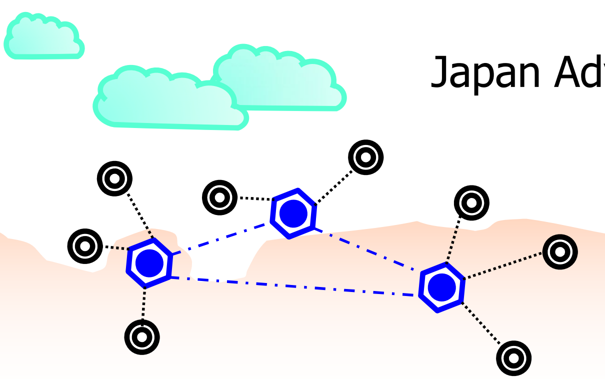
I226
Computer Networks

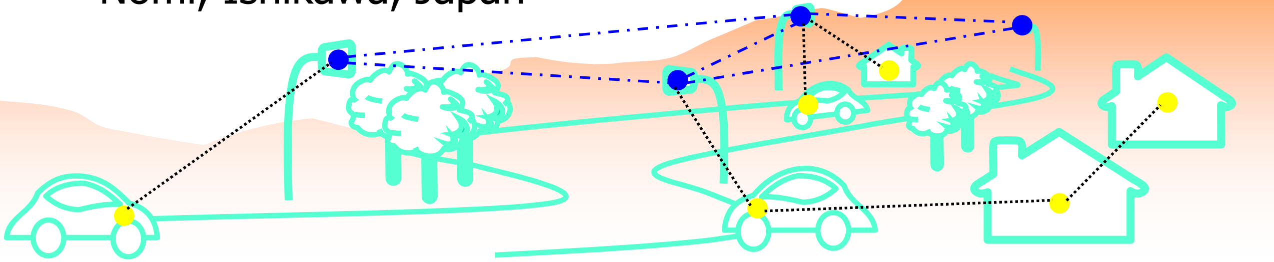
Chapter 5

Network Layer II

Assoc. Prof. Yuto Lim

School of Information Science
Japan Advanced Institute of Science and Technology
Nomi, Ishikawa, Japan





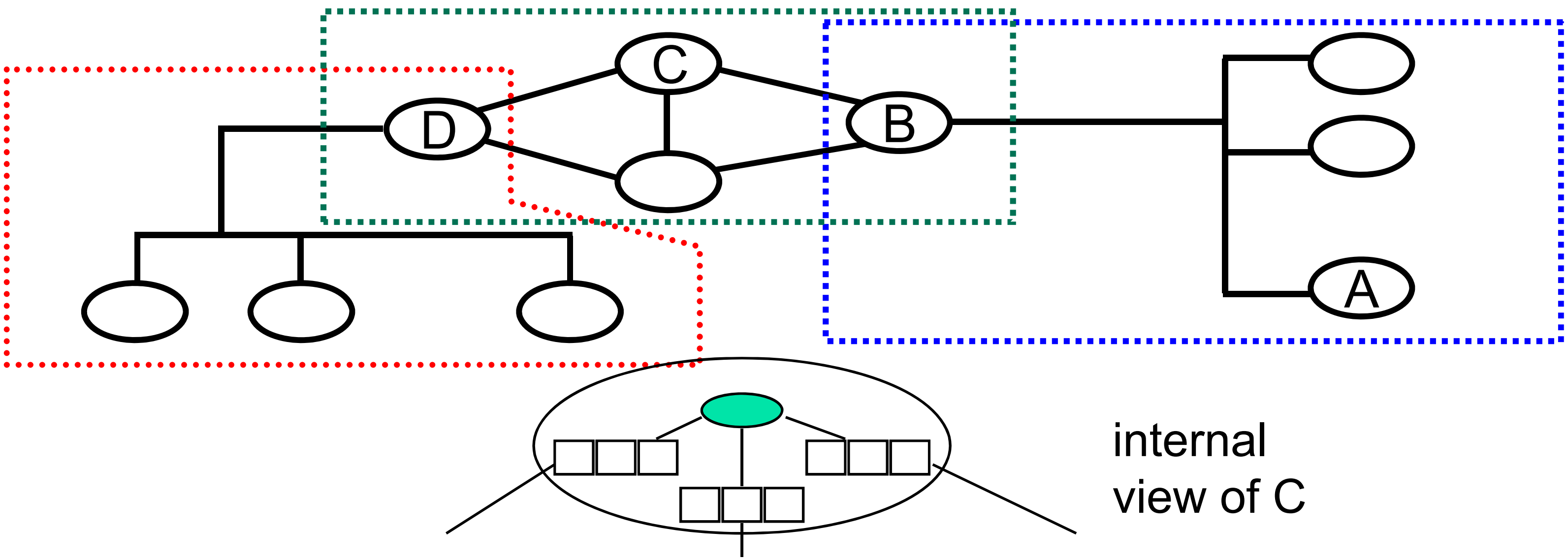
Objectives of this Chapter

- Provide an understanding what are the internetworking devices available for creating a network
- Offer the knowledge of spanning tree algorithm and its operation
- Explain the difference between the bridge and the router
- Give the difference between the router and the switch
- Give an explanation of LAN and its details

Outline

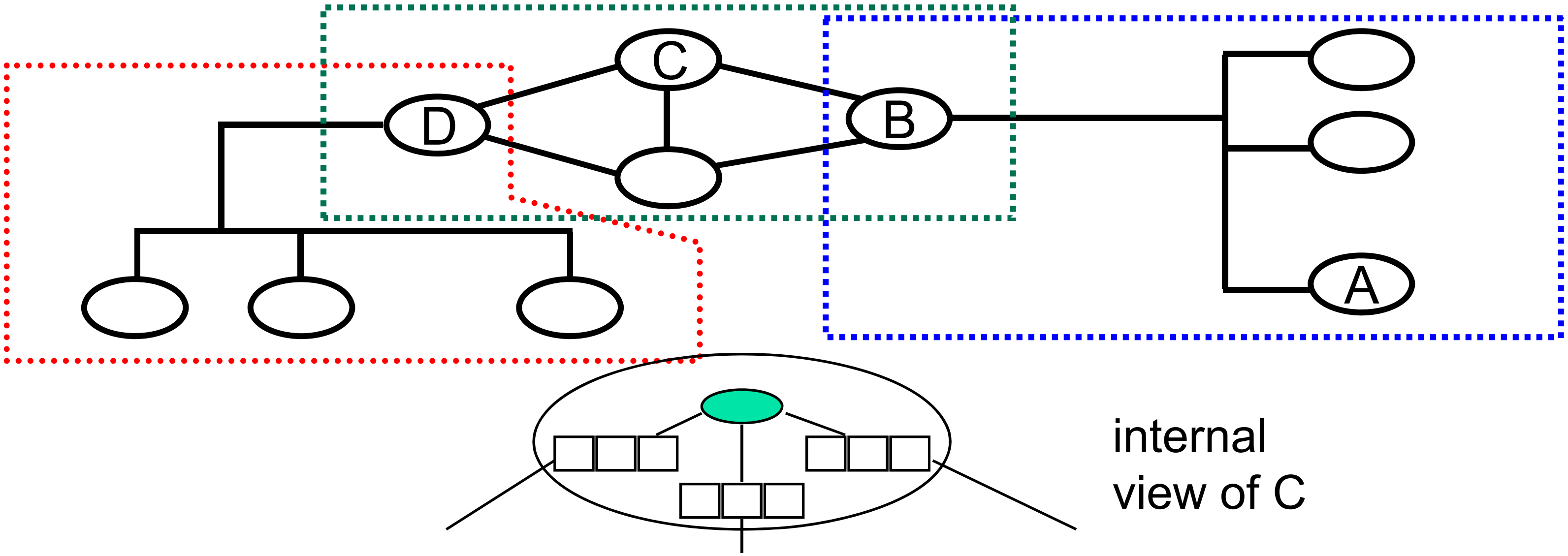
- Elements of a Network
- Networking Devices
  - Repeater
  - Bridge
- Internetworking Devices
  - Router
  - Gateway
- Local Area Network Examples
  - Ethernet LAN

Elements of a Network



- 3 networks forming an internetwork
  - Communication links
  - Buffers – to hold packets when contention for communications link
  - Network – set of nodes (hosts, routers, gateways) within a single administrative domain (department, company)

Elements of a Network (cont.)



- Internetwork: a collection of interconnected networks
- Active network elements: hardware running protocols
  - Host – hardware running applications which use network (e.g., A)
  - Router – hardware (often without application level functions) routing packets from input line to output line (e.g., C)
  - Gateway – a router connected directly to two or more networks (e.g., B and D)

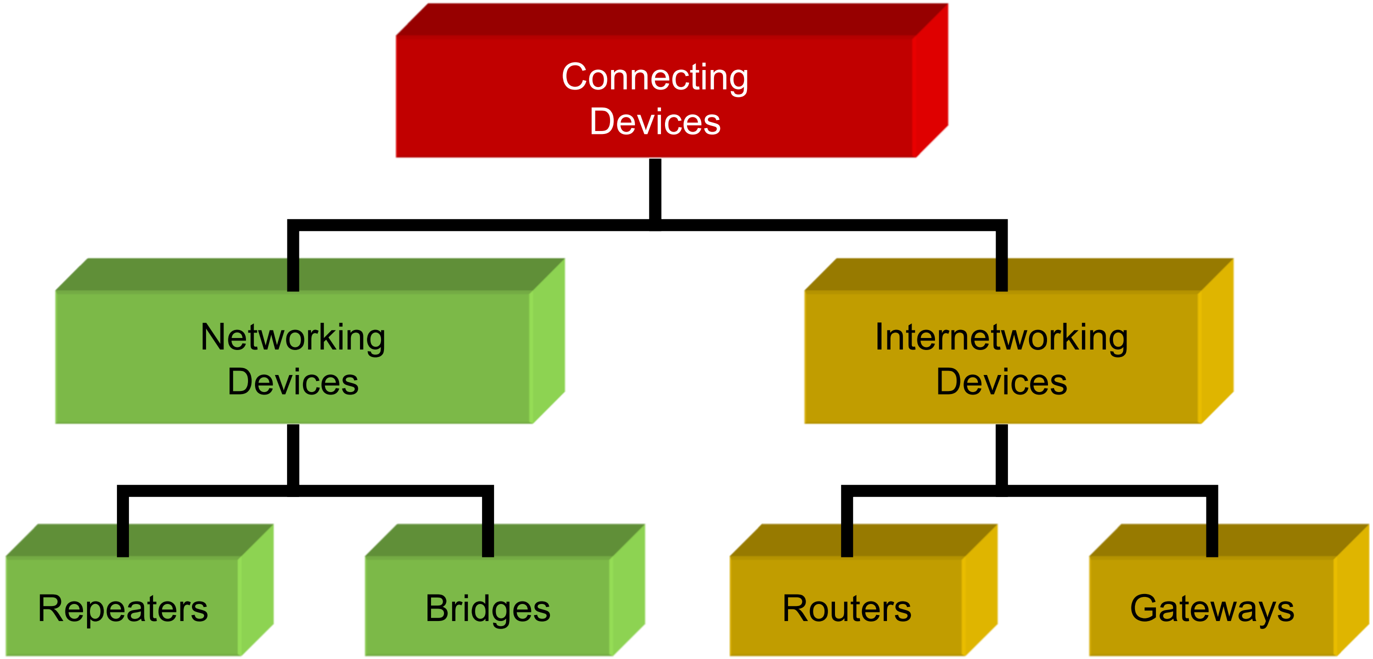
What are Connecting Devices?

- Connecting devices are products used to unite and separate networks, consist of
  - Networking devices
  - Internetworking devices

- As computer networks grow in size and complexity, both the networking and internetworking devices that used to connect them also grow

- Purposes of connecting devices
  - Allow a greater number of nodes to be connected to the network
  - Extend the distance over which a network can extend
  - Localize traffic on the network
  - Merge existing networks
  - Isolate network problems so that internetworking device can be diagnosed more easily

Connecting Devices



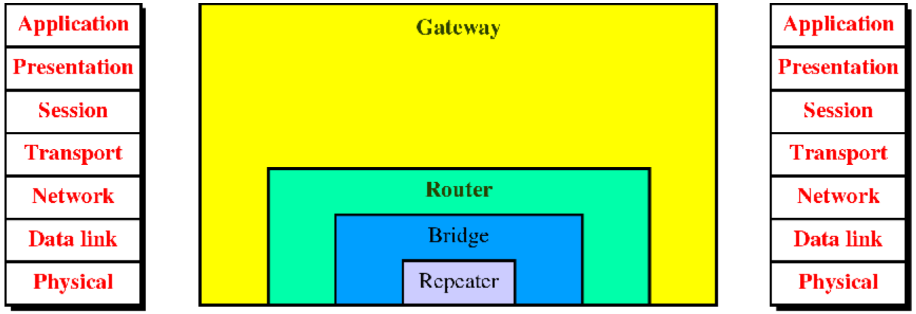
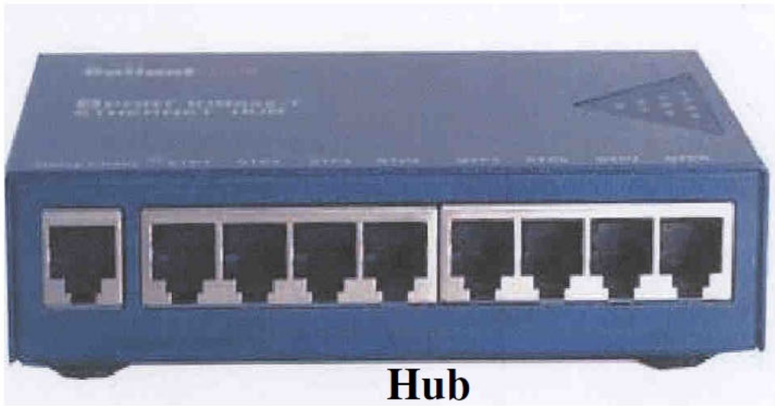
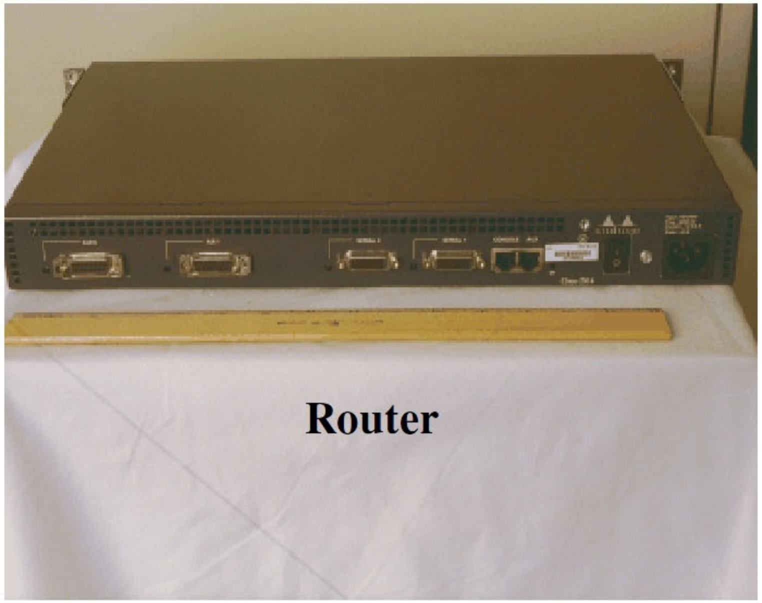


Figure: Connecting devices and the OSI model

Example

Switch

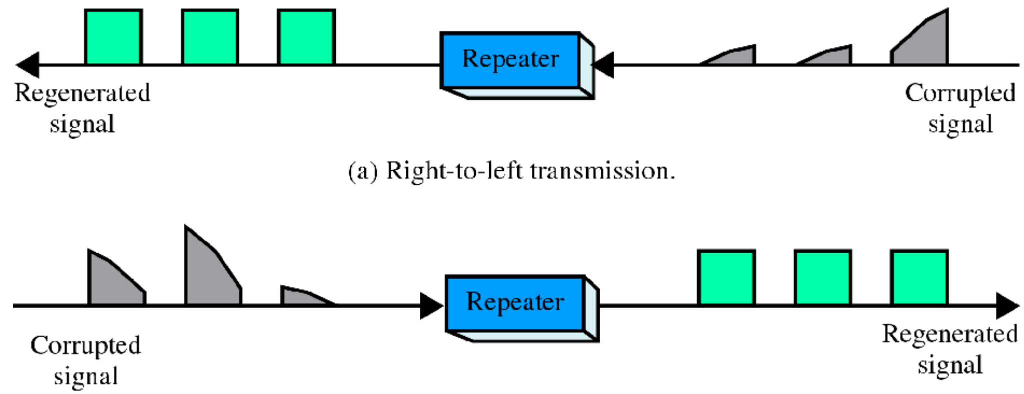

Hub


Router

Bridge

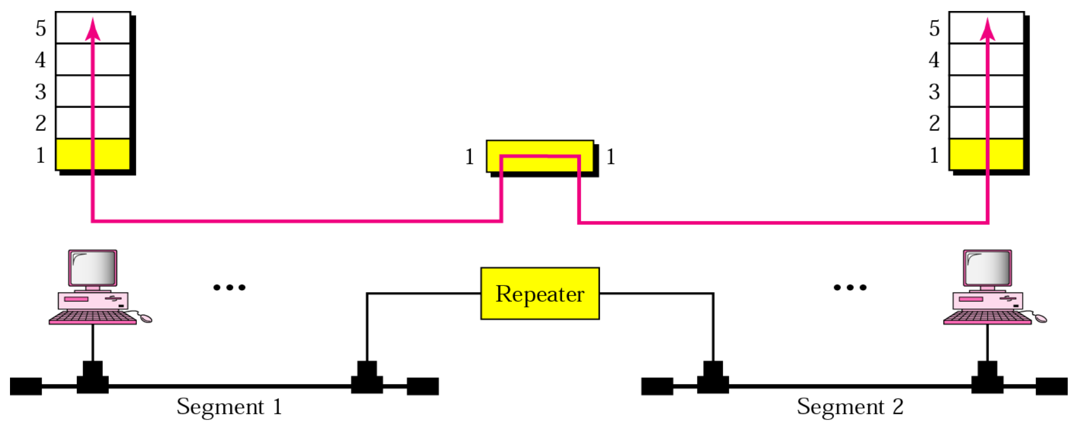
Repeater

- Repeater (regenerator, not an amplifier) is an electronic device that operates on only the physical layer of the OSI model
  - Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data
- It extends the physical length of a network
- No network function has been changed
- Location is matter



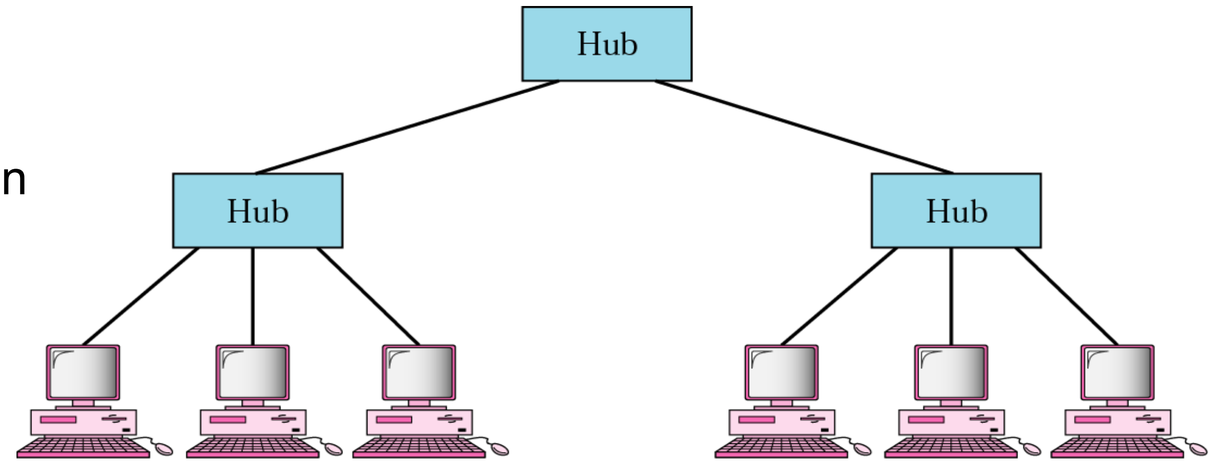
(a) Right-to-left transmission.

(b) Left-to-right transmission.



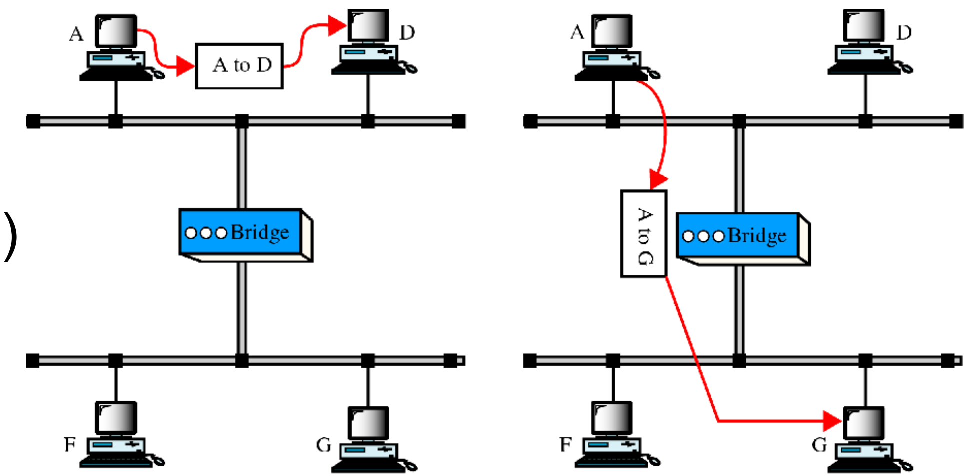
Hub

- Hub that is very common networking device actually is a multiport repeater
- The term hub is used instead of repeater when referring to the device that serves as the center of a star topology network
- Hubs do not isolate collision domains: node may collide with any node residing at any segment in LAN
- Advantages
  - Simple
  - Inexpensive device
  - Multi-tier provides graceful degradation
  - Extends maximum distance between node pairs (100 m per Hub)

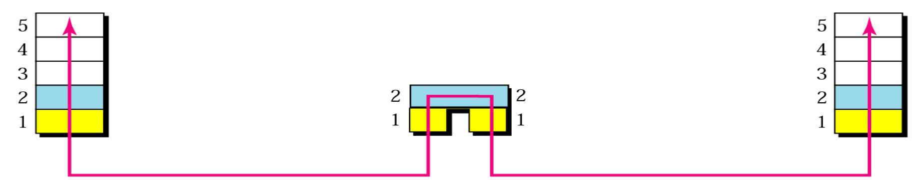


Bridge

- Divide a large network into smaller segment
- Isolating and controlling the link problems (e.g., congestion)
- Regenerate signal + Checking Physical Address and forward only to the specified segment
- Advantages
  - Isolates collision domains resulting in higher total max throughput, and does not limit the no. of nodes nor geographical coverage
  - Can connect different type Ethernet since it is a store and forward device
  - Transparent: no need for any change to hosts LAN adapters

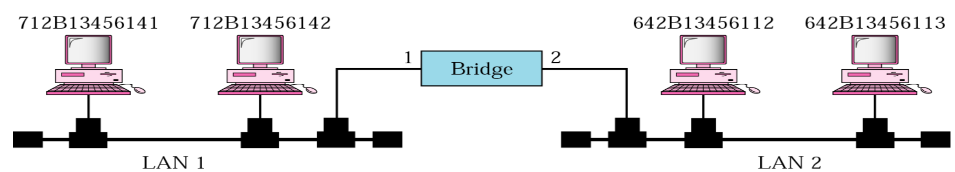


a. A packet from A to D
b. A packet from A to G

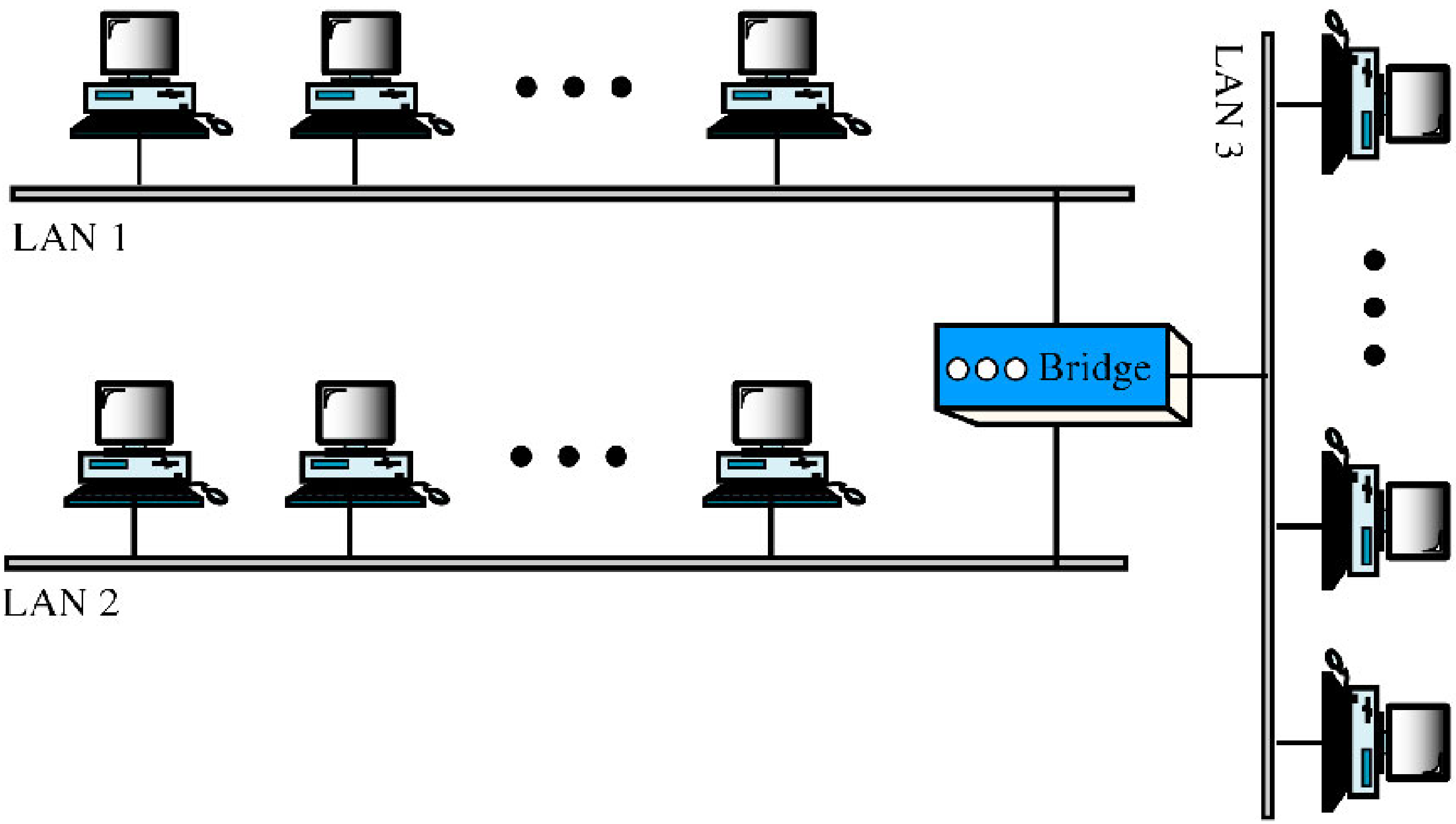


Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

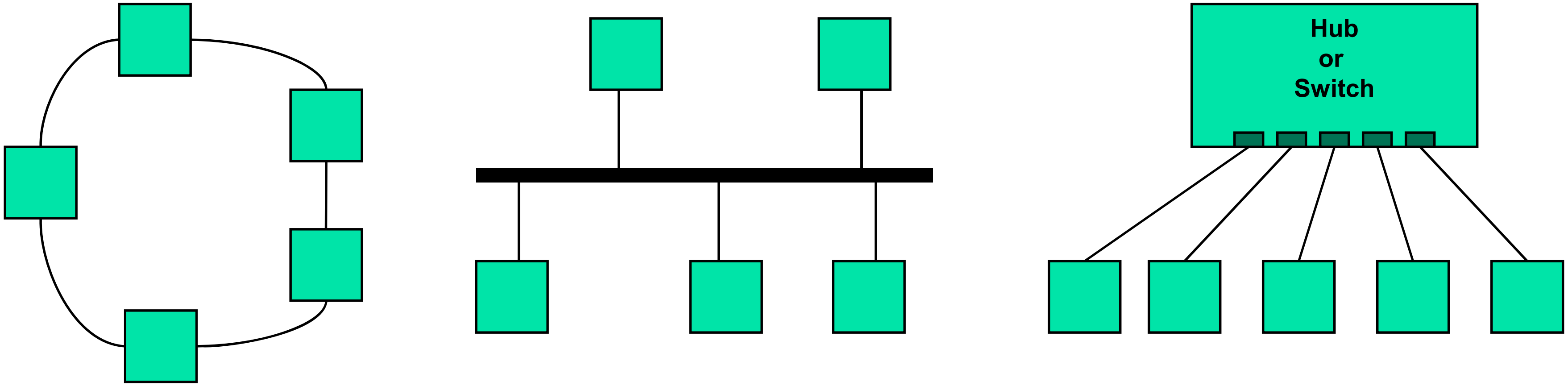
Bridge Table



Multiport Bridge



Networks Without Bridges

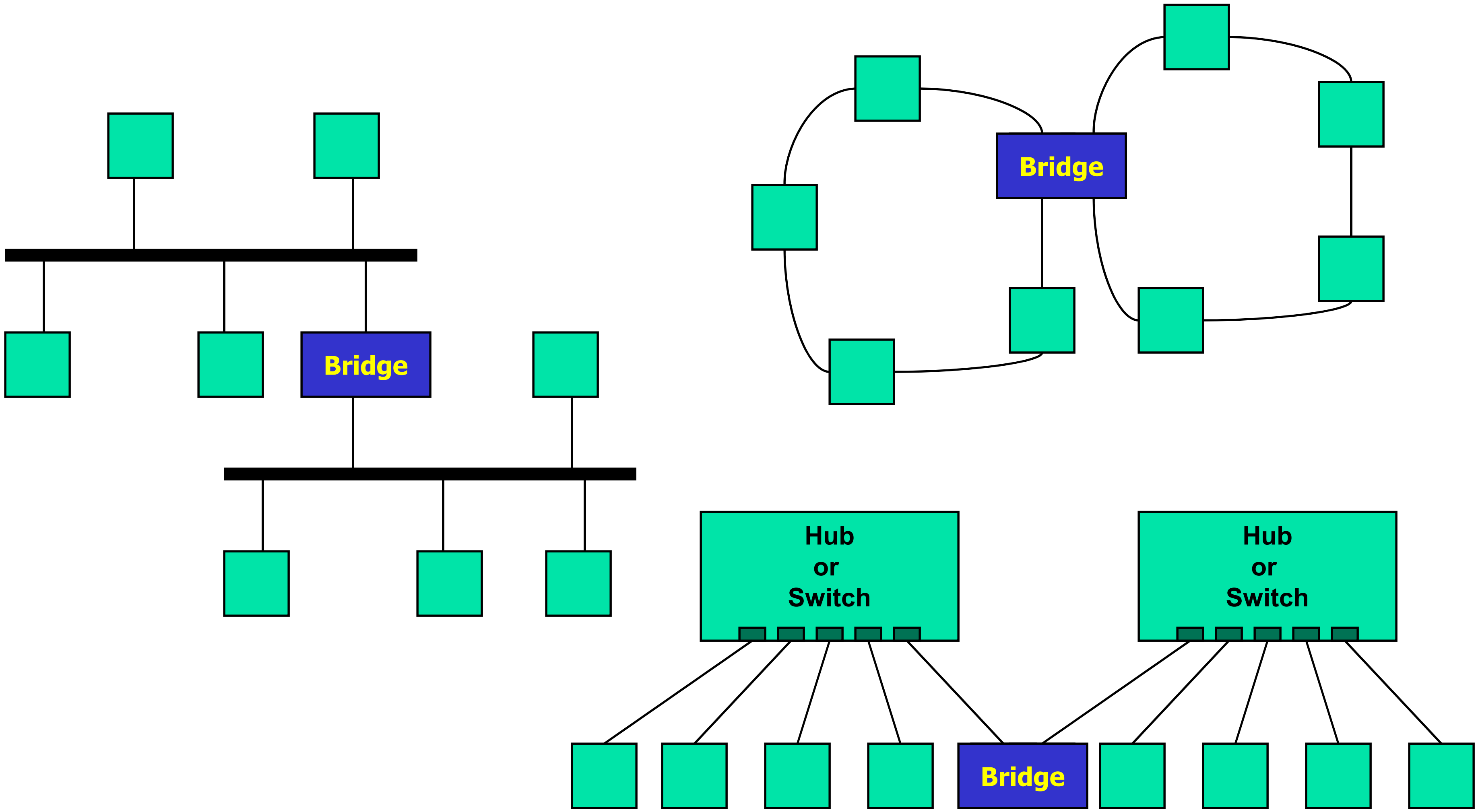


Token Ring
FDDI

Ethernet
(10Base5, 10Base2)

Ethernet
(10BaseT, 100BaseTX)
FDDI
CDDI

Networks With Bridges



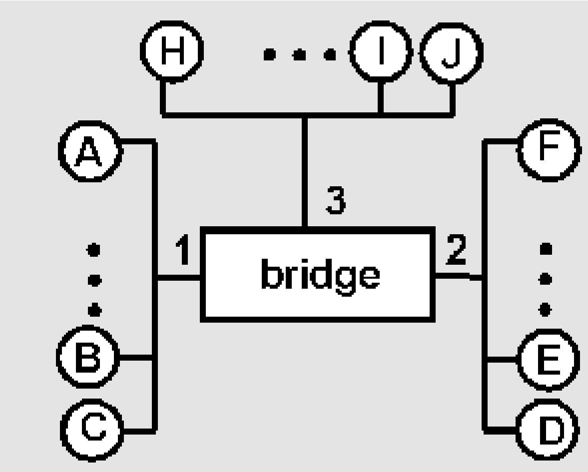
Bridge: Forwarding, Frame Filtering

- Forwarding
  - How to know on which LAN segment to forward frame?
- Bridge filters frames
  - Same-LAN-segment frames not forwarded onto other LAN segments
- Bridge learns which hosts can be reached through which interfaces: maintain filtering tables
  - When frame received, bridge "learns" location of sender: incoming LAN segment
  - Records sender location in filtering table
- Filtering table entry
  - Entry content (Node LAN Address, Bridge Interface, Time Stamp)
  - Stale entries in filtering table dropped (TTL can be 60 minutes)

Bridge Operation

```
bridge procedure(in_MAC, in_port, out_MAC)

/*learning*/
Set filtering table (in_MAC) to in_port;
lookup in filtering table (out_MAC) receive out_port;

/*no entry found for destination*/
if (out_port not valid)
/*forward on all but the interface on which the frame arrived*/
then flood;

/*destination is on LAN on which frame was received*/
if (in_port = out_port)
then drop the frame;

/*entry found for destination*/
Otherwise (out_port is valid)
then forward the frame on interface indicate;
```

Bridge Learning: Example

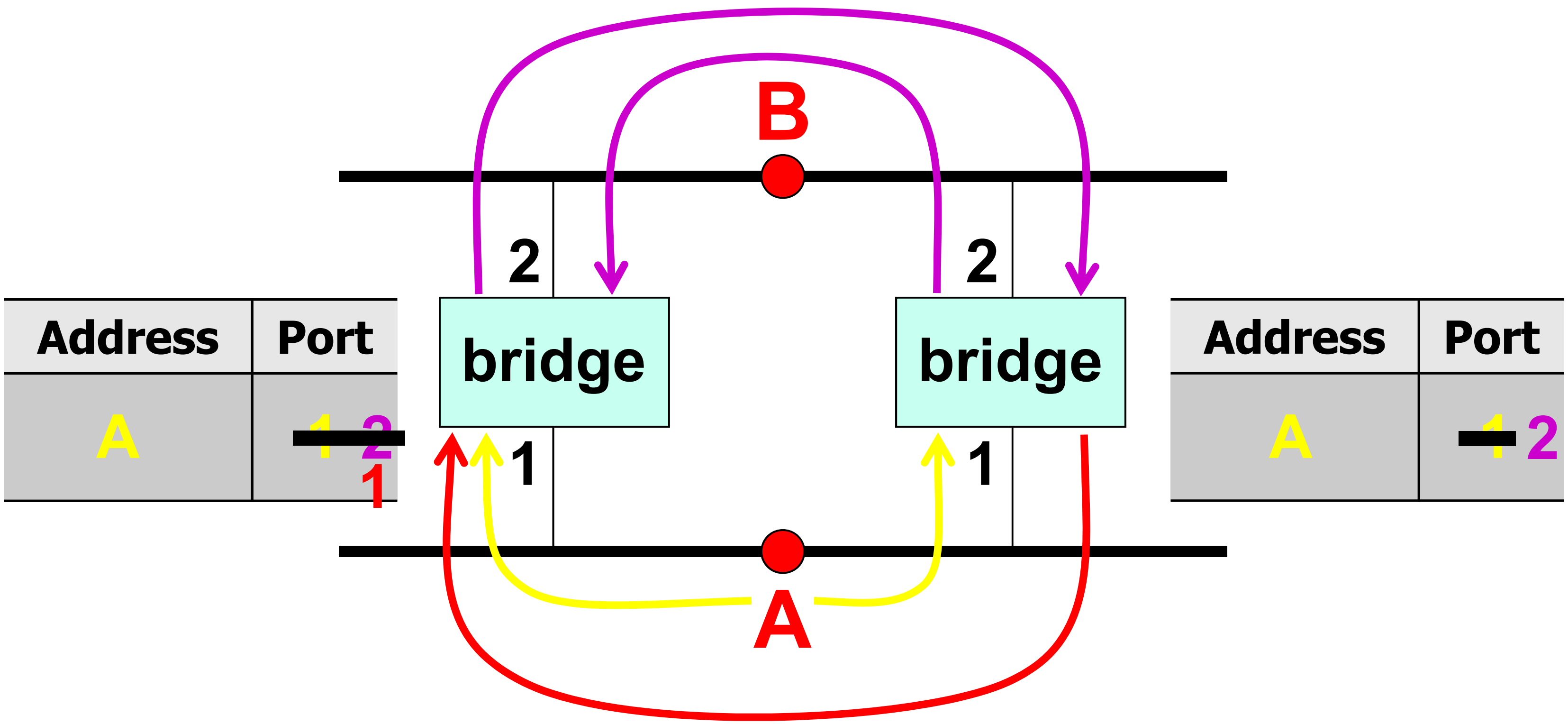


address	port
A	1
B	1
E	2
H	3
J	3

- Suppose C sends frame to D, D replies back with frame to C
- C sends frame, bridge has no info about D, so floods to both LANs
  - bridge notes that C is on port 1
  - frame ignored on upper LAN
  - frame received by D
- D generates reply to C, sends
  - bridge sees frame from D
  - bridge notes that D is on interface 2
  - bridge knows C on interface 1, so selectively forwards frame out via interface 1

Bridge: Incorrect learning

- What will happen with loops?
  - Frame looping happen ⇒ address A is keep changing



Spanning Tree Concepts

- Allow a path between every LAN without causing loops (loop-free environment)
- Bridges communicate with special configuration messages (BPDUs) and standardized by IEEE 802.1D
- Each bridge is assigned a unique identifier, a broadcast address for bridges on a LAN
- A unique port identifier for all ports on all bridges
  - MAC address
  - Bridge ID + port number
- Bridge with the lowest bridge ID value is elected root bridge
- One root bridge chosen among all bridges, every other bridge calculates a path to the root bridge

Spanning Tree Concepts (cont.)

- Path cost
  - Cost associated with each port on each bridge, default is 1
  - Cost associated with transmission onto the LAN connected to the port
  - Can be manually or automatically assigned
  - Can be used to alter the path to the root bridge

- Root port
  - Port on each bridge that is on the path towards the root bridge
  - Root port is part of the lowest cost path towards the root bridge
  - If port costs are equal on a bridge, the port with the lowest ID becomes root port

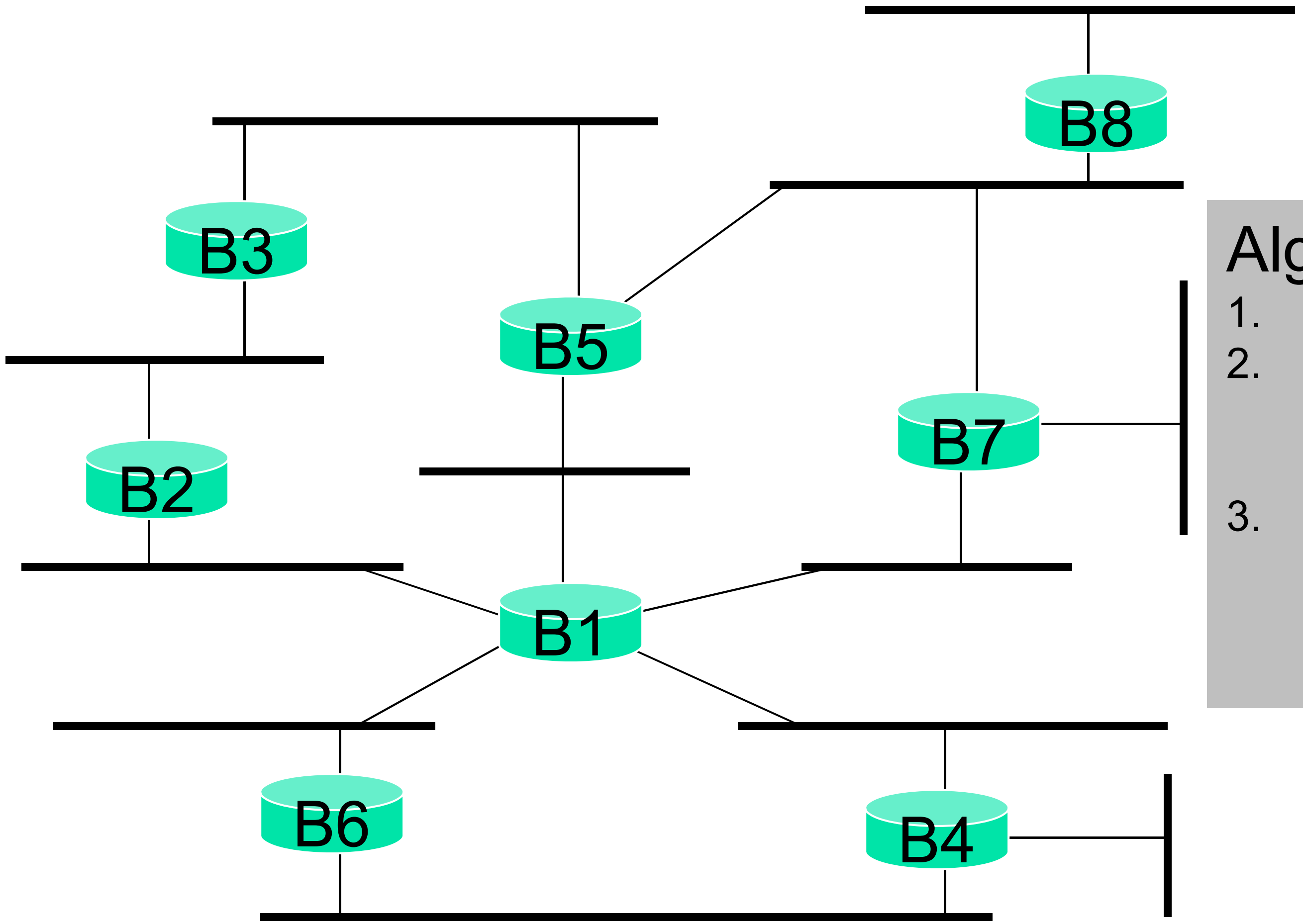
- Root path cost
  - Minimum cost path to the root bridge
  - Cost starts at the root bridge
  - Each bridge computes root path cost independently based on their view of the network

- Designated bridge
  - Only one bridge on a LAN at one time is chosen the designated bridge
  - This bridge provides the minimum cost path to the root bridge for the LAN
  - Only the designated bridge passes frames towards the root bridge

Spanning Tree Algorithm

- Step 1: Determine root bridge among all bridges
- Step 2: Each bridge determines its root port
  - Port in the direction of the root bridge
- Step 3: Determine the designated bridge on each LAN
  - Bridge which accepts frames to forward towards root bridge
  - Frames are sent on the root port of the designated bridge

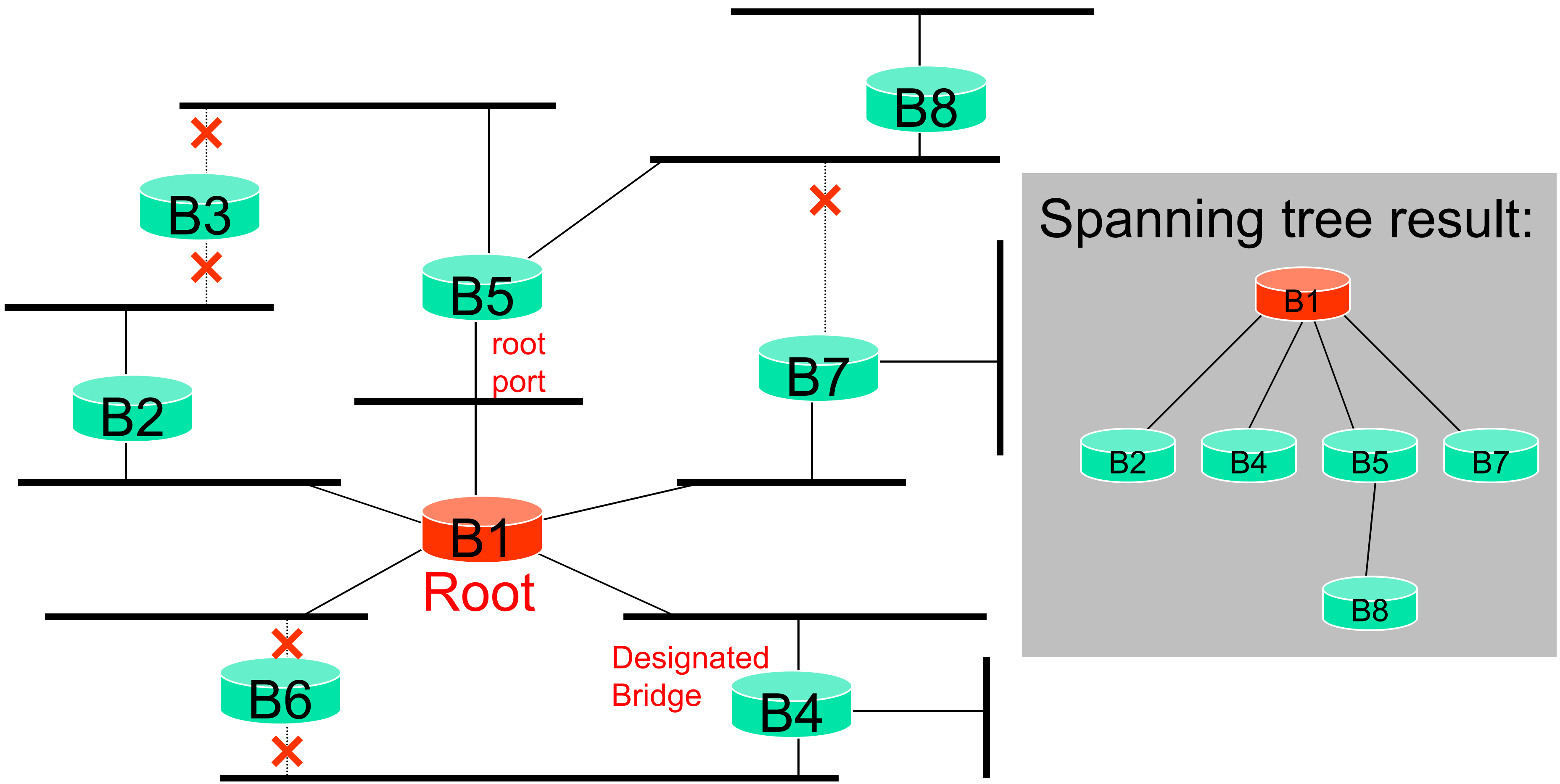
Example



Algorithm operation:

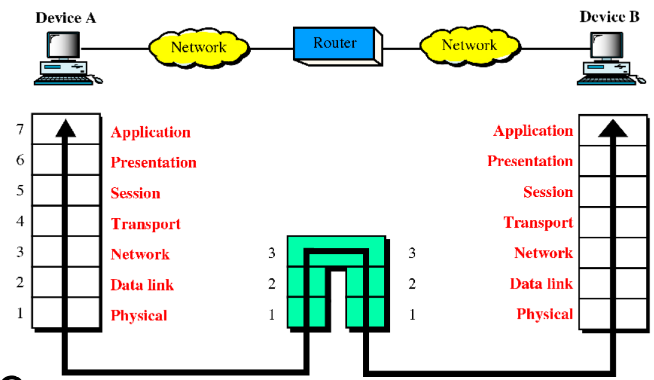
1. Picks a root
2. For each LAN, picks a designated bridge that is closest to the root
3. All bridges on a LAN send frames towards the root via the designated bridge

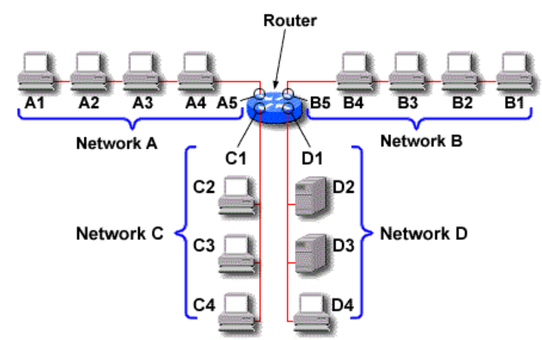
Example (cont.)

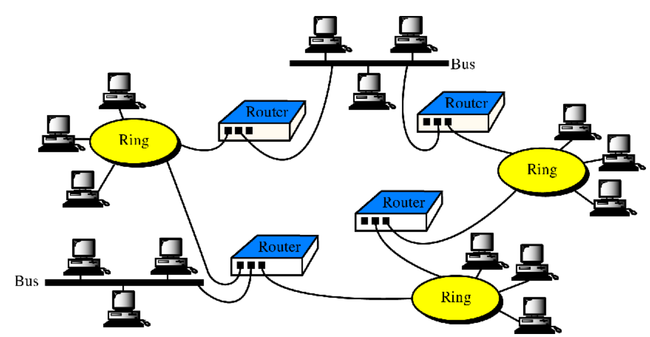


Router

- Router that acts like stations on a network connects 2 or more networks
- Definition (Goal):
  - Learning how to get from here to there
  - Process of discovering, selecting, and employing paths from one place to another (or to many others) in a network
- To perform routing, each network must have a unique network number
- Router determines to send the data from network A to network B out its port with the IP address B5

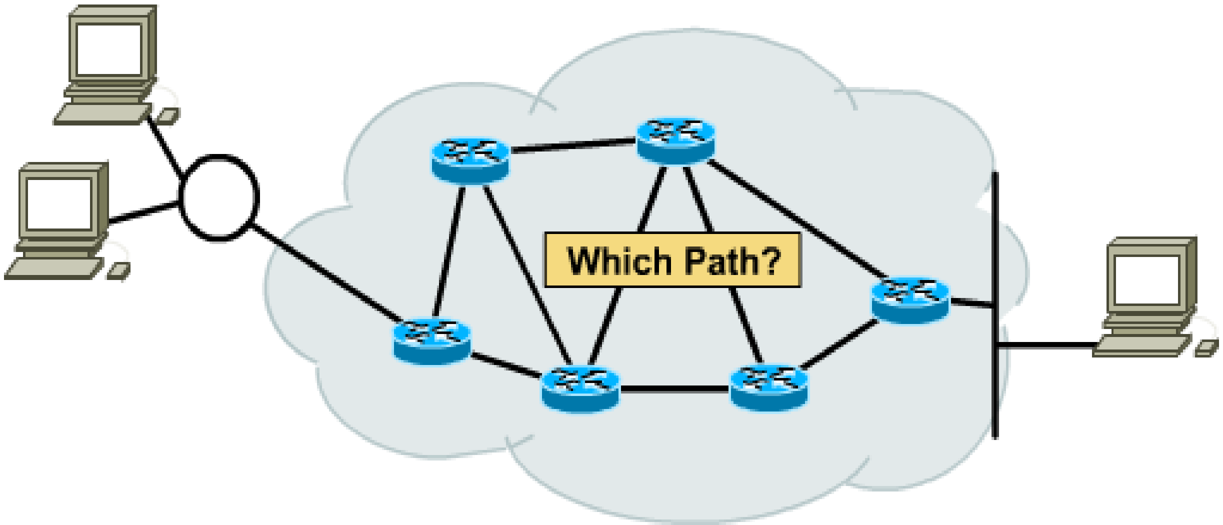






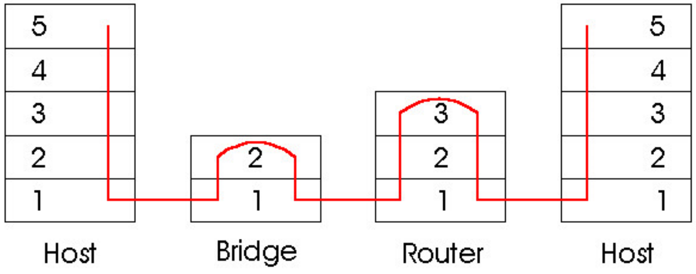
Routing Principle

- Goal: arriving at the destination
- Considerations …
  - Direct route (shortest)
  - Reliable route
  - Cheap route
  - Safe route
  - Scenic route



Bridge vs. Router

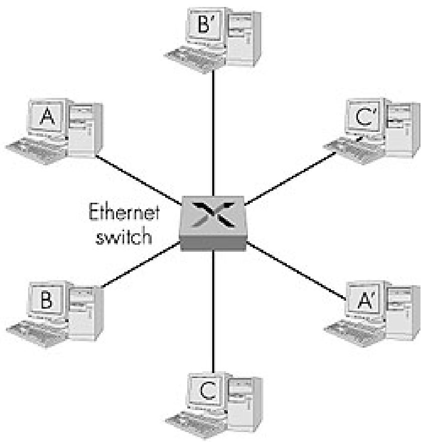
- Both store-and-forward devices
- Bridge does well in small (few hundred hosts) while router used in large networks (thousands of hosts)

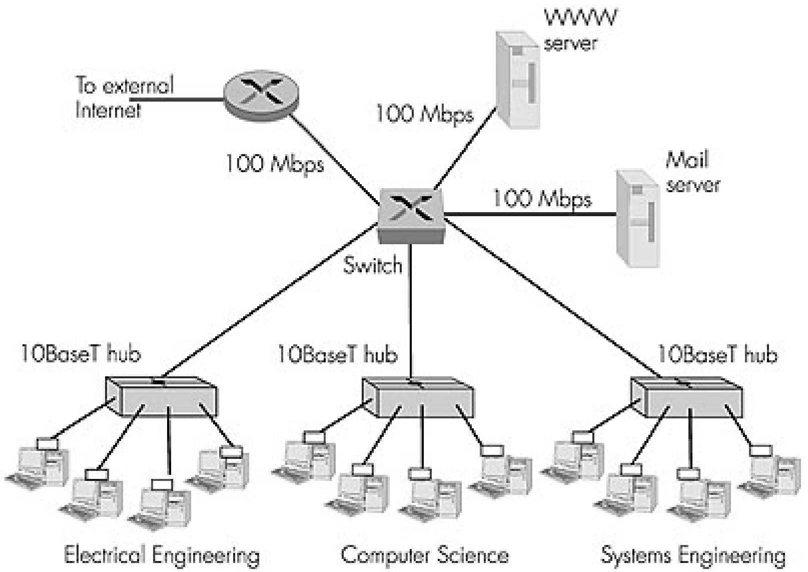


Device	Bridge	Router
OSI model	● Link layer devices	● Network layer devices (examine network layer headers)
Operation	● It maintains filtering tables, implement filtering, learning and spanning tree algorithms	● It maintains routing tables, implement routing algorithms
Advantage	● Bridge operation is simpler requiring less processing	● Arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols) ● Provide firewall protection against broadcast storms
Disadvantage	● Topologies are restricted with bridges: a spanning tree must be built to avoid cycles ● Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)	● Require IP address configuration (not plug and play) ● Require higher processing

Ethernet Switches

- Layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-B and A'-to-B' simultaneously, no collisions
- Large number of interfaces
- Often: individual hosts, star-connected into switch
  - Ethernet, but no collisions
- Cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- Combinations of shared/dedicated, 10/100/1000 Mbps interfaces





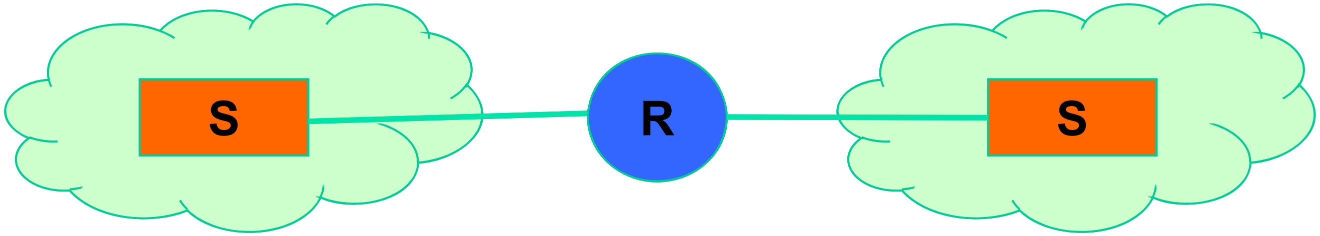
Switch vs. Router

- Routers deal with IP packets, switches deal with Ethernet frames
  - A router looks at the IP packet destination and checks its routing table to decide where to forward the packet

- Some differences:
  - IP packets travel inside Ethernet frames
  - IP networks can be logically segmented into subnets
  - Switches do not know about IP, they only deal with Ethernet frames

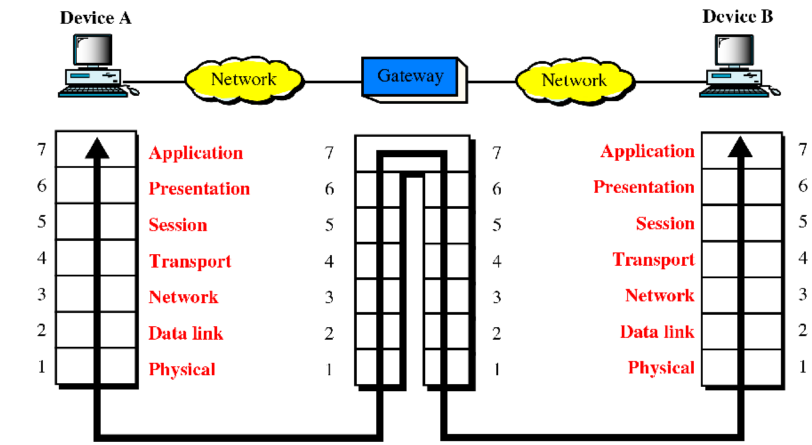
- Routers do not forward Ethernet broadcasts
  - Switches reduce the collision domain
  - Routers reduce the broadcast domain

- This becomes really important when trying to design hierarchical, scalable networks that can grow sustainably



Gateway

- Gateway potentially in all seven layers of OSI model
  - It is a protocol converter
- Gateway can accept packet formatted for one protocol (e.g., AppleTalk) and convert it to a packet formatted for another protocol (e.g., TCP/IP) before forwarding it
- Gateway is generally software installed within a router



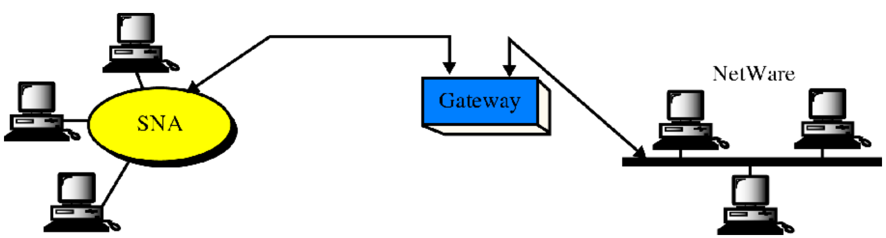


Figure: A gateway connecting an SNA network (IBM) to a Netware network (Novell)

Local Area Networks

- Local Area Network (LAN) is a data communication system that allows a number of independent devices to communicate directly with each other in a limited geographical area

- LANs can be connected to form a Metropolitan Area Network (MAN) or a Wide Area Network (WAN)

- Examples of LAN:
  - Ethernet (IEEE802.3)
  - Token Ring (IEEE802.5)
  - Fiber Distributed Data Interface, FDDI (IEEE802.8)

- Most popular local area networking today is Ethernet. Most network administrator building a network from scratch use Ethernet as a fundamental technology

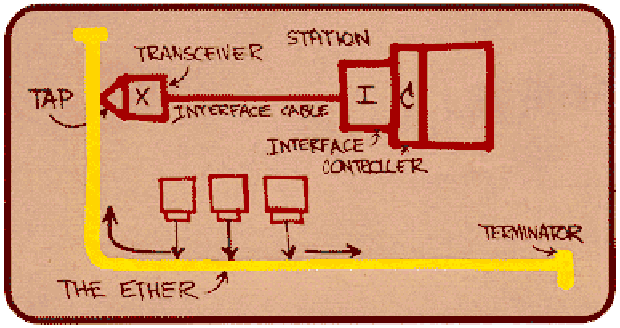
- Token ring technology is widely used in IBM networks

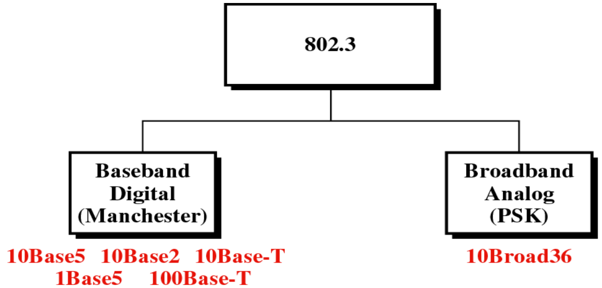
- FDDI networks are popular for campus LANs – and are usually built to support high bandwidth needs for backbone connectivity

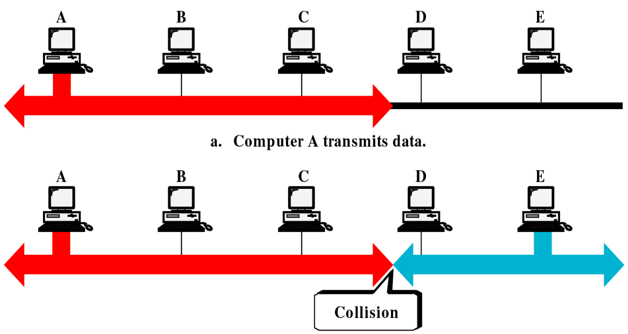
Ethernet

- Developed by Xerox, and extended by DEC, Intel and Xerox
- 2 categories
  - Baseband – specifies a digital signal (i.e., Manchester encoding)
  - Broadband – specifies an analog signal (i.e., PSK encoding)
- Access Method: CSMA/CD
  - Multiple Access: Multiple users access to a single line
  - Carrier Sense: A device listens to the line before it transmits
  - Collision Detection: Extremely high voltage indicates a collision

Metcalfe's Ethernet sketch



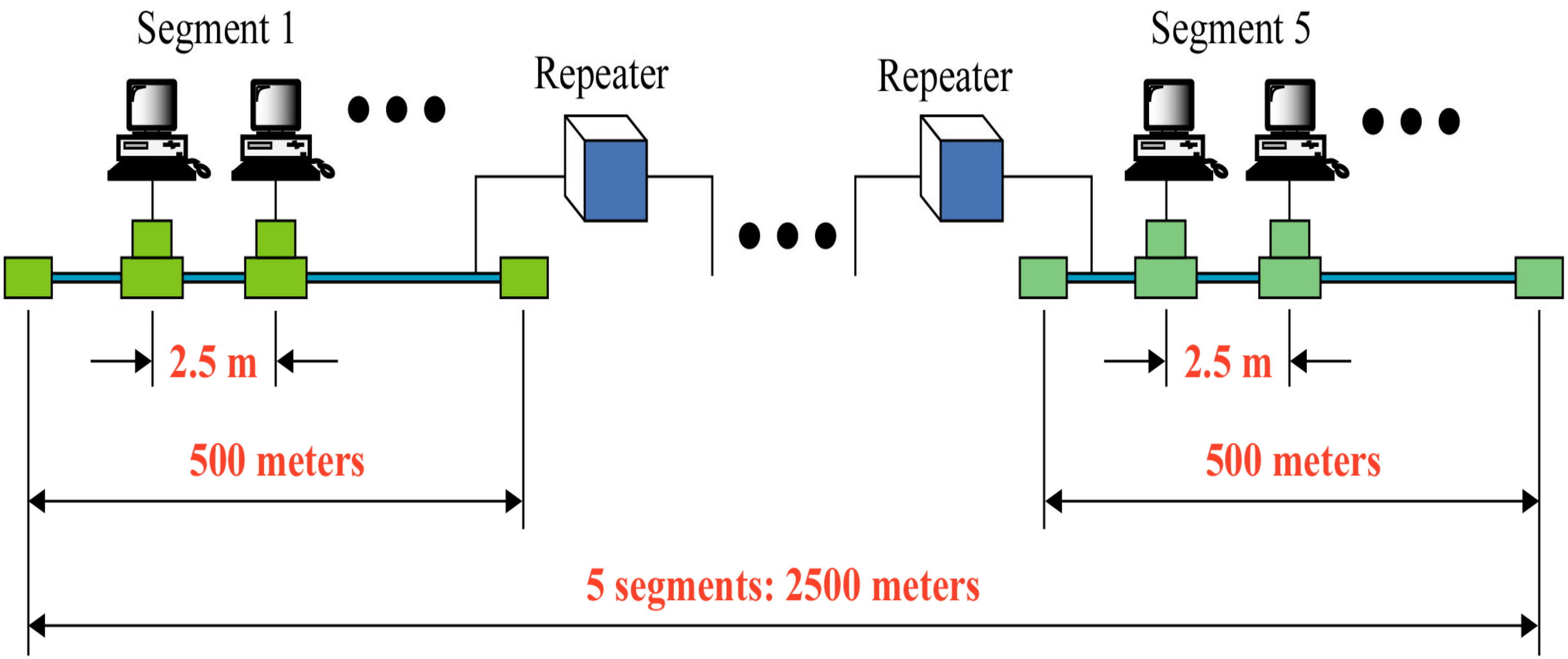




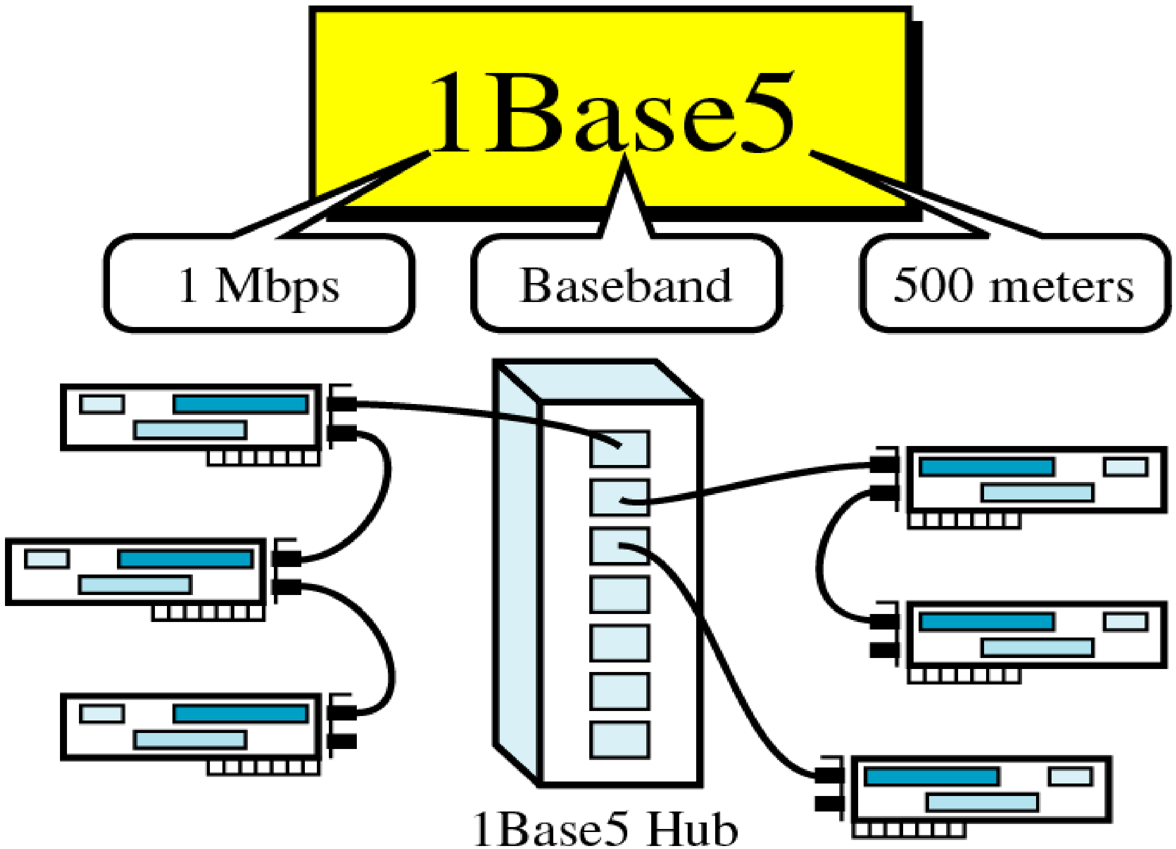
a. Computer A transmits data.

b. Before the signal reaches Computer E, E transmits data. Collision occurs.

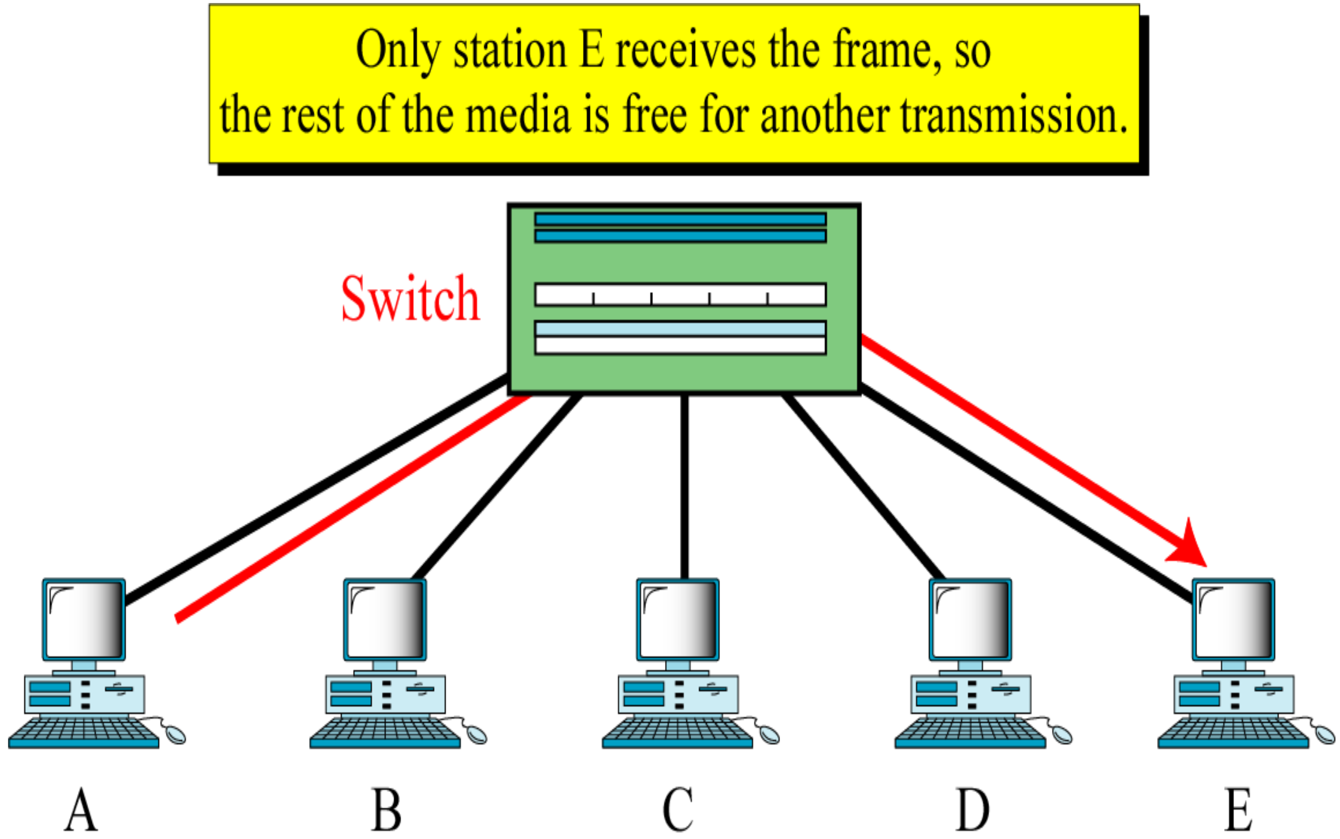
Typical Ethernet



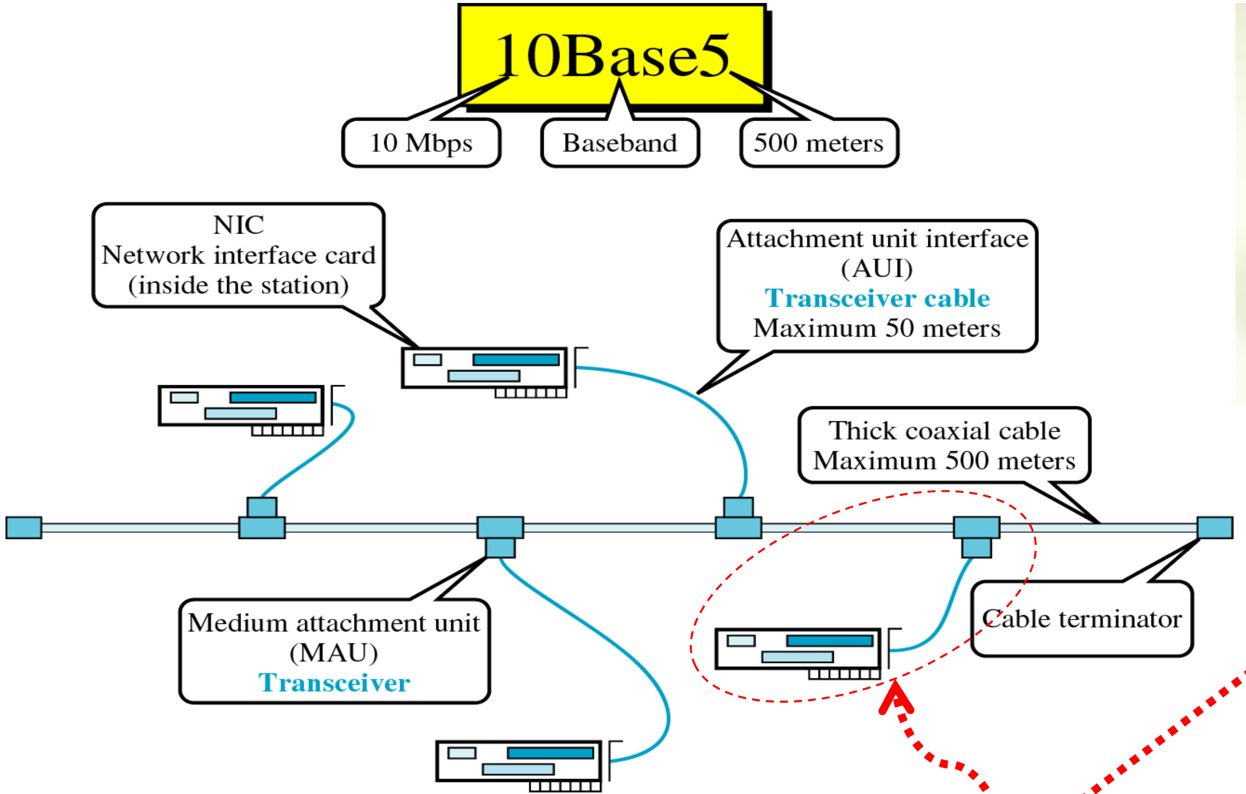
StarLAN

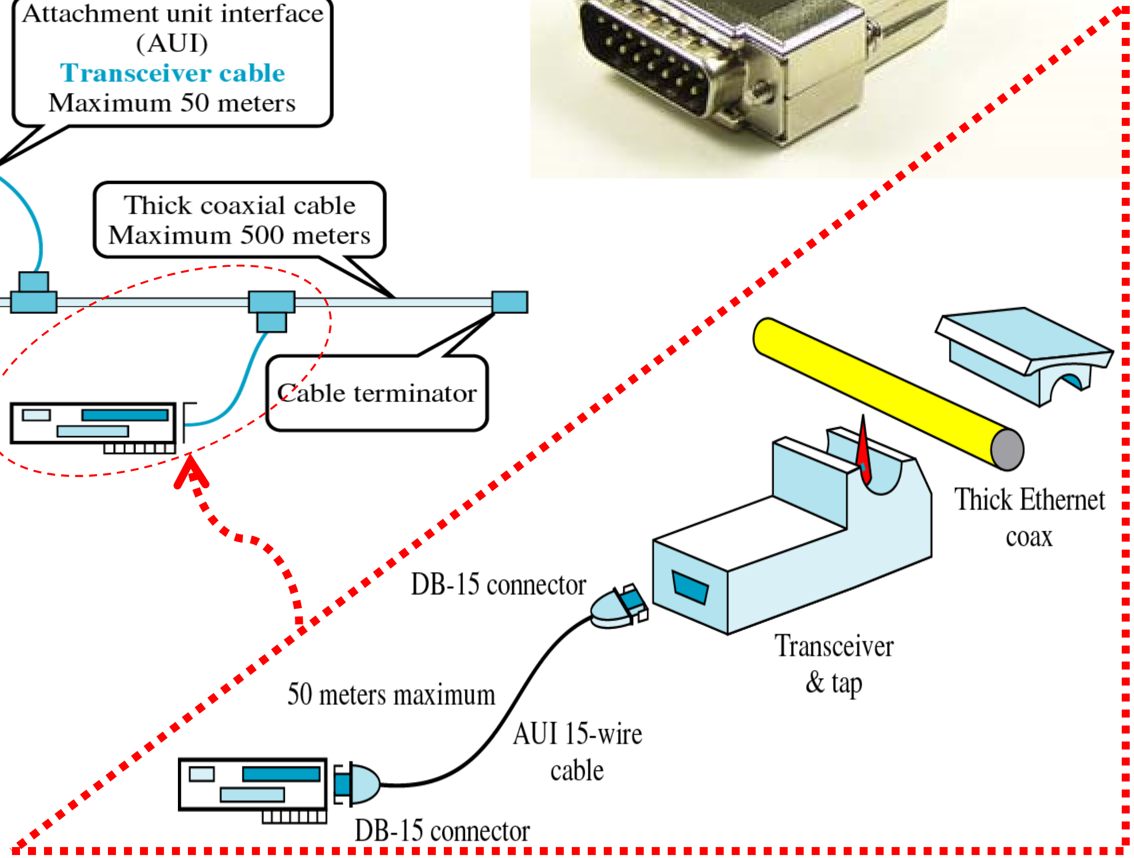


Switched Ethernet

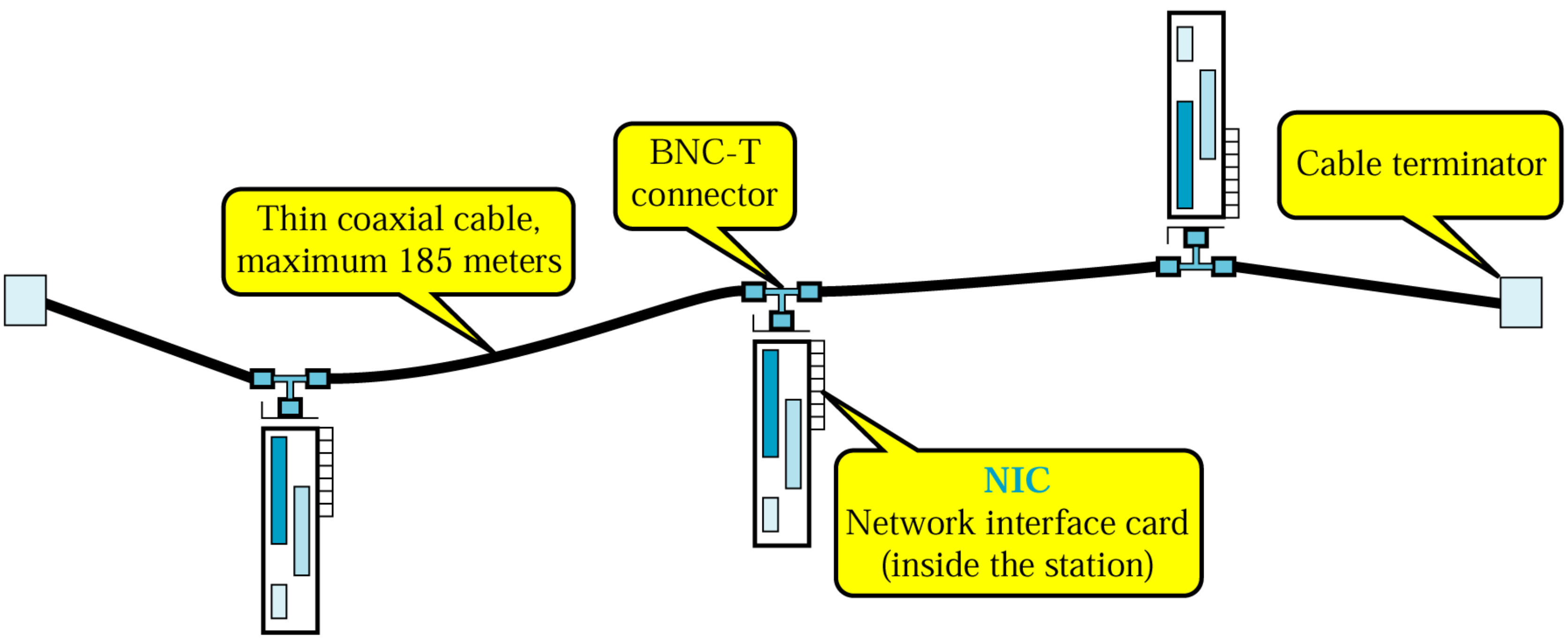


Thick Ethernet: 10BASE5

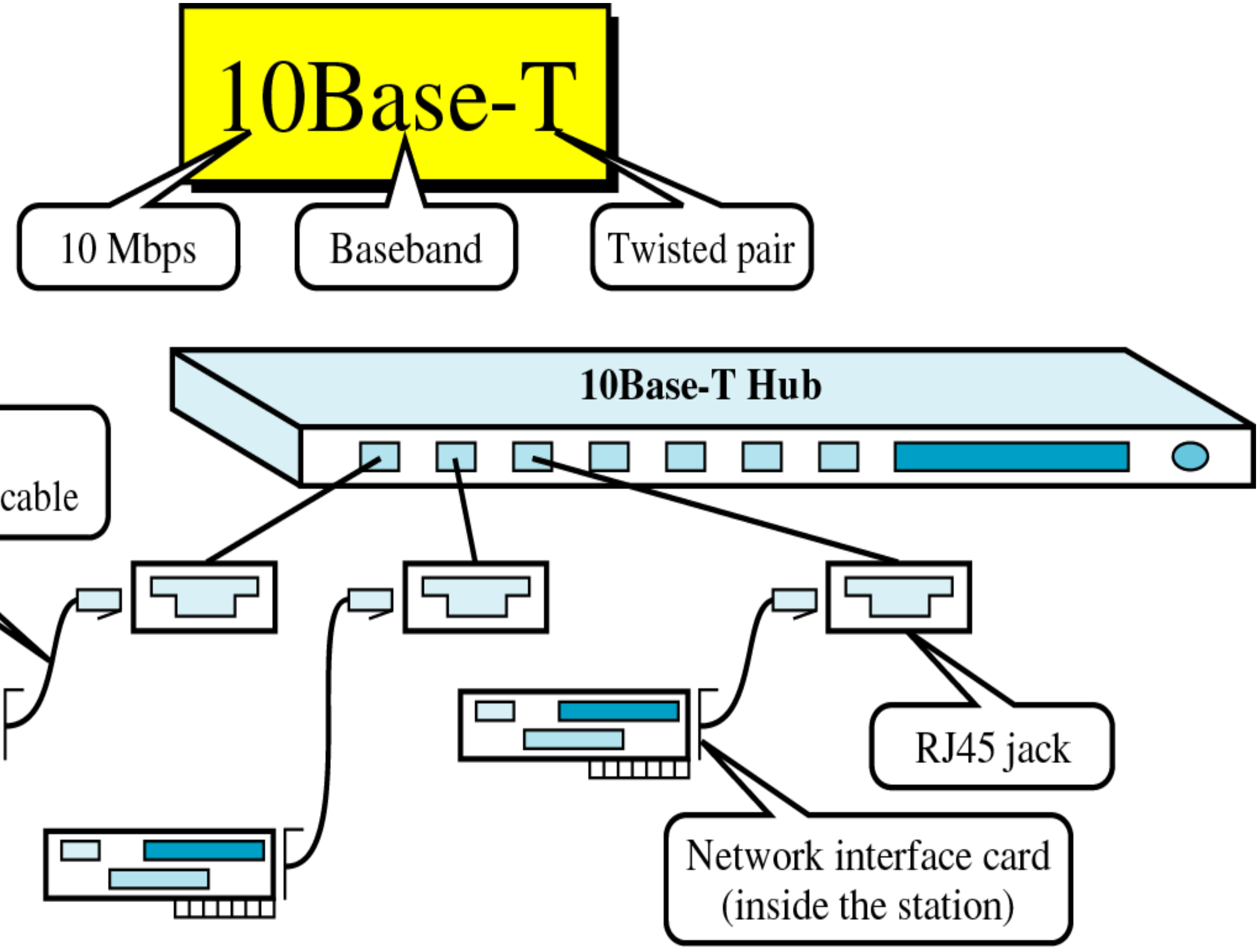




Thin Ethernet: 10BASE2



Twisted Pair Ethernet: 10 BASE-T



Ethernet: Physical Configurations

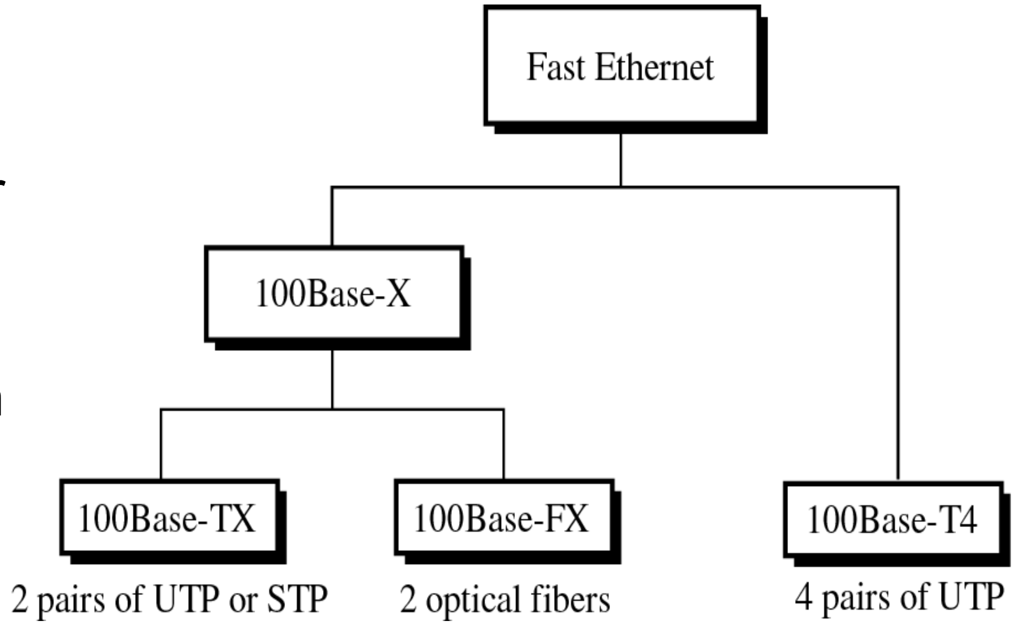
	10BASE5	10BASE2	10BASE-T	10BASE-F
Transmission medium	Coaxial cable (50 ohm)	Coaxial cable (50 ohm)	Unshielded twisted pair	850-nm optical fiber pair
Signaling technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/On-off
Topology	Bus	Bus	Star	Star
Maximum segment length (m)	500	185	100	500
Nodes per segment	100	30	-	33
Cable diameter	10 mm	5 mm	0.4 to 0.6 mm	65.5/125 µm

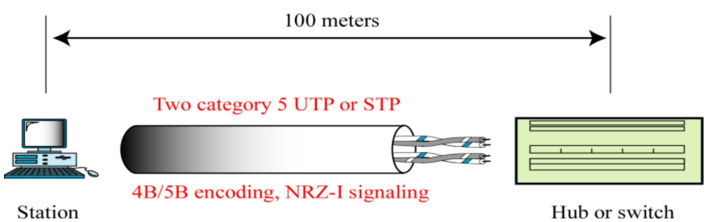
Note:

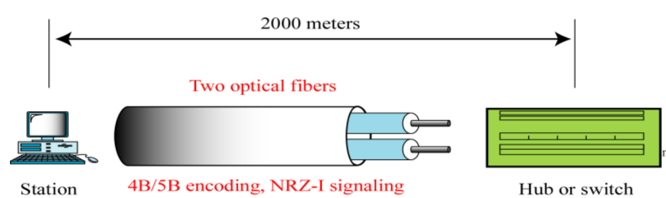
10	= data rate in Mbps	2	= thinner 50 ohm coaxial cable
BASE	= baseband	T	= unshielded twisted pair cable
5	= coaxial cable 50 ohm	F	= fiber optic cable

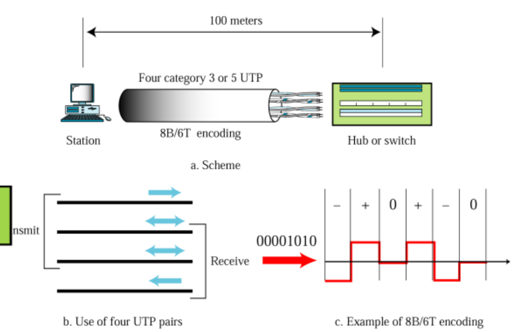
Fast Ethernet

- 10/100 Mbps rate; latter called "Fast Ethernet"
- Nodes connected to hubs or switches in a "star topology"
- Max distance from node to Hub is 100 meters based on electrical properties of TP
- Smart hubs
  - Disconnect "jabbering adapter" versus 10Base2



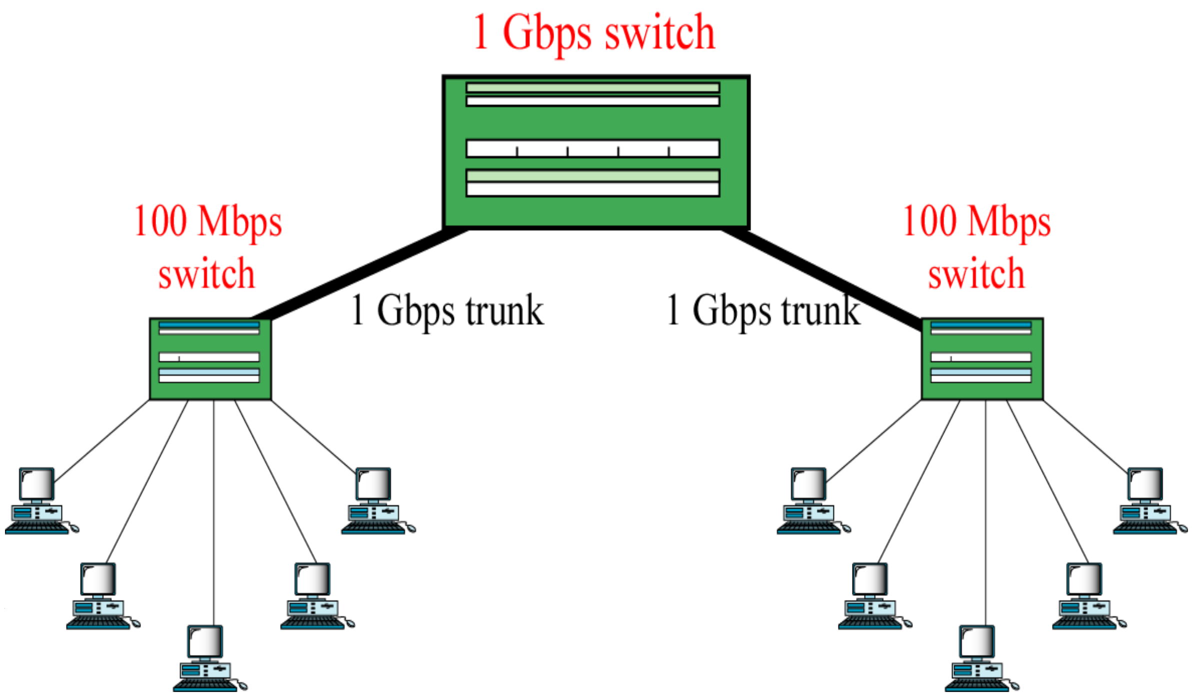






Gigabit Ethernet

- Use standard Ethernet frame format
- Allows for point-to-point links and shared broadcast channels
- In shared mode, CSMA/CD is used
  - Short distances required to be efficient
- Full-duplex at 1 Gbps for point-to-point links
- Usually serves as a backbone
- 4 implementations
  - 1000Base-SX, 1000Base-LX: Optical fiber, 550-5000 m
  - 1000Base-CX (STP) 1000Base-T (UTP): 25 m



Note: SX for short distance, LX for long distance

Announcement

- Next is Chapter 6 Transport Layer
- 09:00 ~ 10:40 on 31 October (Monday)