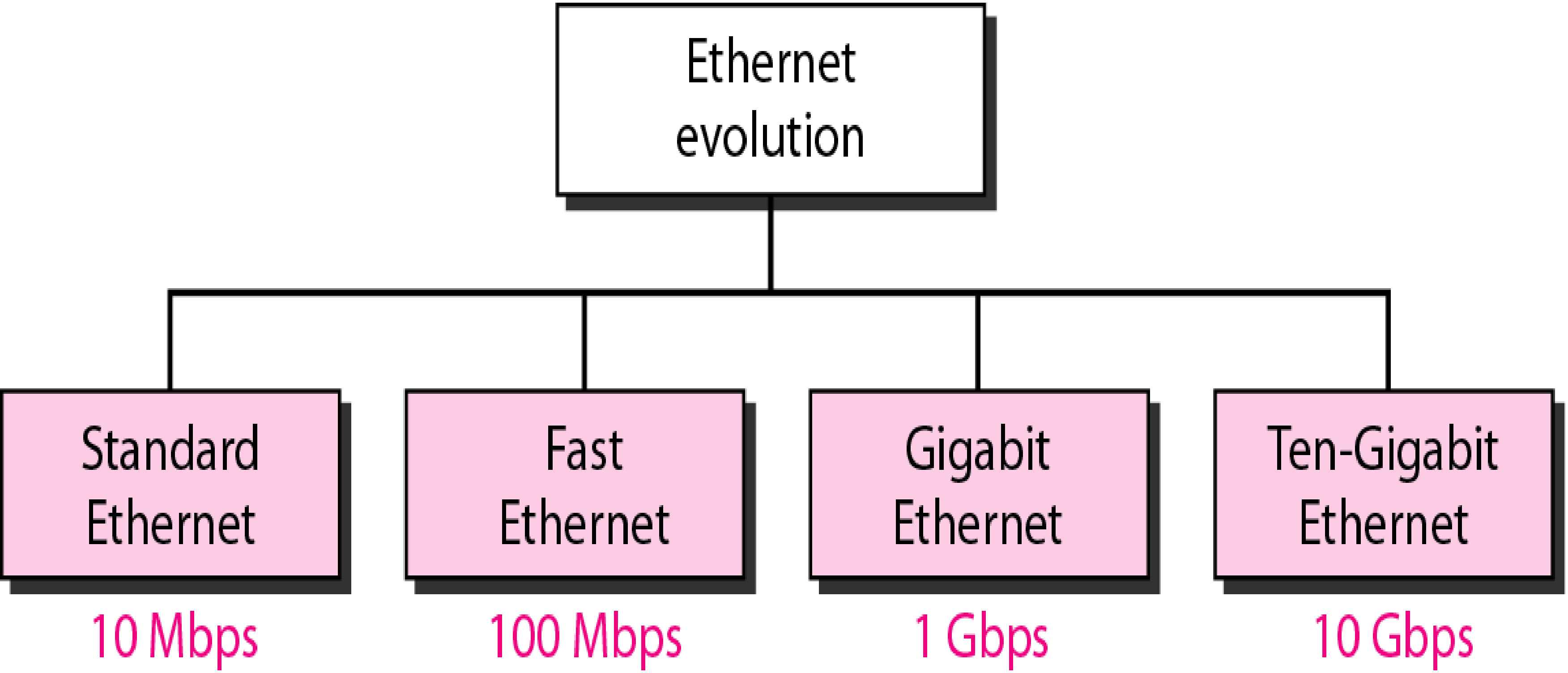
- Cut-through switch is a packet switch wherein the switch starts forwarding that frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed.
- A cut-through switch can achieve the lowest forwarding delays, but it propagates errors from one LAN to another, because errors can only be detected at the end of each frame.
- In other words, this technique reduces latency through the switch, but decreases reliability.

2.Store and Forward Switch

- A switching device that stores a complete incoming data packet before it is sent out.
- Such switches are used when incoming and outgoing speeds differ

LAN Technology Options

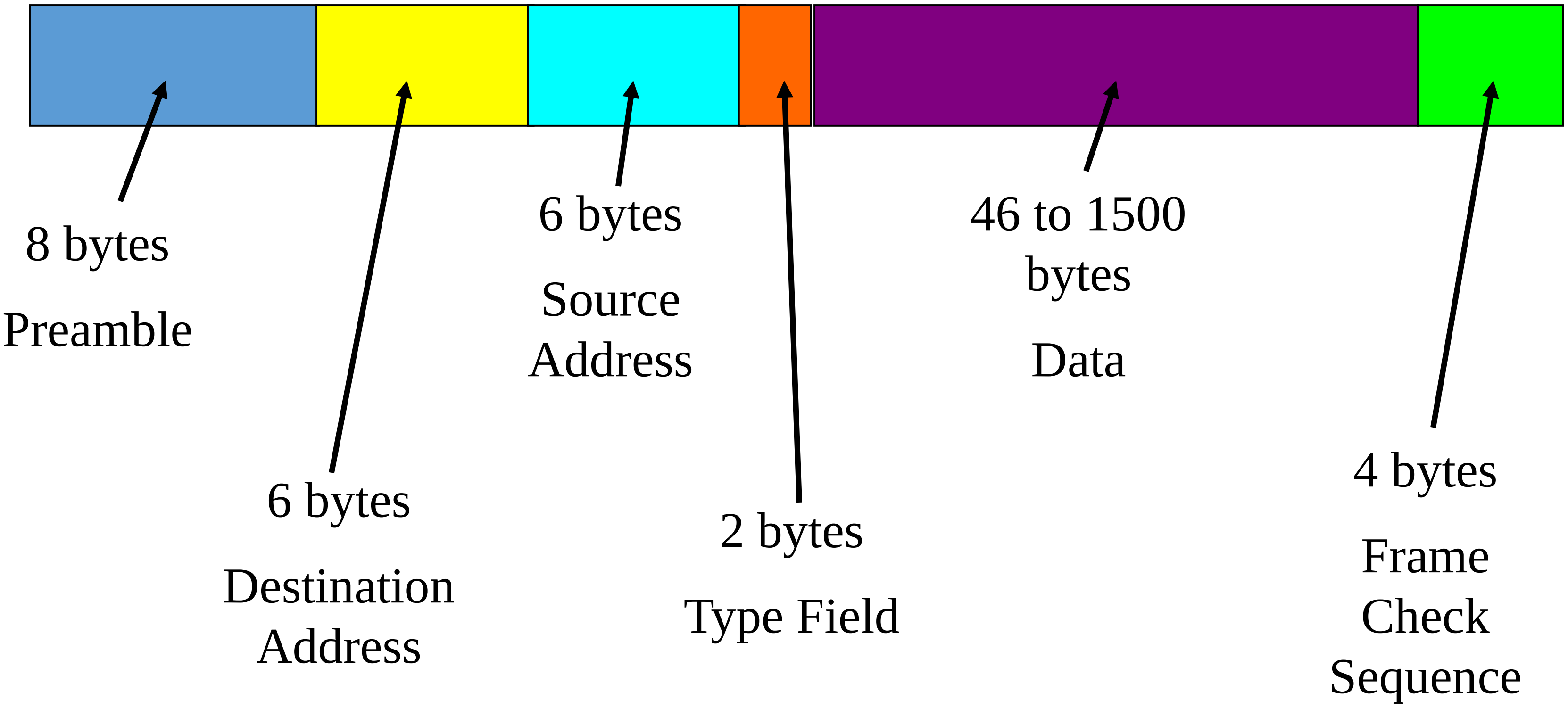
- **Ethernet**
- **Fast Ethernet**
- **Gigabit Ethernet**
- **10 Gig Ethernet**



1. Ethernet

- Developed by Xerox in 1976
- Eventually became an IEEE standard (IEEE 802.3)
  - ✓ Has been modified for wireless applications (IEEE 802.11)
  - ✓ And for higher speeds (IEEE 802.3ae for 10 Gigabit Ethernet)
- **Ethernet** is based on the **Datagram** and functions at the **physical** and **data link layer**

Ethernet Datagram Structure



8 bytes

Preamble

6 bytes

Destination Address

6 bytes

Source Address

2 bytes

Type Field

46 to 1500 bytes

Data

4 bytes

Frame Check Sequence

Ethernet Datagram Structure---

- **Preamble**:

✓Repeating Flag that ID’s the sequence as an Ethernet datagram

- **Destination Address**:

✓Unique identifier found nowhere else but on the Network Interface Card to whom the datagram is being sent

- **Source Address**:

✓Who originated the datagram

- **Type Field**:

✓Tells the recipient what kind of datagram is being received (IP, UDP, etc)

- **Data**:

✓What it is that you are trying to send (text, JEPG, MP3, etc)

- **Frame Check Sequence**:

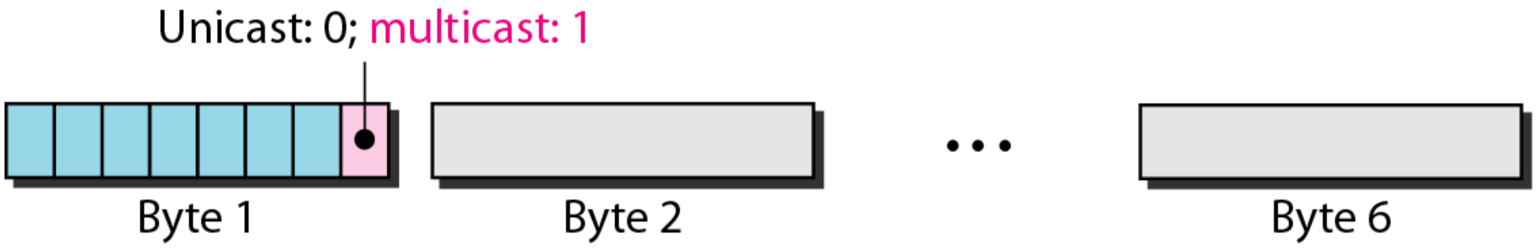
✓Detects and corrects errors

Ethernet Tidbits

- If a message has less than 46 bytes of data, “padding” is added
- Ethernet is often referred to as **100 Base T**
  - First digit is the speed of the system in Mbps
  - Base refers to a cable or wire system
  - T refers to the system is UTP: Unshielded Twisted Pair
  - 10 Base 5 stands for 10 Mbps on a cable that can go 500 m (multiply the last number by 100 meters)
  - 10 Base 2 stands for 10 Mbps for 2 hundred meters
  - 10 Base 5 and 10 Base 2 identifies Ethernet LANs using thick net and thin net coax cables, respectively

Ethernet Address

- **End nodes are identified by their Ethernet Addresses (MAC Address or Hardware Address) which is a unique 6 Byte address.**
- **MAC Address is represented in Hexa Decimal format e.g 00:05:5D:FE:10:0A** (48 bits)
- **The first 3 bytes identify a vendor (also called prefix) and the last 3 bytes are unique for every host or device**
- **The least significant bit of the first byte defines the type of address. If the bit is 0, the address is unicast; otherwise, it is multicast.**
- **The broadcast destination address is a special case of the multicast address in which all bits are 1s.**



Quiz 3(g3-4)

- *Define the type of the following destination addresses:*
  - *a.4A:30:10:21:10:1A*
  - *b. 47:20:1B:2E:08:E7*
  - *c. FF:FF:FF:FF:FF:FF*

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

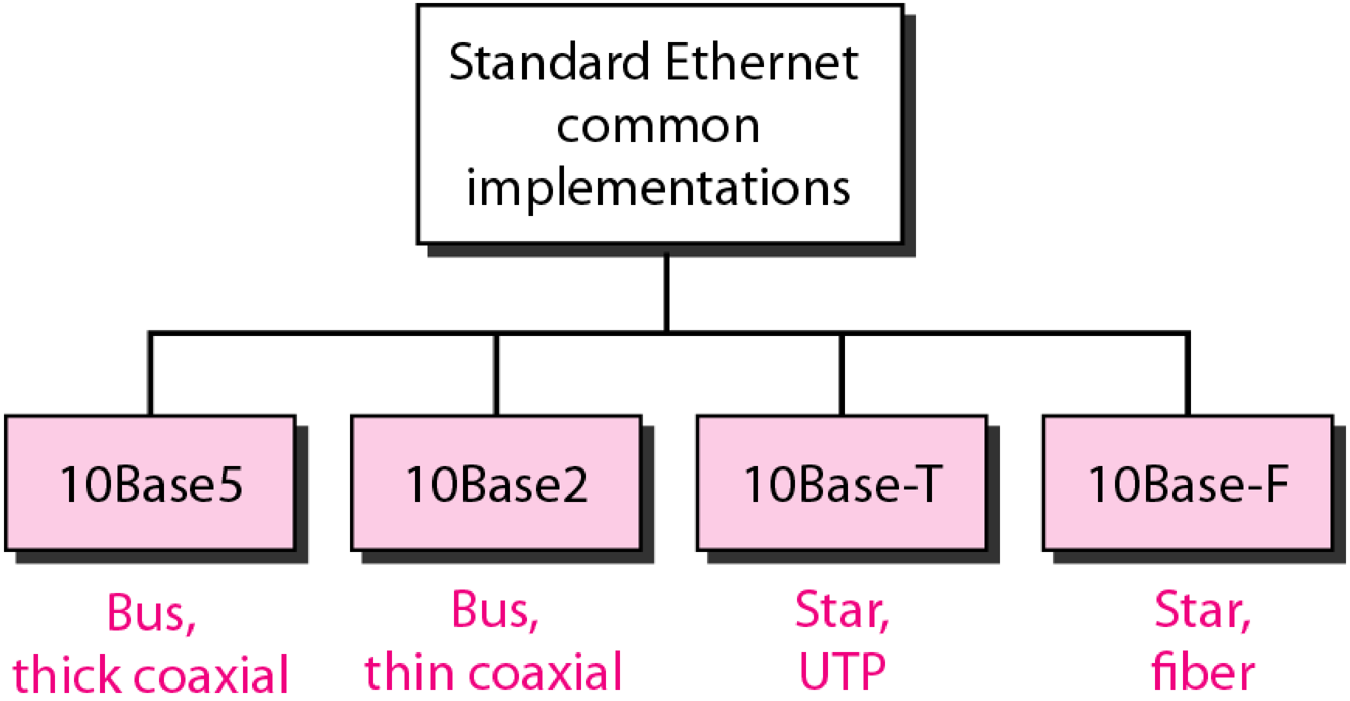
a. This is a unicast address because A in binary is 1010.

b. This is a multicast address because 7 in binary is 0111.

c. This is a broadcast address because all digits are F's.

Standard Ethernet

- 10 Base 5 (Thicknet) (Bus Topology)
- 10 Base 2 (Thinnet) (Bus Topology)
- 10 Base T (UTP) (Star/Tree Topology)
- 10 Base FL (Fiber) (Star/Tree Topology)



Ethernet

- **Physical Media :-**
  - 10 Base5 - Thick Co-axial Cable with Bus Topology
  - 10 Base2 - Thin Co-axial Cable with Bus Topology
  - 10 BaseT - UTP Cat 3/5 with Tree Topology
  - 10 BaseFL - Multimode/Singlemode Fiber with Tree Topology
- **Maximum Segment Length**
  - 10 Base5 - 500 m with at most 4 repeaters (Use Bridge to extend the network)
  - 10 Base2 - 185 m with at most 4 repeaters (Use Bridge to extend the network)
  - 10 BaseT - 100 m with at most 4 hubs (Use Switch to extend the network)

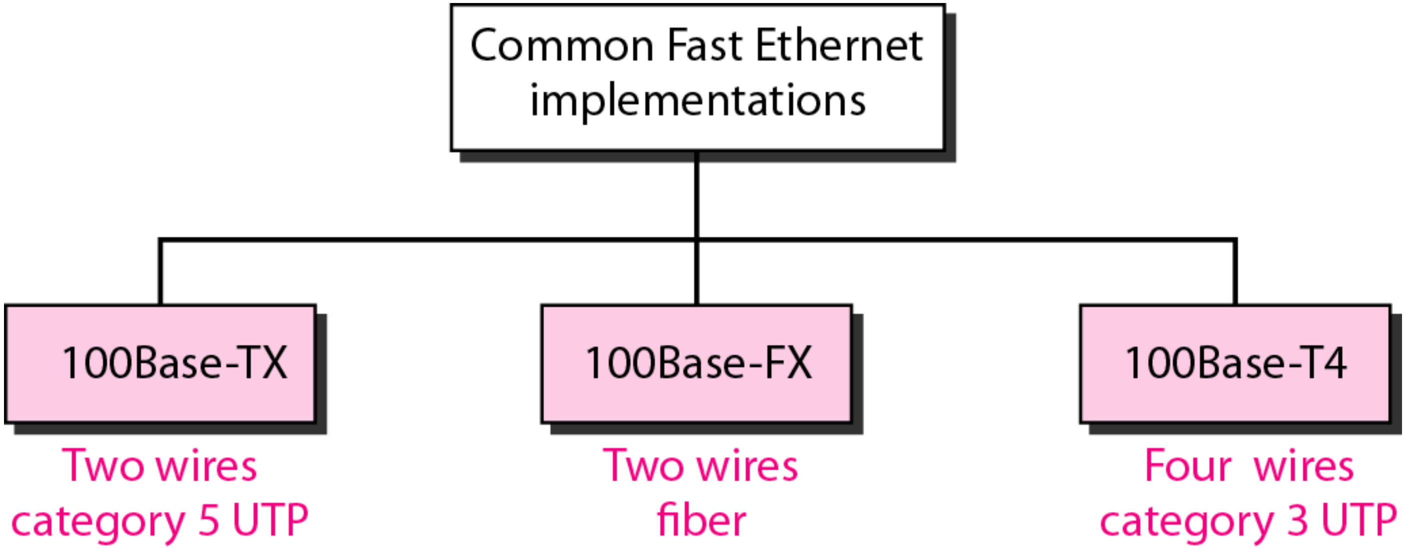
Fast Ethernet

- 100 Mbps bandwidth
- Uses same CSMA/CD media access protocol and packet format as in Ethernet.
- 100BaseTX (UTP) and 100BaseFX (Fiber) standards
- Physical media :-
  - 100 BaseTX - UTP Cat 5e
  - 100 BaseFX - Multimode / Singlemode Fiber
- Full Duplex/Half Duplex operations.

Fast Ethernet

- **Provision for Auto-Negotiation of media speed: 10 Mbps or 100Mbps (popularly available for copper media only).**

- **Maximum Segment Length**
  - **100 Base TX - 100 m**
  - **100 Base FX - 2 Km (Multimode Fiber)**
  - **100 Base FX - 20 km (Singlemode Fiber)**



Gigabit Ethernet

- **1 Gbps bandwidth.**
- **Uses same CSMA/CD media access protocol as in Ethernet and is backward compatible (10/100/100 modules are available).**
- **1000BaseT (UTP), 1000BaseSX (Multimode Fiber) and 1000BaseLX (Multimode/Singlemode Fiber) standards.**
- **Maximum Segment Length**

1000 Base T	- 100m (Cat 5e/6)
1000 Base SX	- 275 m (Multimode Fiber)
1000 Base LX	- 512 m (Multimode Fiber)
1000 Base LX	- 20 Km (Singlemode Fiber)
1000 Base LH	- 80 Km (Singlemode Fiber)

10 Gig Ethernet

- **10 Gbps bandwidth.**
- **Uses same CSMA/CD media access protocol as in Ethernet.**
- **Maximum Segment Length**
  - 10GBase-T - Not available
  - 10GBase-LR - 10 Km (Singlemode Fiber)
  - 10GBase-ER - 40 Km (Singlemode Fiber)

WANs

Characteristics of WANs

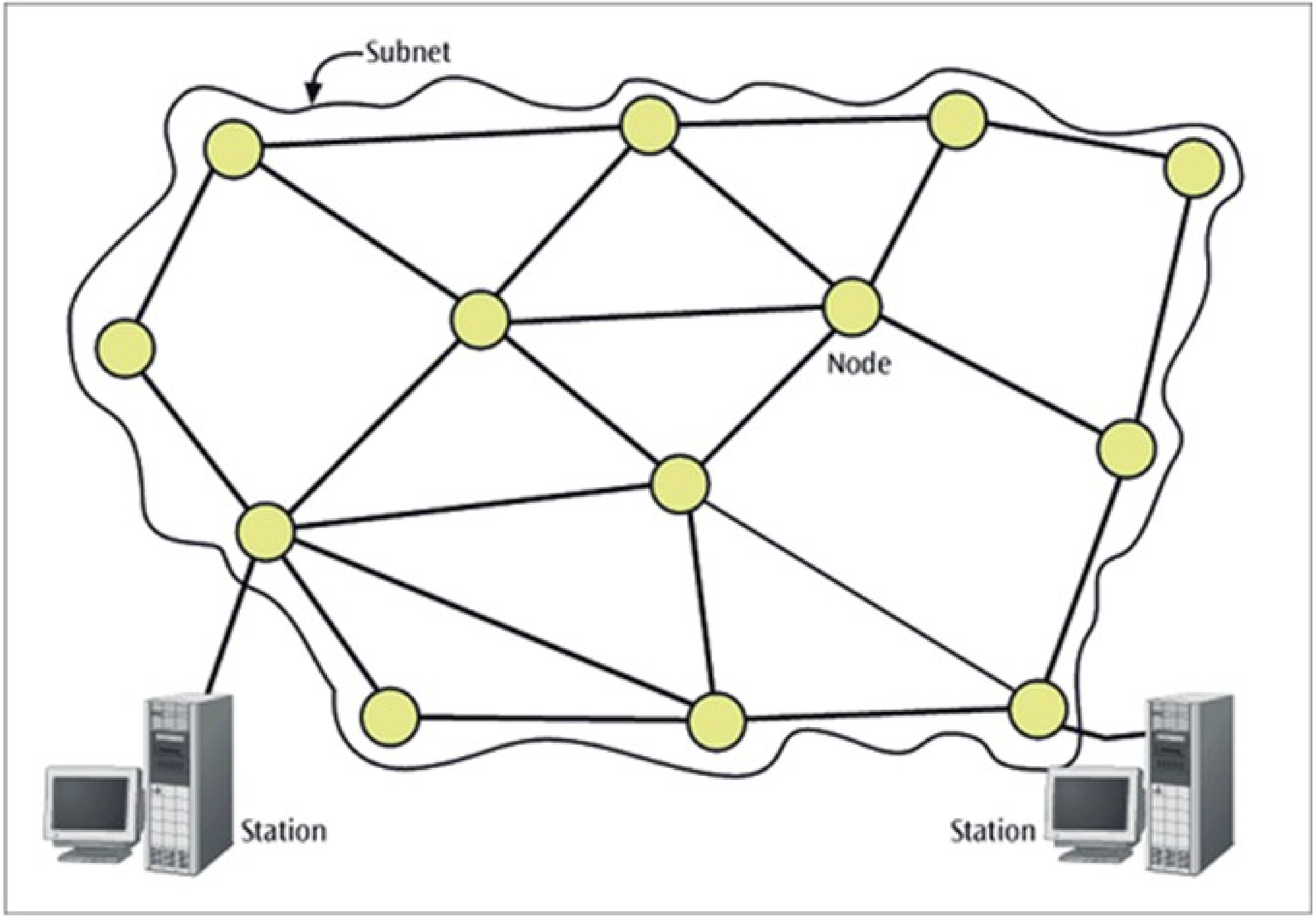
- Similarities to LANs
  - Interconnect computers.
  - Use some form of media for the interconnection.
  - Support network applications.
- Differences to LANs
  - Include both data networks, such as the Internet, and voice networks, like telephone systems.
  - Interconnect more workstations, so that any one workstation can transfer data to any other workstation.
  - Cover large geographic distances, including the earth.

Wide Area Network Basics

- A *station* is a device that interfaces a user to a network.
- A *node* is a device that allows one or more stations to access the physical network and is a transfer point for passing information through a network. A node is often a computer, a router, or a telephone switch.
- The *subnet* (old terminology) or physical network is the underlying connection of nodes and telecommunication links.

WAN Technologies

Network subnet, nodes, and two end stations



Types of WAN Network Subnets

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

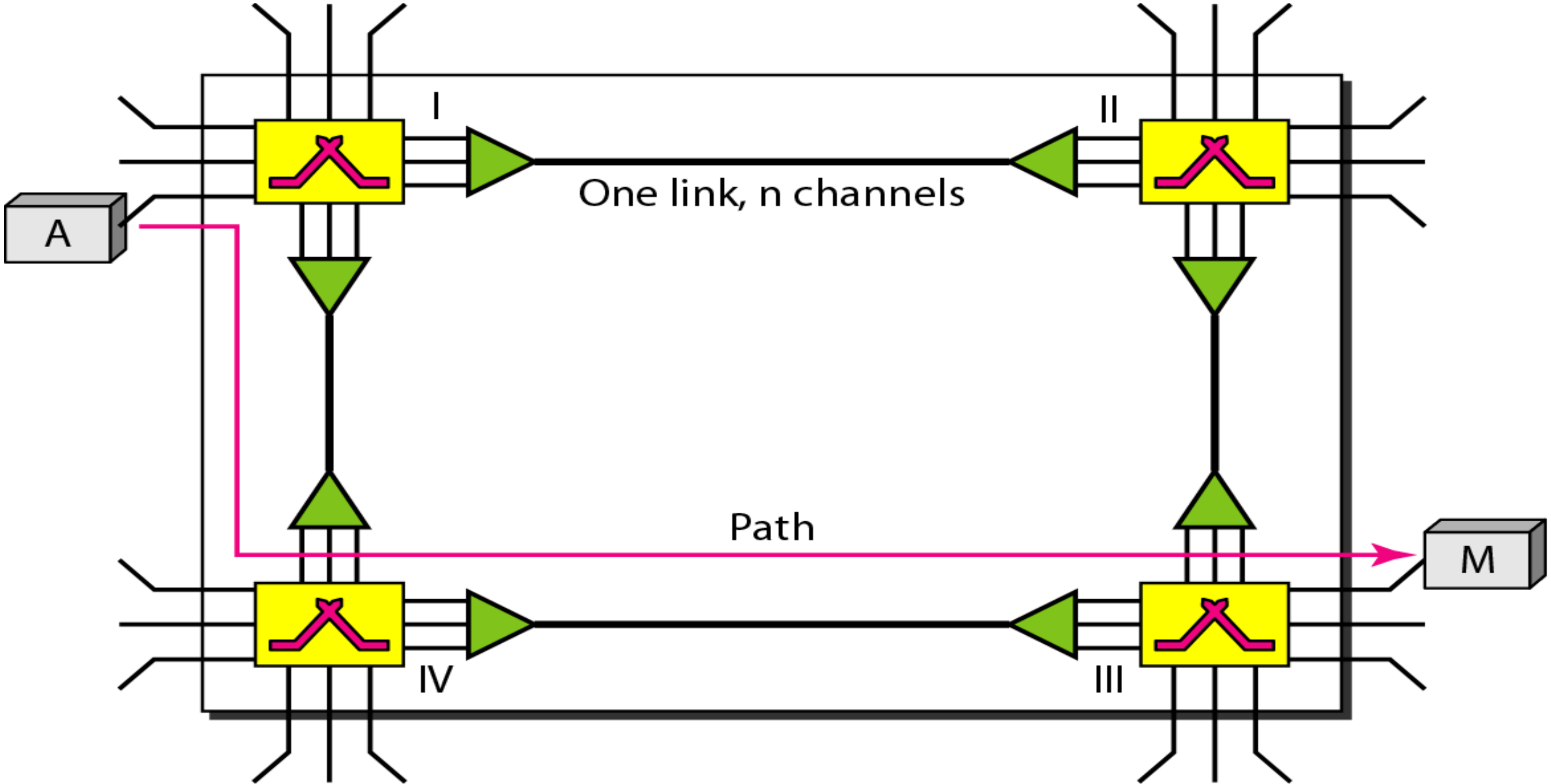
A network categorized by the way it transfers information from one node to another as

1. ***Circuit switched network*** - a network in which a dedicated circuit is established between sender and receiver and all data passes over this circuit. The connection is dedicated until one party or another terminates the connection. The telephone system is a common example.
2. ***Packet switched network*** - a network in which all data messages are transmitted using fixed-sized packages, called packets (data gram and virtual-switched network).

- Packet-switched networks can further be divided into two subcategories-**virtual-circuit networks** and **datagram networks**

CIRCUIT-SWITCHED NETWORKS

- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM



…

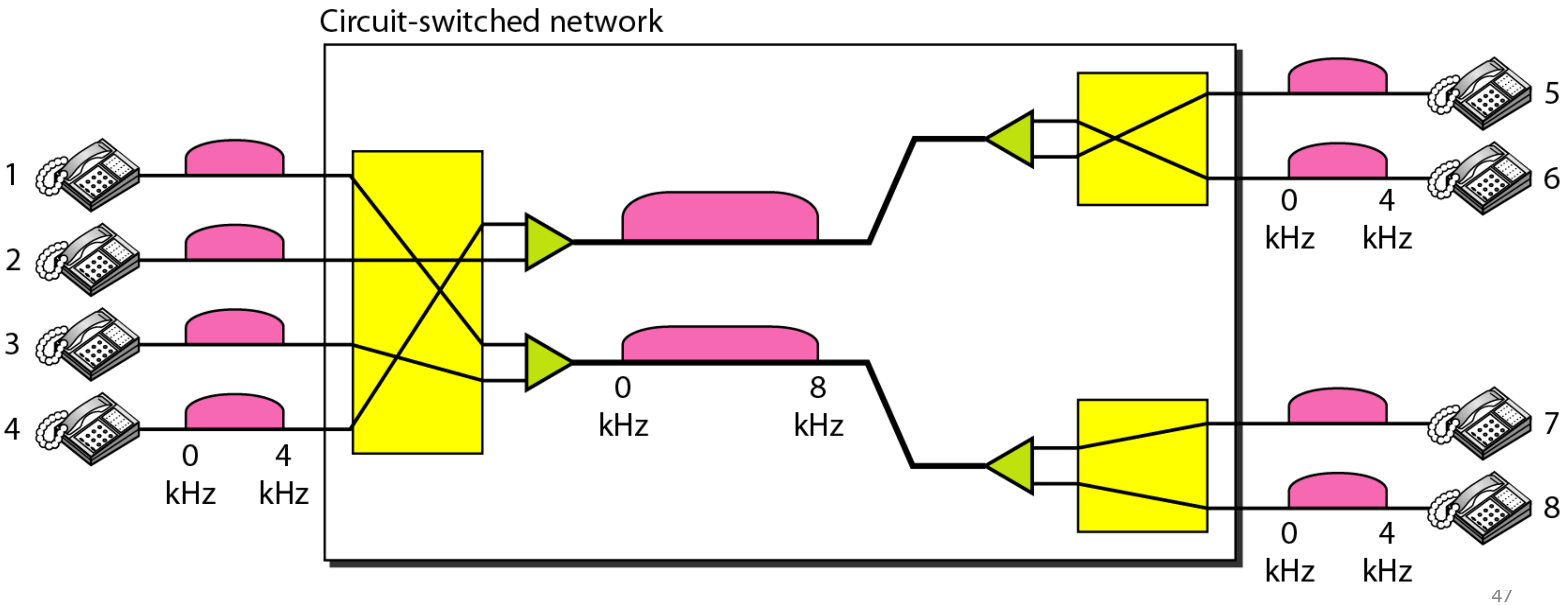
- As shown above, when end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself.
- This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path.
- After the dedicated path made of connected circuits (channels) is established, data transfer can take place.
- After all data have been transferred, the circuits are torn down.

Circuit switched network

1. Circuit switching takes place at the physical layer.
2. Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.
3. Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
4. There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used during the setup phase.

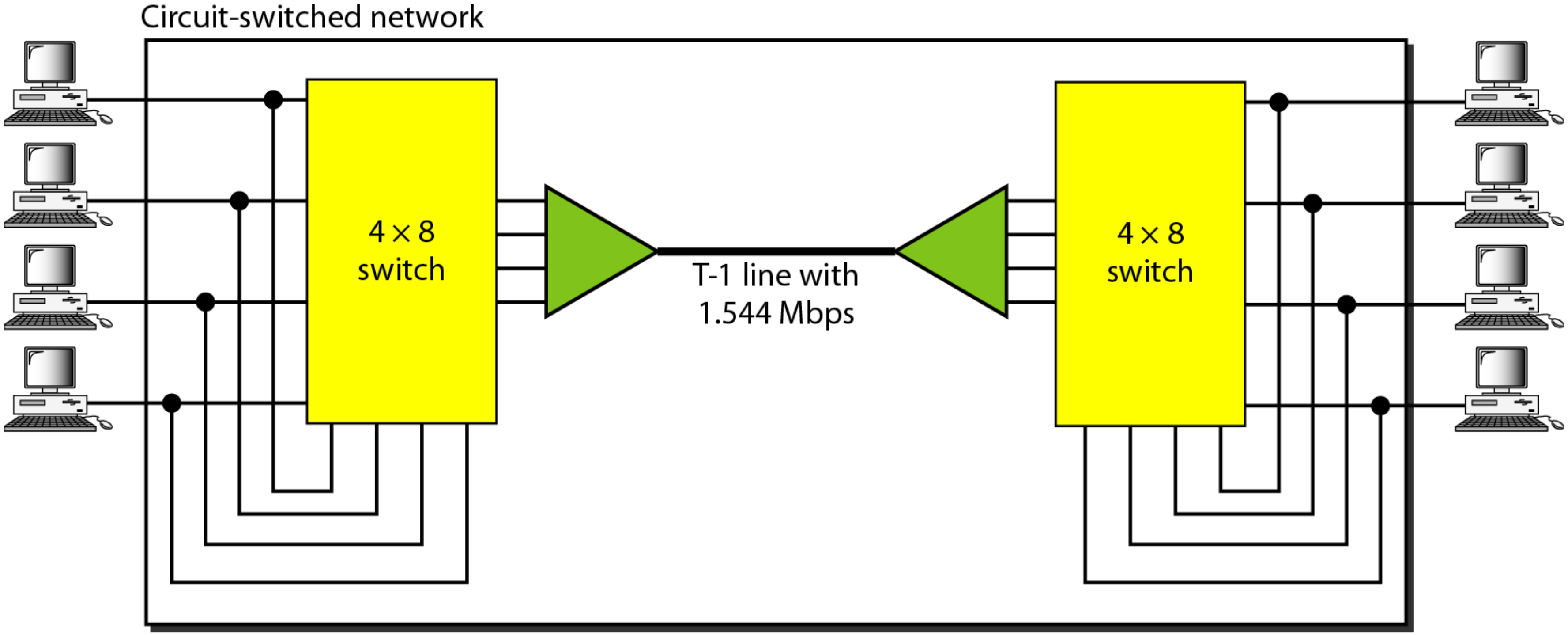
Example

- *As a trivial example, let us use a circuit-switched network to connect eight telephones in a small area. Communication is through 4-kHz voice channels. We assume that each link uses FDM to connect a maximum of two voice channels. The bandwidth of each link is then 8 kHz. The figure below shows the situation. Telephone 1 is connected to telephone 7; 2 to 5; 3 to 8; and 4 to 6. Of course the situation may change when new connections are made. The switch controls the connections.*



Example 2

- *As another example, consider a circuit-switched network that connects computers in two remote offices of a private company. The offices are connected using a T-1 line leased from a communication service provider. There are two 4 × 8 (4 inputs and 8 outputs) switches in this network. For each switch, four output ports are folded into the input ports to allow communication between computers in the same office. Four other output ports allow communication between the two offices.*

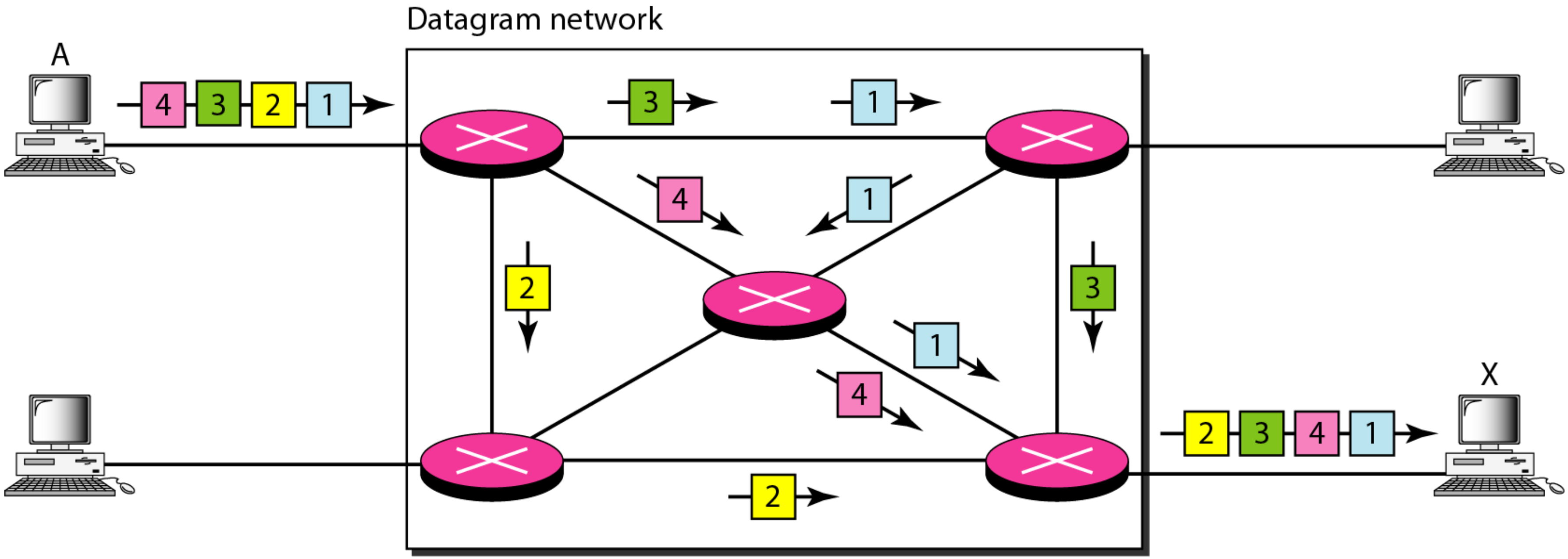


Packet Switched Networks:
DATAGRAM NETWORKS

- In data communications, we need to send messages from one end system to another. If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first-come, first-served basis.
- When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed. As with other systems in our daily life, this lack of reservation may create delay.

…

- In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone.
- Packets in this approach are referred to as datagrams.
- Datagram switching is normally done at the network layer. We briefly discuss datagram networks here as a comparison with circuit-switched and virtual-circuit-switched networks.

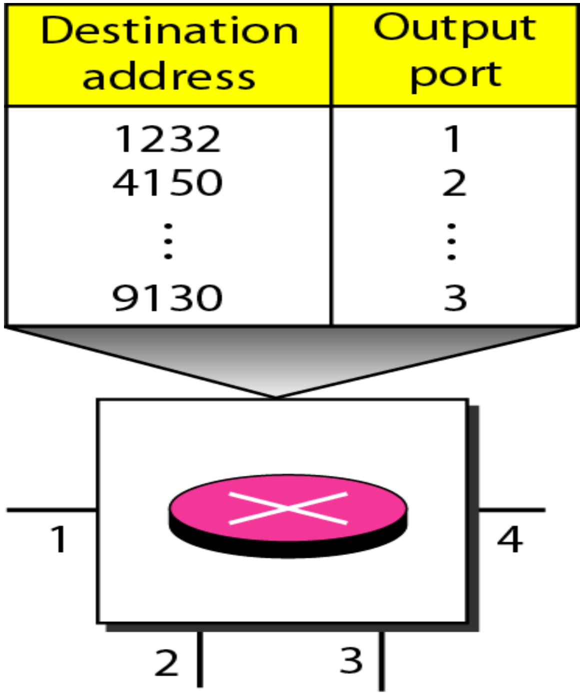


- In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X.
- This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

- The datagram networks are sometimes referred to as connectionless networks.
- The term *connectionless here means that the switch (packet switch) does not keep information* about the connection state.
- There are no setup or teardown phases.
- Each packet is treated the same by a switch regardless of its source or destination.

Routing Table

- If there are no setup or teardown phases, how are the packets routed to their destinations in a datagram network? In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.
- This is different from the table of a circuit-switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.



Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3

Destination Address

- Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.
- This address, unlike the address in a virtual-circuit-switched network, remains the same during the entire journey of the packet.

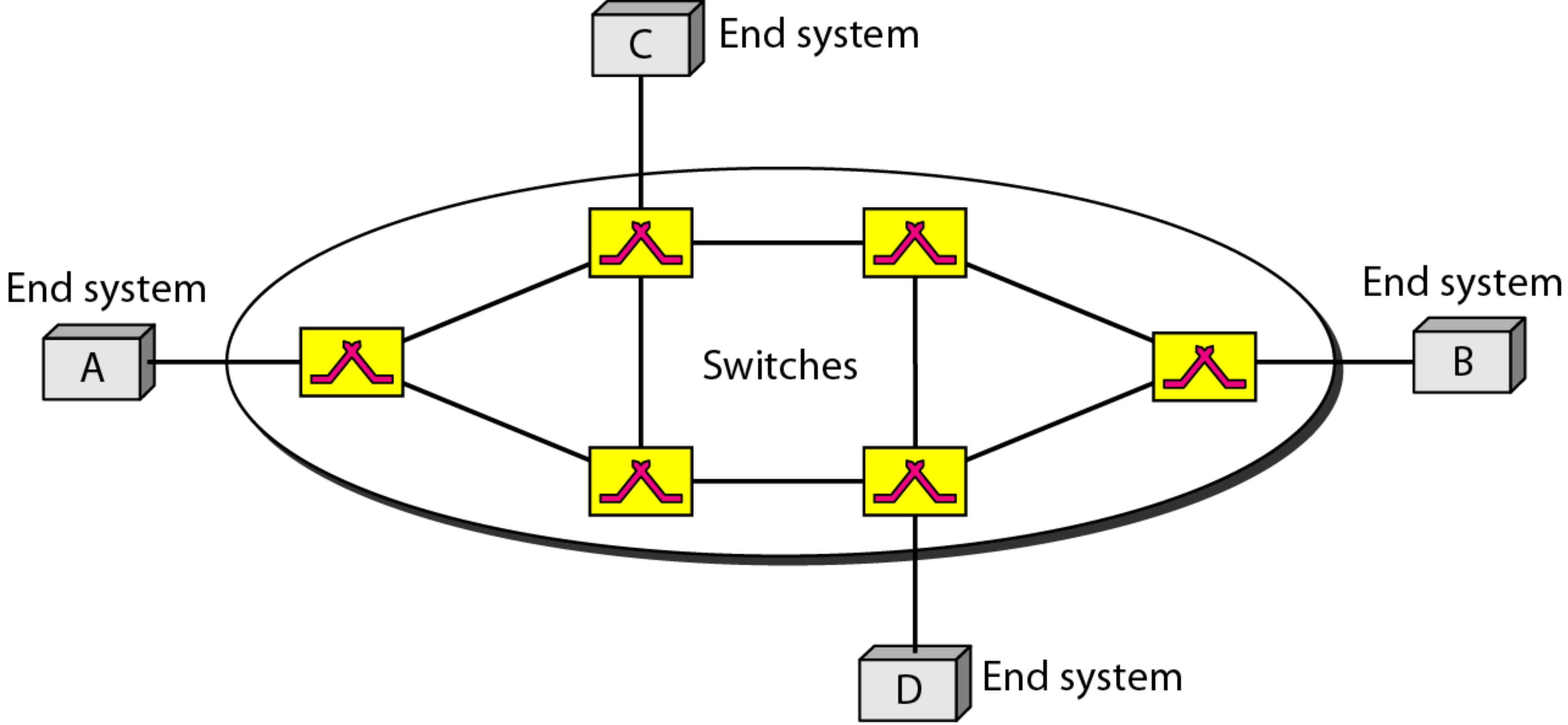
•Efficiency

- The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.

Packet Switched Networks:
VIRTUAL-CIRCUIT NETWORKS

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being carried), not end-to-end jurisdiction. How the intermediate switches know where to send the packet if there is no final destination address carried by a packet? Using virtual-circuit identifiers.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

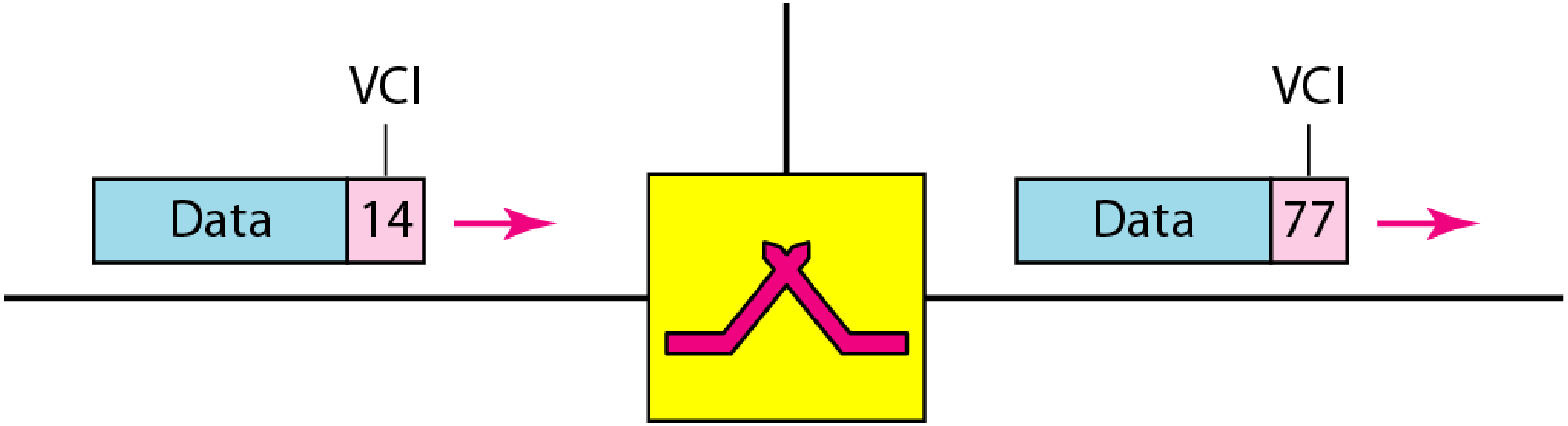


- The above figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.

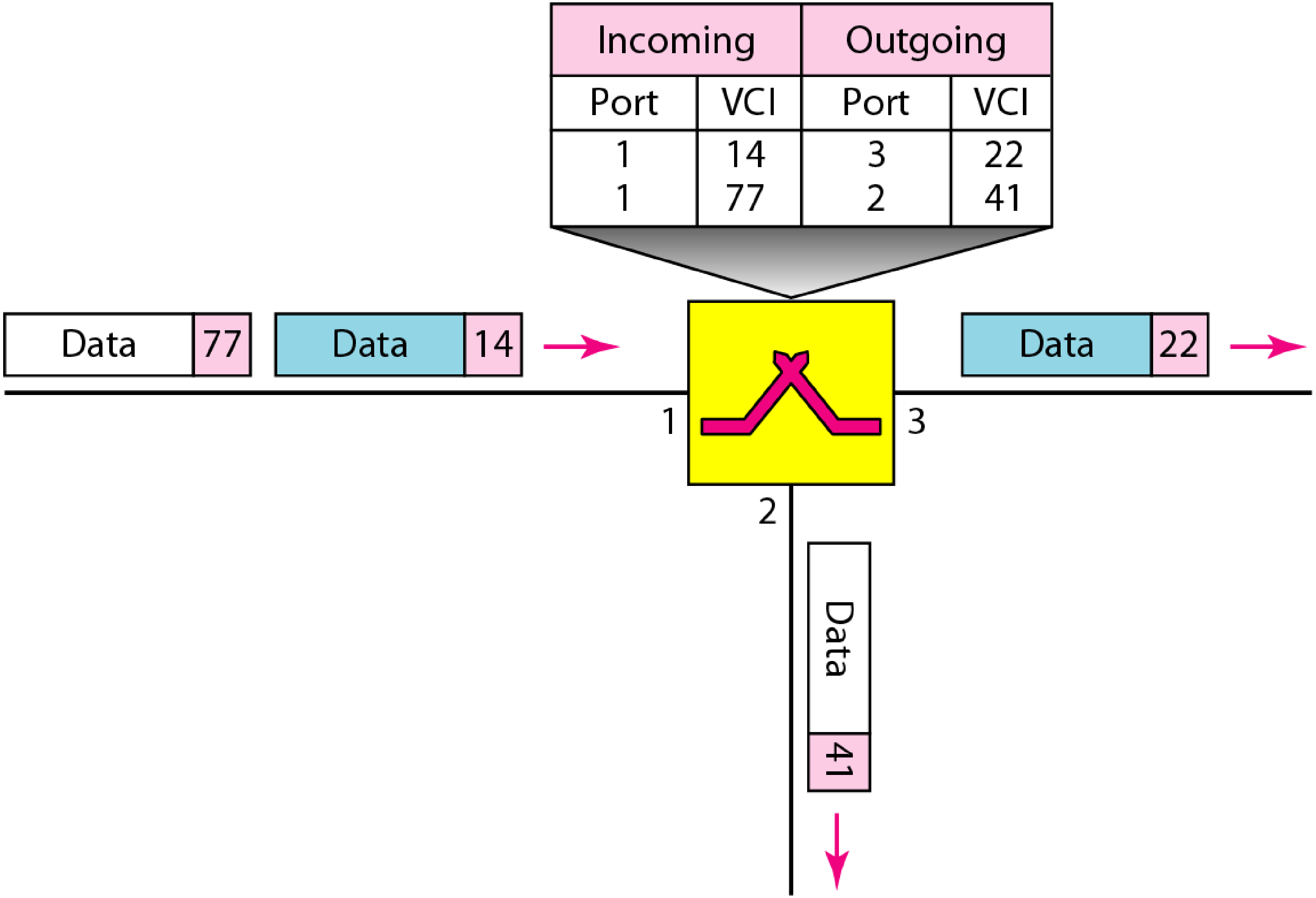
Addressing

- In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).
- *Global Addressing*
  - A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, a global address in virtual-circuit networks is used only to create a virtual-circuit identifier.

- *Virtual-Circuit Identifier*
- The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI. Note that a VCI does not need to be a large number since each switch can use its own unique set of VCIs.

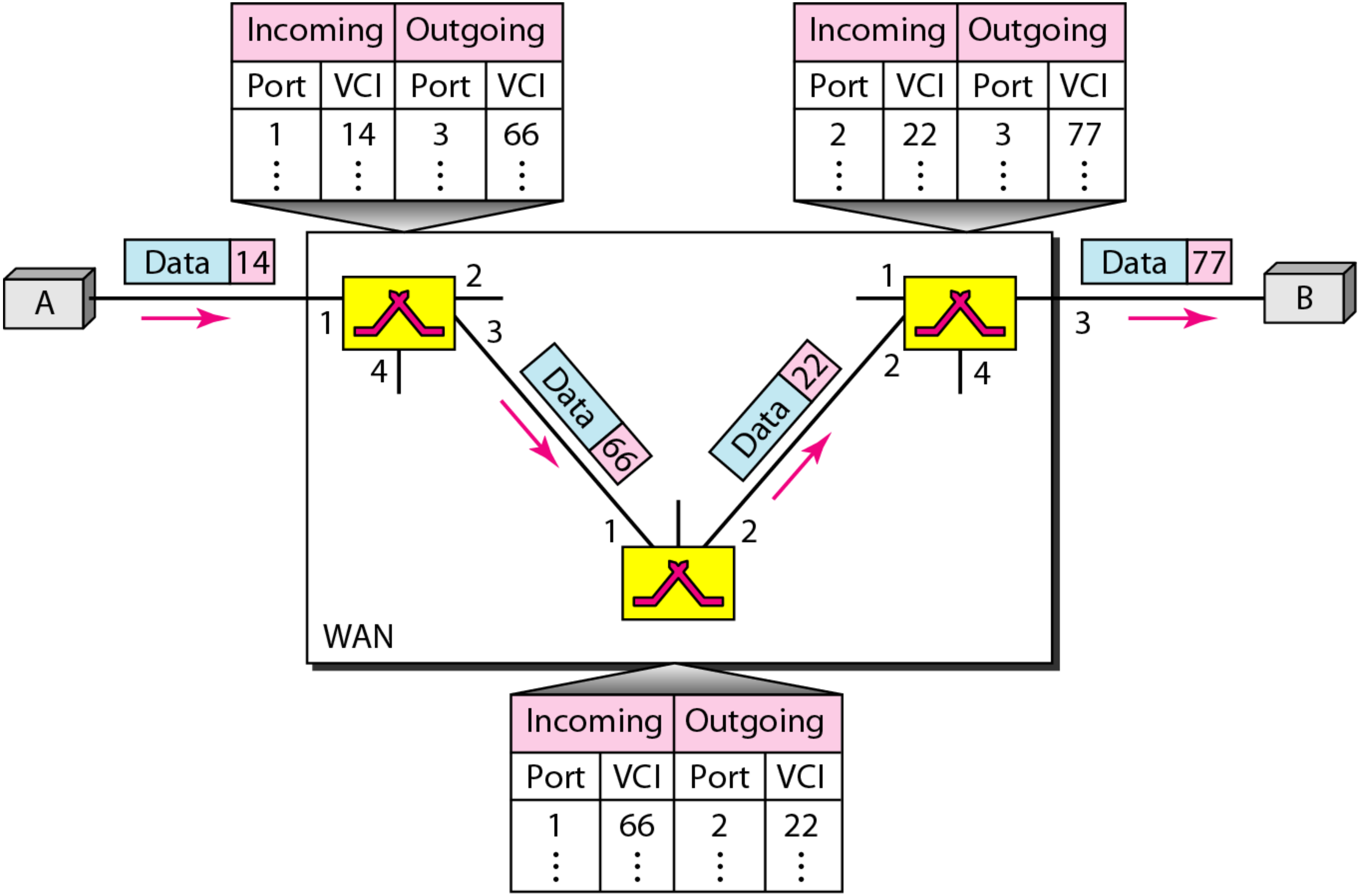


Switch and tables in a virtual-circuit network



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	22
1	77	2	41

Source-to-destination data transfer in a virtual-circuit network



Incoming		Outgoing	
Port	VCI	Port	VCI
1 ⋮	14 ⋮	3 ⋮	66 ⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
2 ⋮	22 ⋮	3 ⋮	77 ⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
1 ⋮	66 ⋮	2 ⋮	22 ⋮

WAN Hardware Devices

- **Router** - An electronic device that connects a local area network (LAN) to a wide area network (WAN) and handles the task of routing messages between the two networks. Operates at layer 3, and makes decisions using IP addresses.
- **Switch** (layer 3 switch) - A switch is a network device that selects a path or circuit for sending a unit of data to its next destination. Operates at layer 2 (and 3), and uses MAC addresses/IP Addresses to send data to correct destination. (LAN switches are not this type)
- **Modem** - Short for modulator/demodulator, a modem enables a computer to communicate with other computers over telephone lines. Operates at layer 1, where signals are converted from digital to analogue and vice versa for transmission and receiving.

Routing Technologies

- **Routing**
- Routing is one of the fundamental aspects of networking. The ability of routers to learn possible routes (rather than make you manually configure and constantly update the routes) is one of the primary reasons that ARPANET which originally connected seven sites, scaled into the modern Internet in only a few short years.
- Routed networks are often large and complex, and it would be prohibitively difficult to manage and update network information on all routers all the time. Several algorithms have been developed to help address these difficulties. These algorithms allow the routers to learn about the network and then make decisions based on that information.
- To learn paths (or routes) through a network, and make decisions on where to send packets, a router use
  - **Destination address** - Typically the Internet Protocol (IP) address of the data's (packet) destination.
  - **Source address** - Where the information came from (typically an IP address).
  - **Possible routes** - Routes that can get information from its present location or source to some other location (the destination or closest known point).
  - **Best route** - The best path to the intended destination. ("Best" can mean many things.)
  - **Status of routes** - The current state of routes, which routers track to ensure timely delivery of information.

What Exactly Does "Best" Mean?

- Routers often make decisions about the best possible path to get information from a source to a destination. "Best," however, is loosely defined, and it depends on what is valued by the network. These measurements of value are referred to as metrics. Which metrics are valued by the network is determined by the network administrator. Several metrics are listed here:
  - **Hop count** - Number of times a packet goes through a router.
  - **Delay time** - Time required to reach the destination.
  - **Reliability** - Bit-error rate of each network link.
  - **Maximum transmission unit (MTU)** - Maximum message length (or packet size) allowed on the path.
  - **Cost** - Arbitrary value based on a network- administrator‘ determined value. Usually some combination of other metrics.

Static Versus Dynamic

- Routers must learn about the network around them to make determinations on where to send packets. This information can either be manually entered (static routes) or learned from other routers in the network (dynamic routes):
- **Static routes** - When a network administrator manually enters information about a route, it is considered a static route. Only a network administrator can change this information. (That is, the router does not learn from, or update, its routing tables based on network events.) Static routes allow for tight control of packets but are difficult to maintain and prone to human error.
- **Dynamic routes** - Routers on a network can learn about possible routes and current route status from other routers in the network. Routes learned in this way are called dynamic routes. Routers in dynamic routes learn about changes in the network without administrative intervention and automatically propagate them throughout the network.

Flat Versus Hierarchical Routing

- With flat networks, all routers must keep track of all other routers on the network. As networks grow, the amount of information contained in the routing tables increases.
- Although this method is simple, it can result in poor network performance because the number of routing updates traffic grows with each new router.
- Hierarchical networks segment routers into logical groupings. This arrangement simplifies routing tables and greatly reduces overhead traffic.

Distance-Vector Versus Link-State Routing

- The two main classes of routing are distant vector routing and link-state routing. With distance-vector routing, routers share their routing table information with each other. Also referred to as "routing by rumor," each router provides and receives updates from its direct neighbor.
- The only information a router knows about a remote network is the distance or metric to reach that network and which path or interface to use to get there
- A distance vector describes the direction (port) and the distance (number of hops or other metric) to some other router. When a router receives information from another router, it increments whatever metric it is using. This process is called distance accumulation.
- Routers using this method know the distance between any two points in the network, but they do not know the exact topology of an internetwork.

…

- Network discovery is the process of learning about indirectly connected routers. During network discovery, routers accumulate metrics and learn the best paths to various destinations in the network.
- With link-state routing, also known as shortest path first (SPF), each router maintains a database of topology information for the entire network. Link-state routing provides better scaling than distance-vector routing because it only sends updates when there is a change in the network, and then it only sends information specific to the change that occurred.
- A router configured with a link-state routing protocol can create a "complete view" or topology of the network by gathering information from all of the other routers.
- Distance vector uses regular updates and sends the whole routing table every time. Link-state routing also uses a hierarchical model, limiting the scope of route changes that occur.

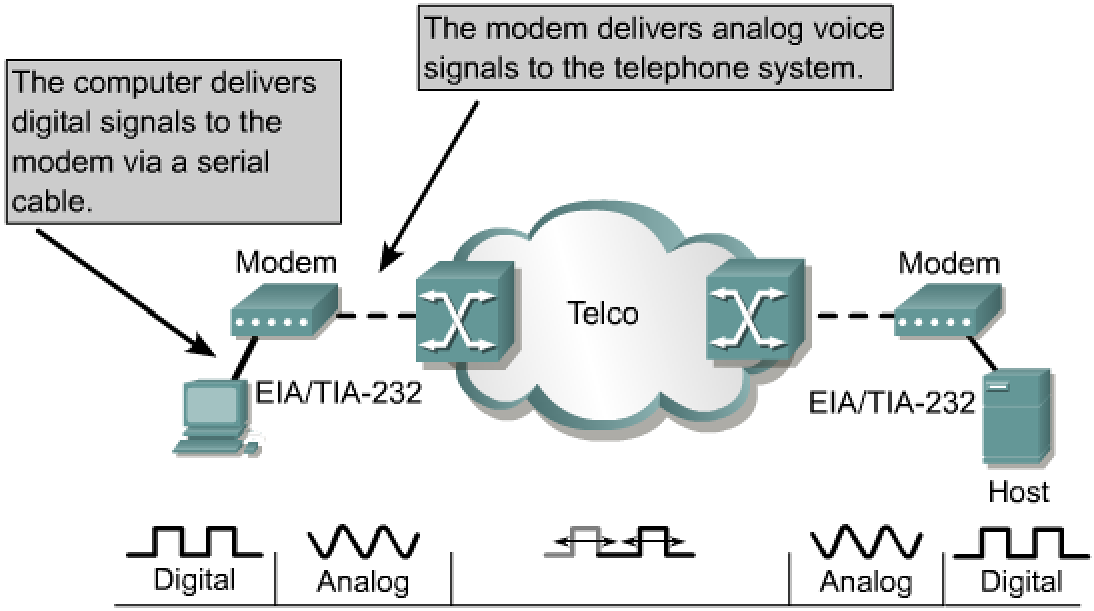
WAN Technology Options

- Dial-up
- Leased Line
- ISDN
- DSL
- X.25 technology
- Frame relay and virtual circuit
- ATM Technology
- Cable Modem
- Microwave Point-to-Point Link
- VSAT

Dial-up

- Uses POTS (Plain Old Telephone System)
- Provides a low cost need based access.
- Bandwidth 33.6 /56 Kbps.
- On the Customer End: Modem is connected to a Telephone Line
- On the Service Provider End: Remote Access Server (RAS) is connected to Telephone Lines (33.6 Kbps connectivity) or E1/R2 Line (56 Kbps connectivity)
- RAS provide dial in connectivity, authentication and metering.
- Achievable bandwidth depends on the line quality.

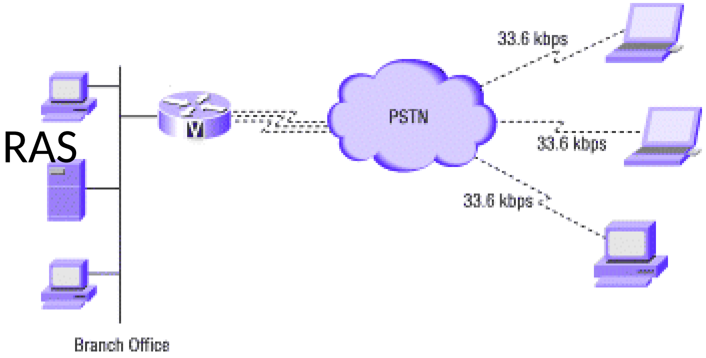
Dial-up



The computer delivers digital signals to the modem via a serial cable.

The modem delivers analog voice signals to the telephone system.

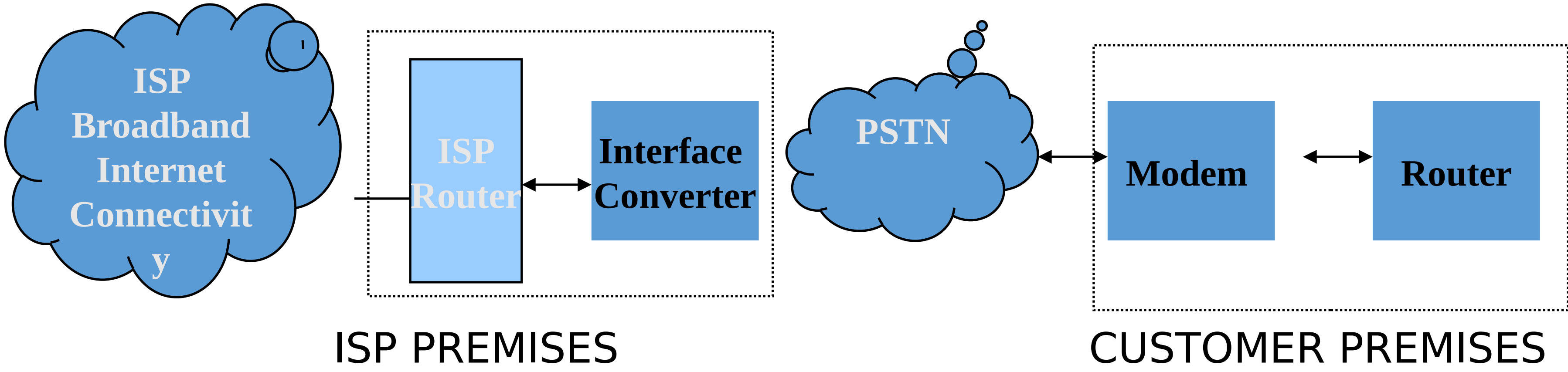
Dial-up



Leased Line

- Used to provide point-to-point dedicated network connectivity.
- Each side of the line permanently connected to the other, unlike dial-up connections, a leased line is always active.
- Connecting two locations in exchange for a monthly rent, the fee for the connection is a fixed monthly rate.
- Typically, leased lines are used by businesses to connect geographically distant offices
- Analog leased line can provide maximum bandwidth of 9.6 Kbps.
- Digital leased lines can provide bandwidths : 64 Kbps, 2 Mbps (E1), 8 Mbps (E2), 34 Mbps (E3) ...

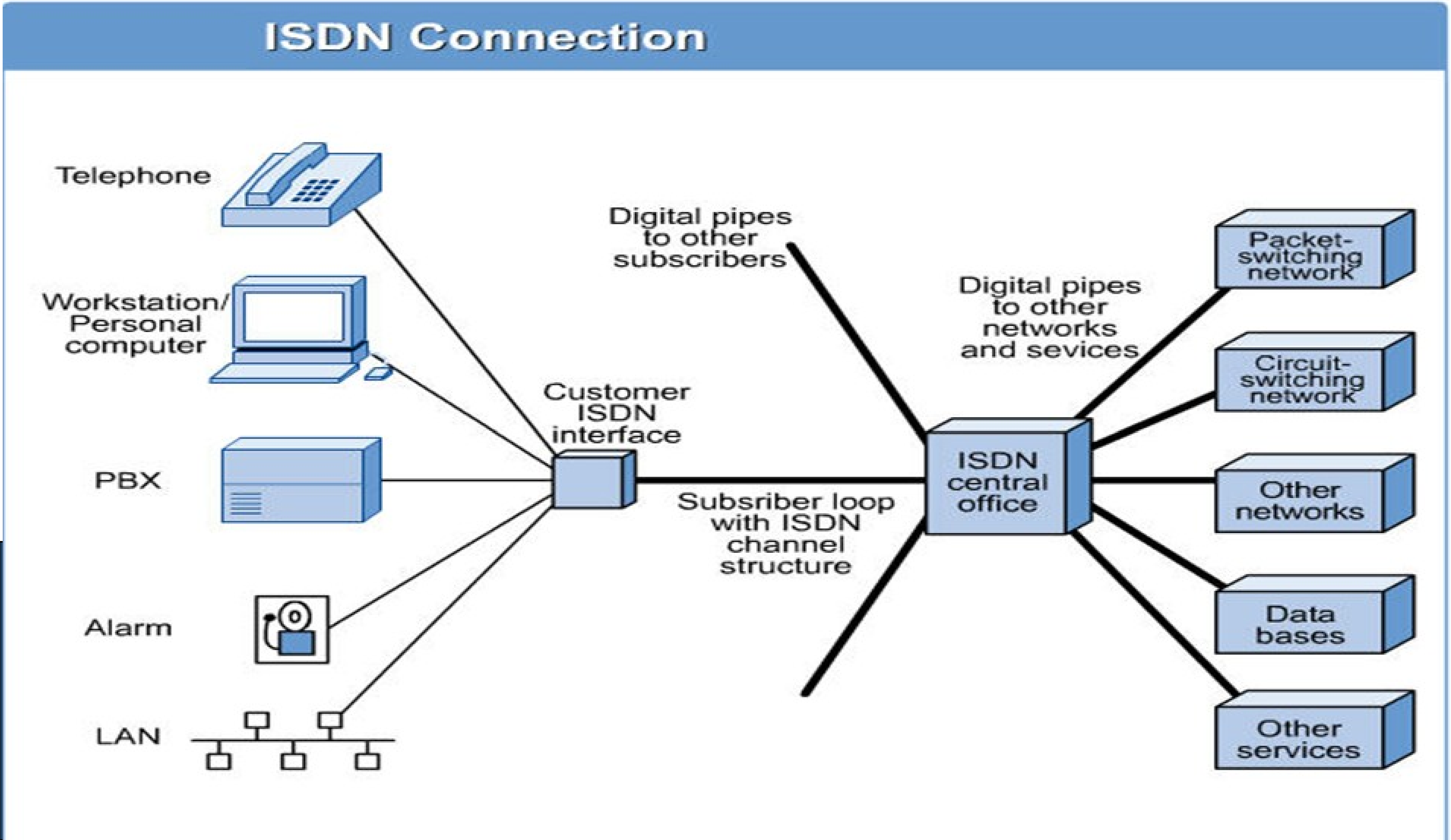
Leased Line Internet Connectivity



ISDN (Integrated Service Digital Network)

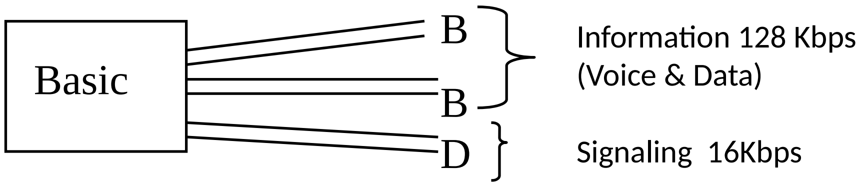
- Another alternative to using analog telephones lines to establish a connection is ISDN.
- It is s a set of communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
- Speed is one advantage ISDN has over telephone line connections.
- ISDN network is a switched digital network consisting of ISDN Switches.
- ISDN user accesses network through a set of standard interfaces provided by ISDN User Interfaces.

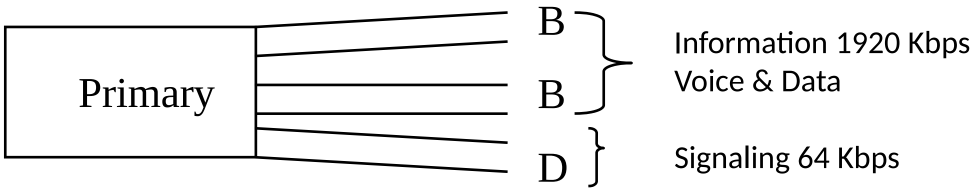
ISDN Connection


ISDN Connection
Telephone
Workstation/ Personal computer
PBX
Alarm
LAN
Customer ISDN interface
Digital pipes to other subscribers
Subsriber loop with ISDN channel structure
ISDN central office
Digital pipes to other networks and sevices
Packet-switching network
Circuit-switching network
Other networks
Data bases
Other services

ISDN

- Two types of user access are defined
  - **Basic Access** - Consists of two 64Kbps user channels (B channel) and one 16Kbps signal channel (timing and alarm channel) (D channel) providing service at 144 Kbps.
  - **Primary access** - Consists of thirty 64Kbps user channels (B channels) and a 64 Kbps signal channel (timing and alarm channel) (D channel) providing service at 2.048Mbps (One 64 Kbps channel is used for Framing and Synchronization).





Digital Subscriber Line (DSL)

- Digital Subscriber Line (DSL) uses the Ordinary Telephone line and is an always-on technology. This means there is no need to dial up each time to connect to the Internet.
- Because DSL is highly dependent upon noise levels, a subscriber cannot be any more than 5.5 kilometers (2-3 miles) from the DSL Exchange
- Service can be symmetric, in which downstream and upstream speeds are identical, or asymmetric in which downstream speed is faster than upstream speed.
- DSL comes in several varieties:
  - Asymmetric DSL (ADSL)
  - High Data Rate DSL (HDSL)
  - Symmetric DSL (SDSL)
  - Very High Data Rate DSL (VDSL)

DSL Modem

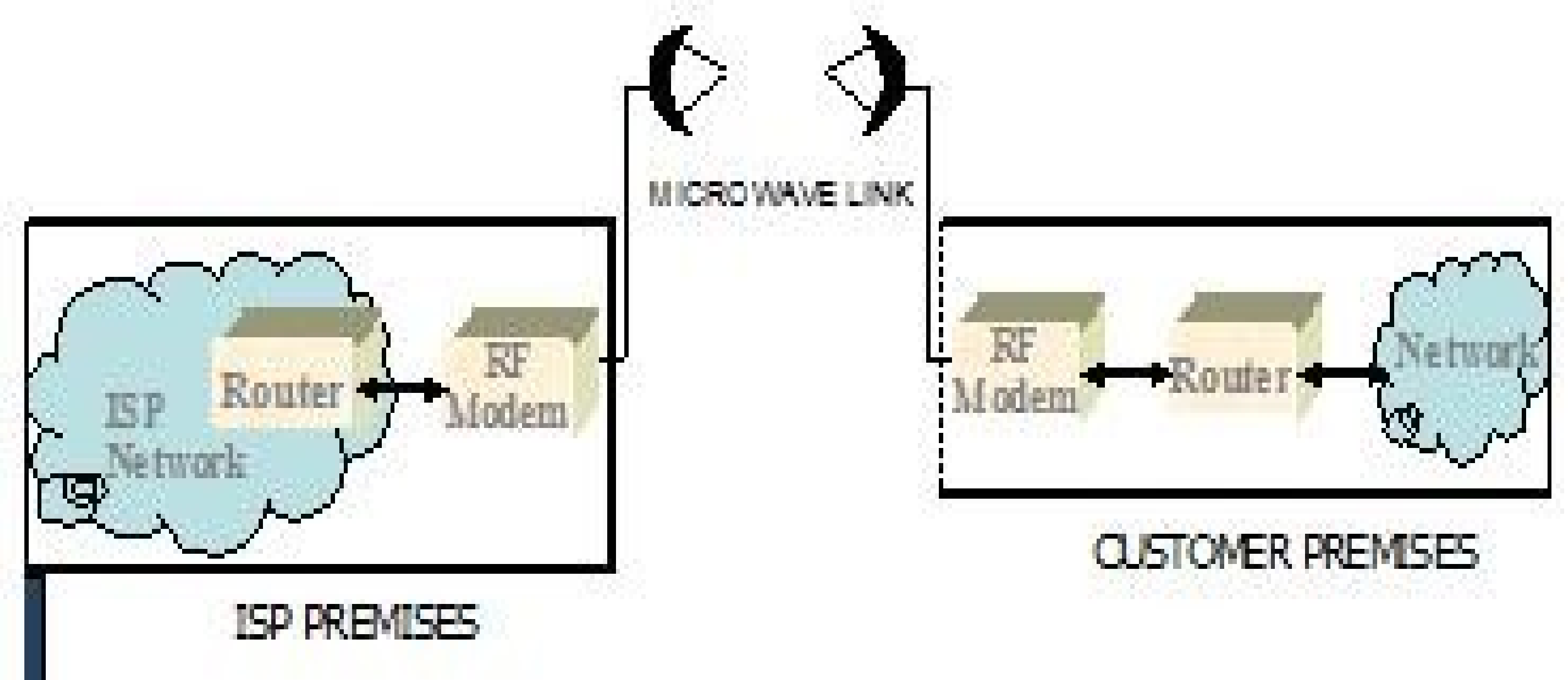
Cable Modems

- **The cable modem connects a computer to the cable company network through the same coaxial cabling that feeds cable TV (CATV) signals to a television set.**
- **Uses Cable Modem at Home End and CMTS (Cable Modem Termination System) at Head End.**
- **Characteristics:**
  - Shared bandwidth technology
  - 10 Mbps to 30 Mbps downstream
  - 128Kbps-3 Mbps upstream
  - Maximum Distance from provider to customer site: 30 miles

- **Cable modems are primarily used to deliver broadband Internet access in the form of cable Internet, taking advantage of the high bandwidth of a cable television network**

Point-to-Point Microwave Link

- Typically 80-100 MHz Band or 5 GHz Radio Link band
- 2.4 GHz WiFi links are becoming popular
- Requires Line of Sight



VSAT

- Very Small Aperture Terminal (VSAT) provide communication between two nodes through a powerful Earth station called a Hub.
- If two terminals want to communicate, they send their messages to the satellite, which sends it to the Hub and the Hub then broadcasts the message through the satellite.
- Typical Bandwidth offered is 9.6/19.2/32/64/128/256/512 Kbps.

VSAT

- **Each satellite sends and receives over two bands**
  - Uplink: From the earth to the satellite
  - Downlink: From the satellite to the earth
- **Satellite frequency bands**

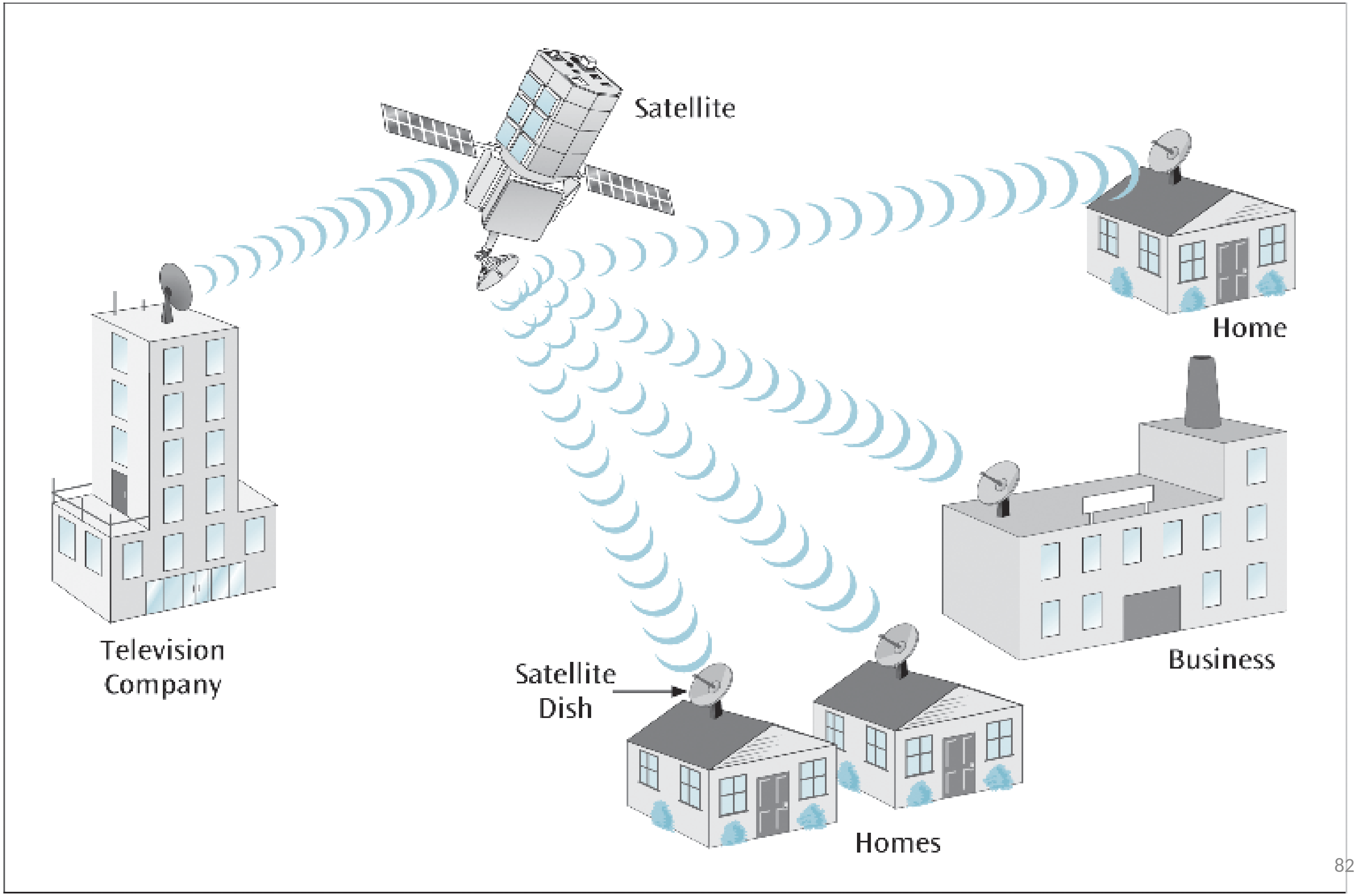
Band	*Downlink*	*Uplink*
C	3.7-4.2 GHz	5.925-6.425 GHz
Ku	11.7-12.2 GHz	14-14.5 GHz

- **Ku-band based networks, are used primarily in Europe and North America and utilize the smaller sizes of VSAT antennas.**
- **C-band, used extensively in Asia, Africa and Latin America, require larger antenna.**

VSAT

- **VSATs are most commonly used to transmit narrowband data (point of sale transactions such as credit card, polling or RFID data), or broadband data (for the provision of Satellite Internet access to remote locations, VoIP or video).**
- **VSATs are also used for transportable, on-the-move (utilising phased array antennas) or mobile maritime communications.**

VSAT


Satellite
Home
Business
Television Company
Satellite Dish
Homes

Reading Assignment

Read about the following WAN Technology options and prepare your own note

- X.25 technology
- Frame relay and virtual circuit
- ATM Technology