

## LAN Overview

by

Dr. Manas Khatua

Assistant Professor

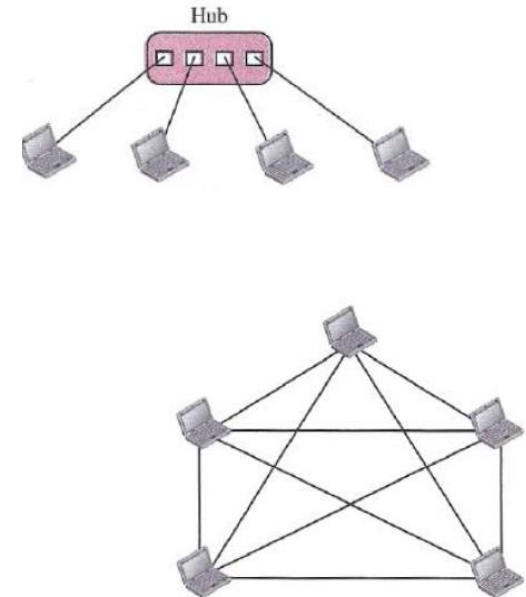
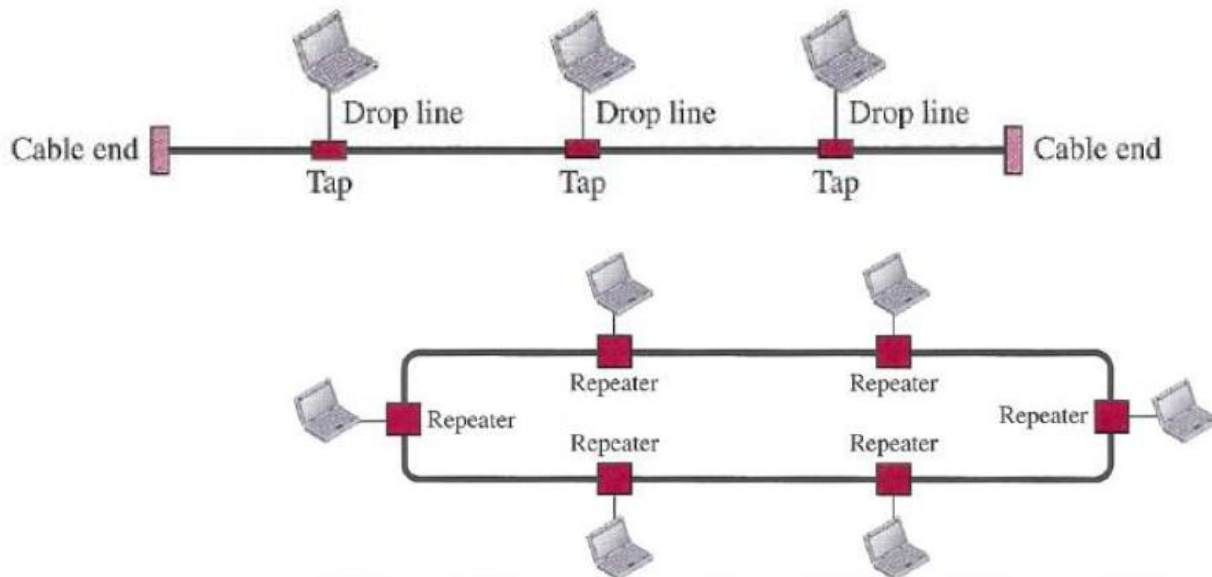
Dept. of CSE

IIT Guwahati

E-mail: [manaskhatua@iitg.ac.in](mailto:manaskhatua@iitg.ac.in)

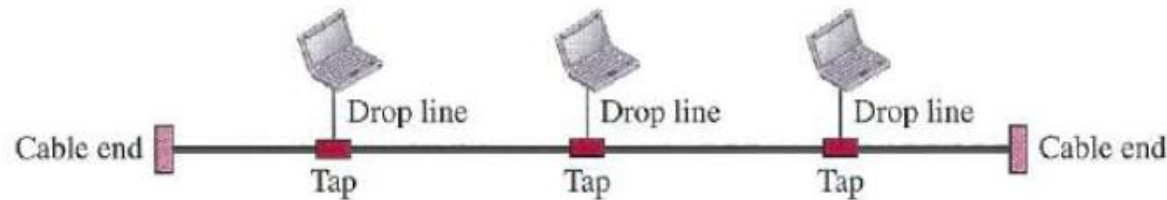
# Communication Network Topology

- **Topology** refers to the way in which the endpoints, or stations, attached to the network are interconnected.
- Common topologies for LANs
  - bus, tree/star, ring, and mesh



- **bus topology** shares many characteristics with **Wireless LANs**.

# Bus Topology



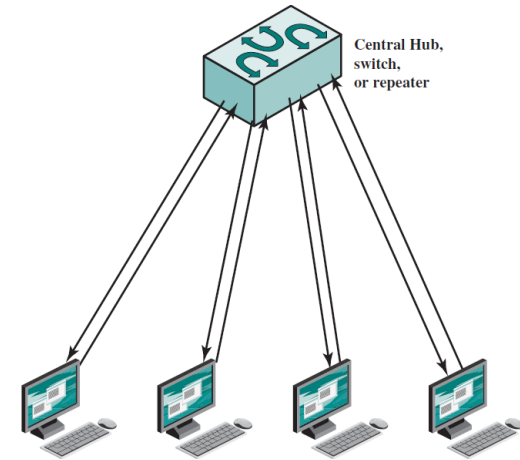
- All stations attach, through appropriate hardware interfacing known as a **tap**, directly to a linear transmission medium, or bus.
- **Full-duplex** operation **between** the **station** and the **tap** allows data to be transmitted onto the bus and received from the bus.
- A transmission from any station **propagates in both directions** and can be **received by all** other stations
- **Two problems:**
  - needs to be some way of indicating for whom the transmission is **intended**
  - a mechanism is needed to regulate transmission to avoid signal **overlap**

# Cont...

- To solve these problems, stations **transmit data in small blocks**, known as **frames**.
- **Frame header** contains control information - solves the first one.
- Each station on the bus is **assigned a unique address**, or identifier
- the destination address for a frame is included in its header.
- stations **send frames** in some **cooperative fashion** - solves the second
- It involves putting additional control information into frame header.
- **Note:** No special action needs to be taken **to remove frames from the bus**. When a signal reaches the end of the bus, it is **absorbed by the terminator**.

# Star Topology

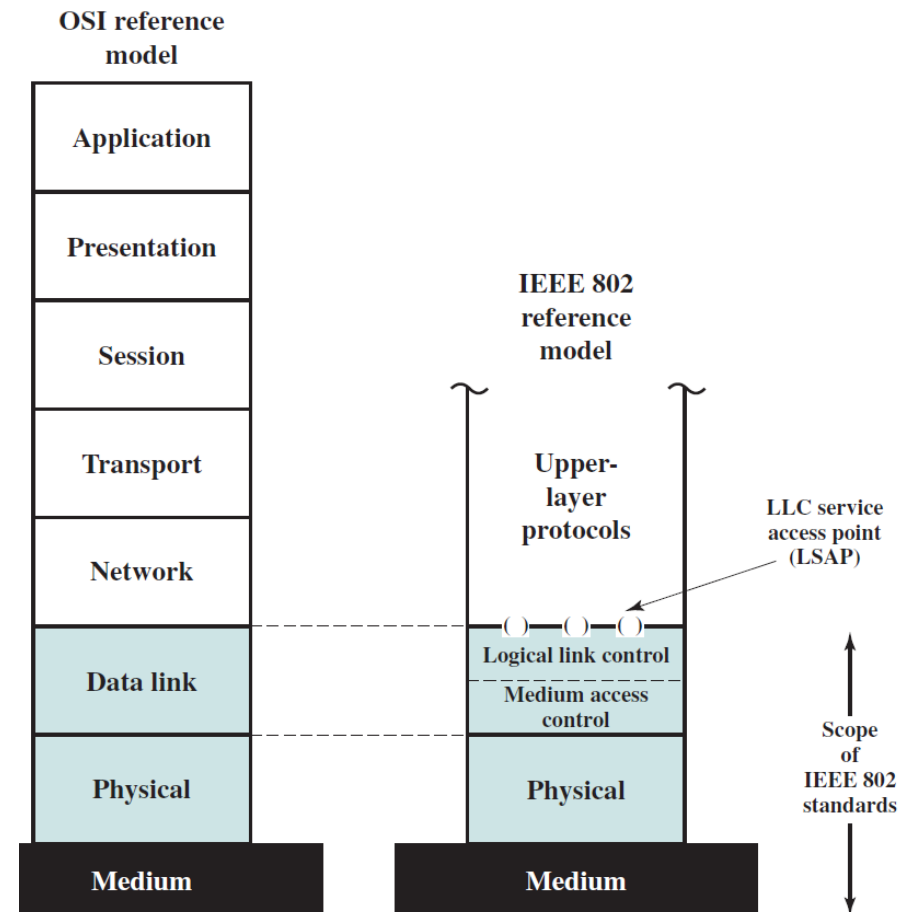
- each station is **directly connected** to a common central node e.g. **hub**
- Connected via two P2P links – uplink & downlink
- **Two type** of operations:
  - central node operates in a **broadcast fashion**
    - although the arrangement is **physically a star**, it is **logically a bus**: A transmission from any station is received by all other stations, and only **one station at a time** may successfully transmit
  - central node acts as a **frame-switching device**
    - incoming frame is **buffered** in the node and then **retransmitted** on an outgoing link to the destination station



# LAN Protocol Architecture

# LAN Protocol Architecture

- Standardized **protocol architecture for LANs**, encompasses
  - Physical layer
  - Medium access control (MAC) sub-layer
  - Logical link control (LLC) sub-layer
- IEEE 802 Reference Model
  - Defines protocols** specifically for LAN, MAN
  - Higher Layer protocols (layer 3 and above) in OSI Reference Model are **independent of network architecture** and thus applicable to LANs, MANs, WANs
- Physical layer services**
  - Encoding/decoding signals
  - Synchronization using Preamble
  - Bit Transmission/Reception
- 802 Model also includes:
  - Topology
  - Transmission Medium

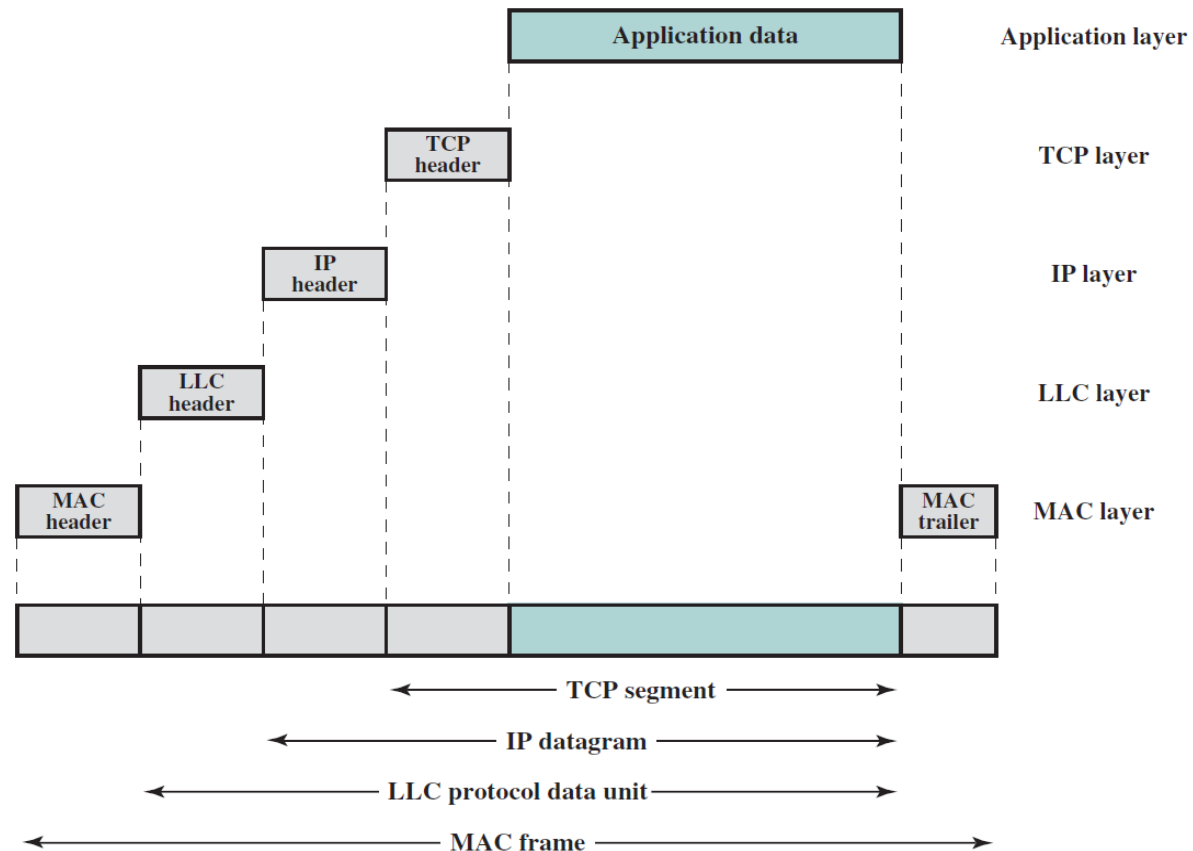


- Above the PHY layer
    - Service related to LAN users
      - On transmission:
        - Assemble data into Frame
        - Addressing
        - Error detection coding
      - On reception:
        - Disassemble Frame
        - Perform address recognition
        - Perform error detection
    - Govern access to the transmission medium (multiple access rules)
  - Provide an **interface to higher layer** and perform flow and error control
- Functions of **Medium Access Control (MAC)** sub-layer
- Functions of **Logical Link Control (LLC)** sub-layer



# Relationship of Levels

- **LLC** is concerned with the **transmission of a link-level protocol data unit** (PDU) between two stations;
- and mechanisms for **addressing** stations across the medium
- **MAC** protocol controls access to shared transmission medium



## Note:

- In most **data link control (DLC) protocols** (e.g. HDLC), the DLC entity is responsible for detecting errors using the CRC and recovering from those errors by retransmitting damaged frames.
- In the **LAN protocol architecture**, these two functions are **split between** the MAC and LLC layers.
- The **MAC layer** is responsible for **first one**, and the **LLC layer** performs the **second one**.

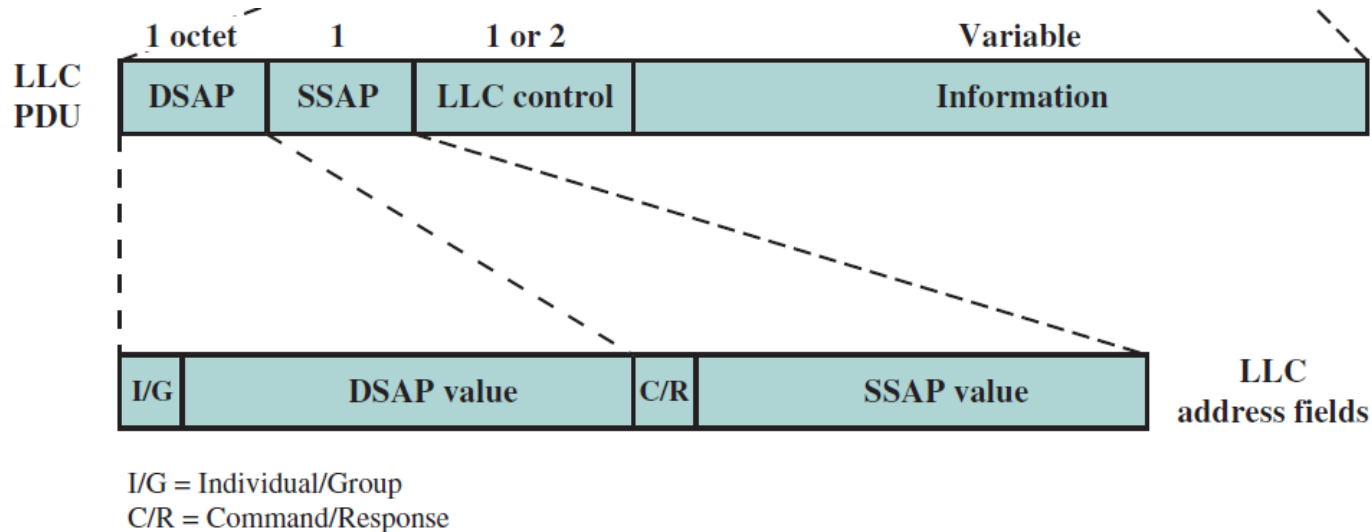
- **Three services** are provided for attached devices using LLC:
  - **Unacknowledged connection-less** service
    - This service is a **datagram-style** service.
    - very simple service
    - **does not involve** any of the **flow-** and **error-control** mechanisms.
    - Thus, the **delivery** of data is **not guaranteed**.
  - **Connection-mode** service
    - A **logical connection is set up** between two users exchanging data,
    - **Flow** control and **error control** are provided.
    - This service is similar to that offered by **HDLC**.
  - **Acknowledged connection-less** service
    - It provides that datagrams are to be **acknowledged**,
    - but, **no prior logical connection** is set up.
- Typically, a vendor will provide these services as options that the **customer can select** when purchasing the equipment.

# LLC's Application



- The **unacknowledged connectionless service** requires minimum logic
- It is **useful in two contexts**:
  - **First**, higher layers of software will provide the necessary **reliability and flow-control** mechanism (e.g. TCP in Internet)
  - **Second**, there are instances in which the **overhead of connection establishment** and maintenance is unjustified (e.g. Monitoring applications)
- The **connection-mode service** could be used in very simple devices, such as terminal controllers, that have little software operating above this level.
  - the LLC software must **maintain some sort of table** for each active connection, to keep track of the status of that connection.
- The **acknowledged connectionless service** is useful in several contexts.
  - a **process control** or **automated factory environment** where a central site may need to communicate with a large number of processors and programmable controllers
  - Another use is the handling of important and **time-critical alarm or emergency control** signals in a factory.

# LLC Protocol



**Figure 11.5** LLC PDU in a Generic MAC Frame Format

- Basic of LLC protocol is modeled from **HDLC**.
- **Addressing in LLC** involves specifying the source and destination LLC users.
- **LLC user** is a higher-layer protocol OR a network management function in a station.
- **LLC user addresses** are referred to as **service access points** (SAPs)
- **DSAP**: Destination service access points
- **SSAP**: Source service access points

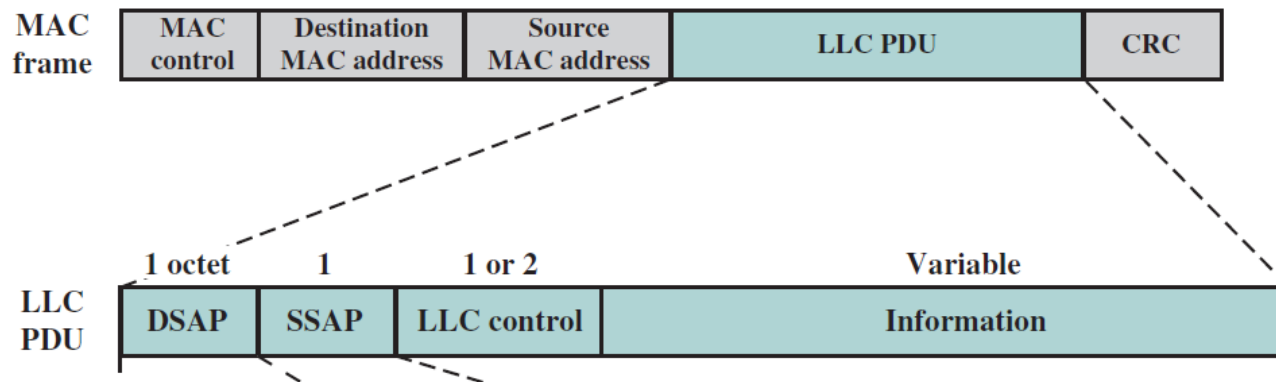
# Medium Access Control (MAC)



- All LANs and MANs consist of collections of devices that must **share the network's transmission capacity**.
- Key parameters of MAC:
  - **Where**: centralized or distributed control
  - **Who & When**: access control techniques
    - constrained by the topology and is a trade-off among competing factors, including cost, performance, and complexity
- **Advantages** of centralized scheme
  - relatively simple access logic
  - afford greater control over access for providing priorities, overrides, and guaranteed capacity
  - avoids problems of distributed coordination
- **Disadvantages** of centralized scheme
  - single point of failure
  - may act as a bottleneck, reducing performance
- **Access control techniques** are either **synchronous** or **asynchronous**
- **Synchronous**: a specific capacity is dedicated to a connection
  - Likewise TDM, FDM in switching

- **Asynchronous/dynamic**: allocate capacity more or less w.r.t immediate demand
  - **Round Robin / Channelization**
    - each station in turn is given the opportunity to transmit
    - Control of sequence may be centralized or distributed
    - **Polling** is an example of a centralized round robin technique
    - When **many stations have data** to transmit **over an extended period of time**, it is very efficient
  - **Reservation**
    - time on the medium is divided into slots
    - A station wishing to transmit reserves future slots
    - For **stream traffic** (voice commun., bulk file transfer, telemetry/monitoring), it is well suited
    - reservations may be made in a centralized or distributed fashion
  - **Contention / Random-access**
    - appropriate for **bursty traffic** (short, sporadic transmissions)
    - no control is exercised to determine whose turn it is
    - all stations contend for time in a way that rough and tumble
    - These techniques are of necessity distributed in nature
    - they are simple to implement and, under light-to-moderate load, efficient
    - performance tends to collapse under heavy load

# MAC Frame Format



- **MAC Control:** it contains any protocol control information needed for the functioning of the MAC protocol.
- **Destination MAC Address:** The destination physical attachment point on the LAN for this frame.
- **Source MAC Address:** The source physical attachment point on the LAN for this frame.
- **LLC PDU:** The LLC data from the next higher layer.
- **CRC:** The Cyclic Redundancy Check field (also known as the Frame Check Sequence, FCS, field). This is an error-detecting code.

We will discuss more about MAC Protocol during the discussion of **Wireless LAN**.

# Networking Devices



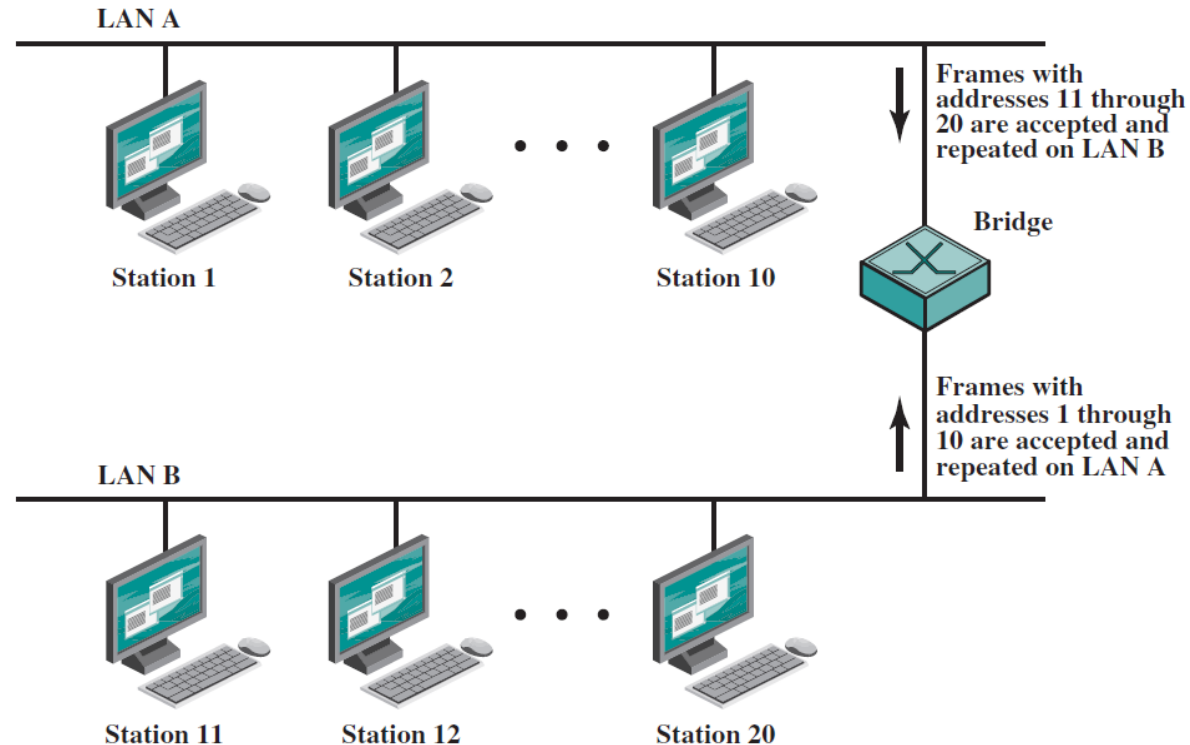
# Bridge



- to **expand** beyond the confines of a single LAN,
- to **provide interconnection** to other LANs and WANs
  - Two general approaches for this: using **bridges** and **routers**
- bridge is used **between LANs** that use **identical protocols** for the **physical** and **link layers**
- More sophisticated bridges are **capable of mapping** from one **MAC format** to another (e.g., to interconnect an **Ethernet** and a **token ring** LAN).
- **Why not simply have one large LAN?**
  - **Reliability**: a fault on the network may disable communication for all devices. By using bridges, the network can be **partitioned into self-contained units**.
  - **Performance**: performance on a LAN **declines** with an increase in the number of devices or the length of the wire.
  - **Security**: to support different **types of traffic** (e.g., accounting, personnel, strategic planning) that have **different security needs**
  - **Geography**: two separate LANs are needed to support devices **clustered in two geographically** distant locations.

# Functions of a Bridge

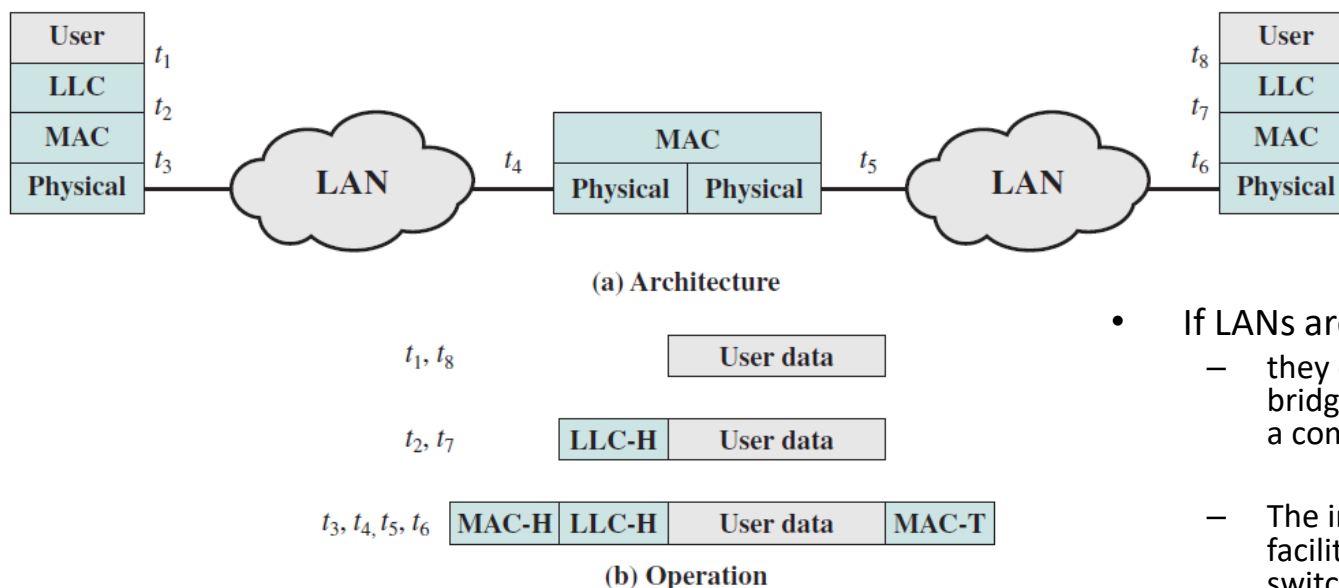
- The bridge makes **no modification to the content** or format of the frames it receives,
- It **doesn't encapsulate** the frames with an additional header



- The bridge should **contain enough buffer** space to meet peak demands
- The bridge must **contain addressing and routing intelligence**
- A bridge may **connect more than two LANs**.

# Bridge Protocol Architecture

- IEEE 802.1D defines the protocol architecture for MAC bridge
- The bridge can **function at** the **MAC level**
- The bridge **does not strip off** the MAC fields; its function is to **relay the MAC frame** intact to the destination LAN.
- The concept of **MAC relay bridge** is not limited to the use of a single bridge to connect two nearby LANs.

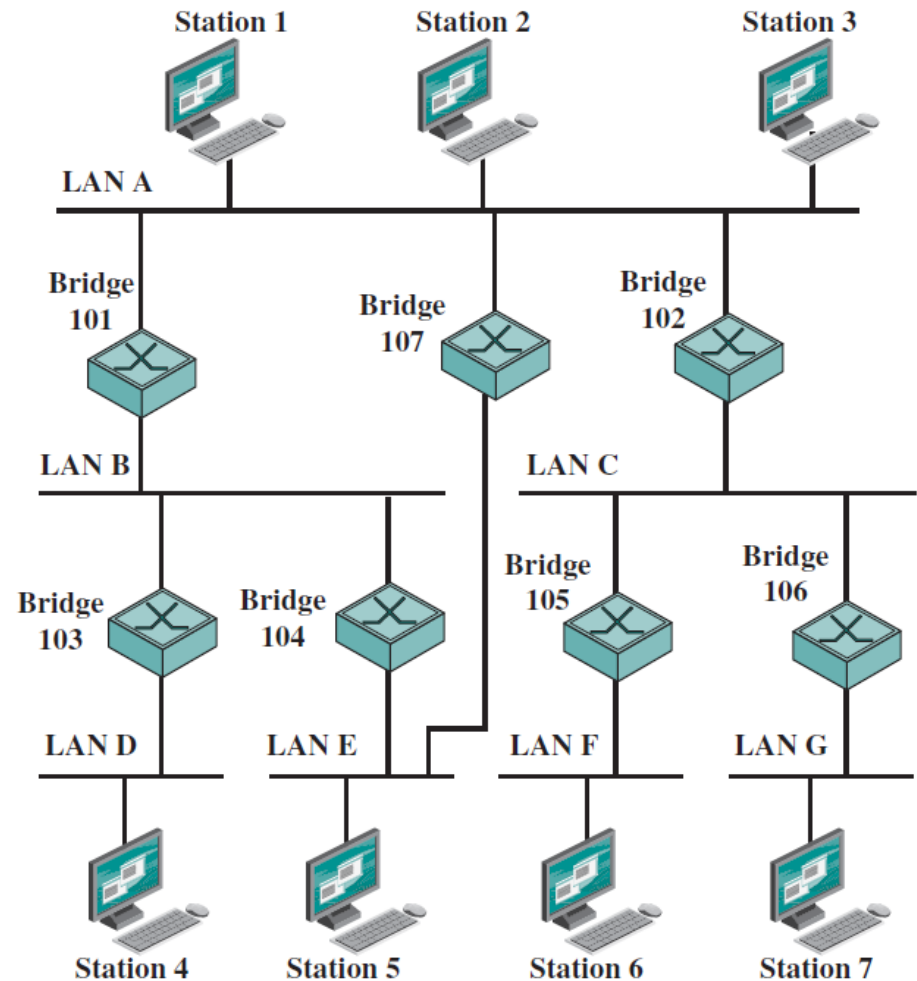


- If LANs are some distance apart, then
  - they can be connected by two bridges that are in turn connected by a communications facility.
  - The intervening communications facility can be a network (e.g. packet-switched network)

**Figure 11.7** Connection of Two LANs by a Bridge

# Frame Routing in Bridge

- Important to provide **alternate paths** between LANs **via** bridges
  - for load balancing
  - for reconfiguration in response to failure
- So, bridge must be **equipped with routing capability** (**note**: not like Layer 3 routing)
- When a bridge receives a frame
  - it **must decide** whether or not to forward the frame and,
  - if so, on which LAN the frame should be transmitted.
- Routing decision always not simple
- Routing Strategy:
  - **Fixed Routing** (most commonly used)
  - Spanning Tree (used in IEEE 802.1)
  - Source Routing (used in IEEE 802.5)



**Figure 11.8** Configuration of Bridges and LANs, with Alternate Routes

# Fixed Routing



- suitable for **small internets** and for internets that are **relatively stable**.
- **widely used in** commercially available products.
- A route is selected **for each source–destination pair** of LANs
- If alternate routes are available, then the route with **least number of hops** is selected.
- The **routes are fixed**, or at least **only change when** there is a change in the topology
- A **central routing matrix** is created, to be stored perhaps at a network control centre.
- Network manager **manually load** the data **into the routing tables** in fixed routing
- In a complex internet, it is **an overhead to maintain the routing table**.

# Hub

- The **hub** is the active central element of the **star topology** layout.
- Each station is connected to the hub **by two lines** (transmit and receive).
- The **hub acts as a repeater**
- Ordinarily, the line consists of **two unshielded twisted pairs**. the length of a line is limited to about **100 m**.
- An **optical fiber** link may be used. The maximum length is about **500 m**.
- **Note that** although this scheme is physically a star, it is **logically a bus**
- **Multiple levels** of hubs can be cascaded in a hierarchical configuration
- **HHUB** : header hub
- **IHUB**: intermediate hubs

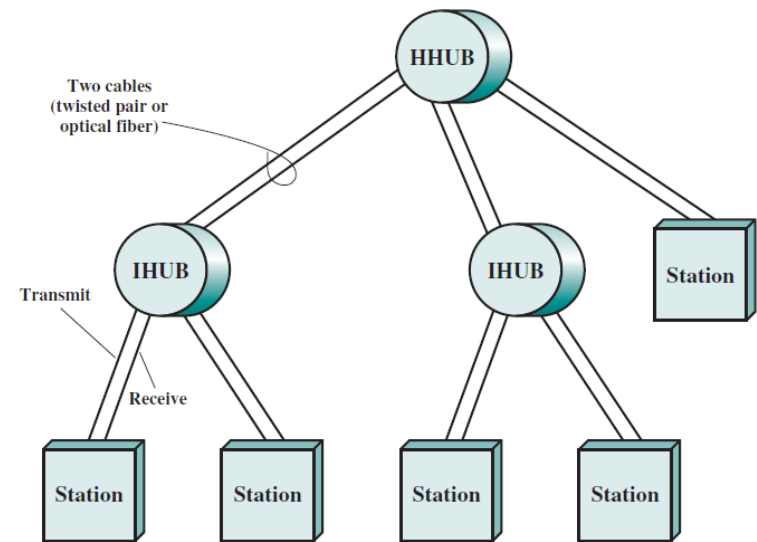


Figure 11.10 Two-Level Star Topology

# Switch (up to Layer 2)

- (a) it shows a typical **bus** layout of a traditional 10-Mbps LAN
- all the stations **must share the total capacity** of the bus, which is **10 Mbps**
- (b) **hub** uses a star wiring arrangement to attach stations to the hub.
- the **total capacity** of the LAN is **10 Mbps**.
- (c) central hub acts as a **switch**, much as a packet switch or circuit switch
- an incoming frame from a particular station is switched to the appropriate output line to be delivered to the intended destination
- At the same time, other unused lines can be used for switching other traffic
- In this example, the current **throughput on the LAN is 20 Mbps!**

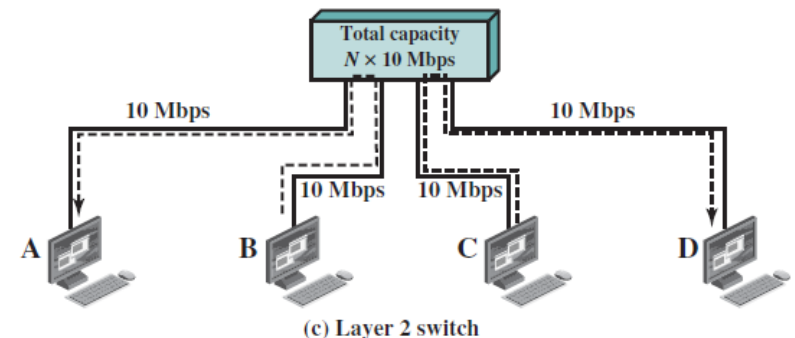
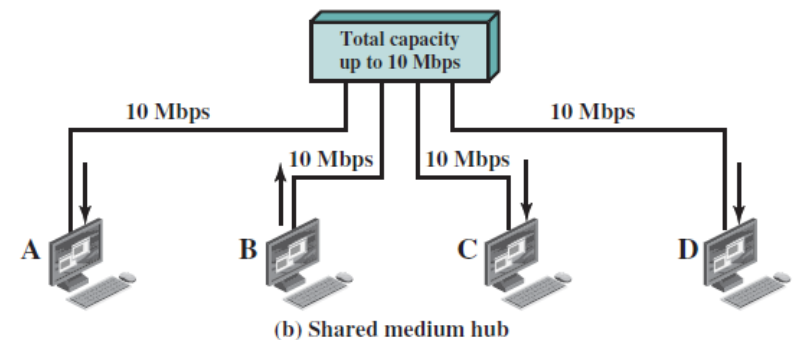
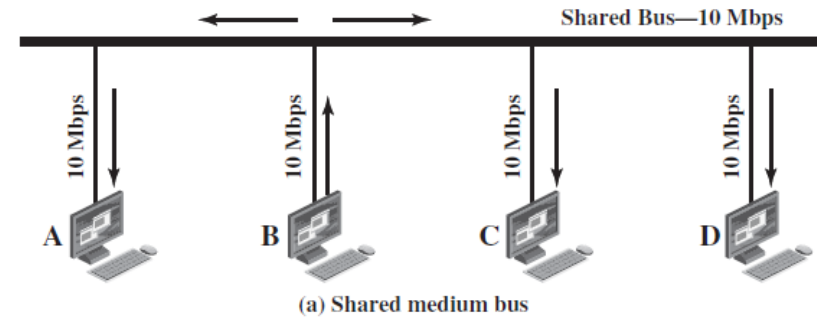
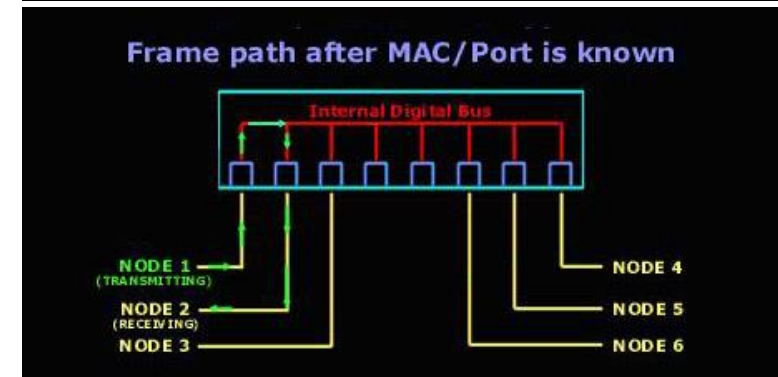
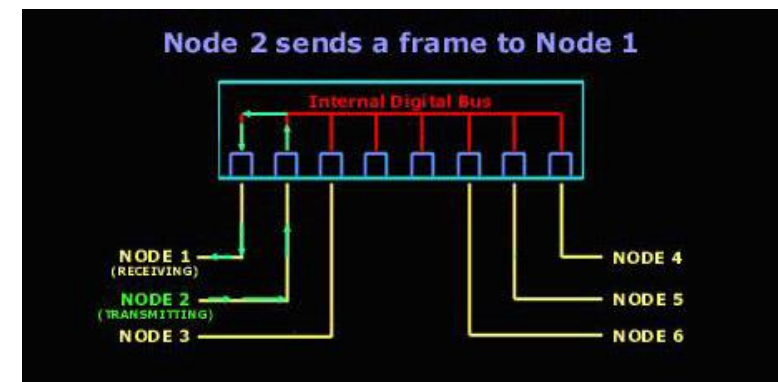
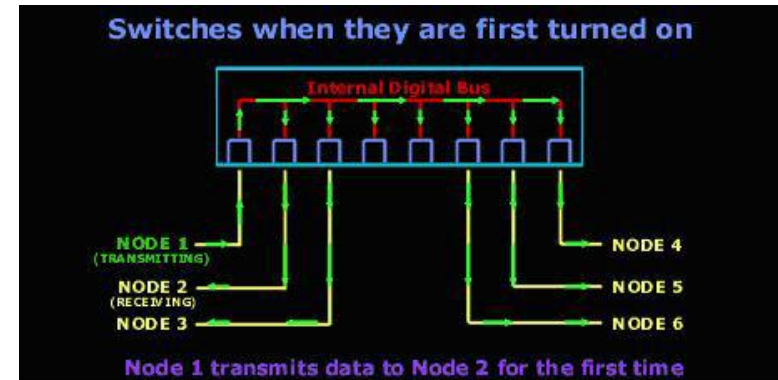
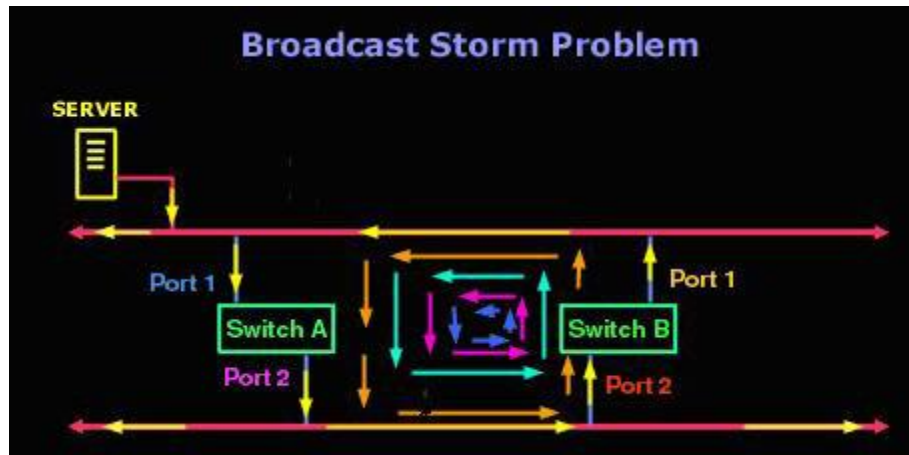


Figure 11.11 LAN Hubs and Switches

# Switch Operations

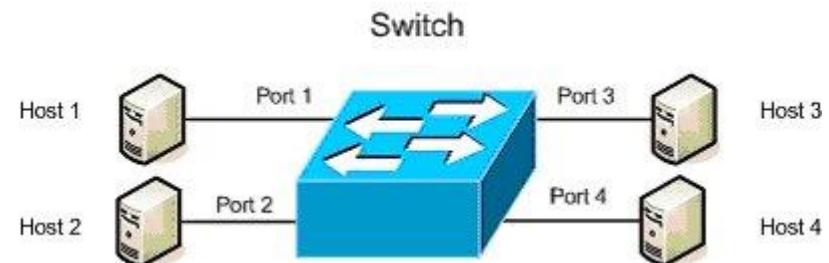
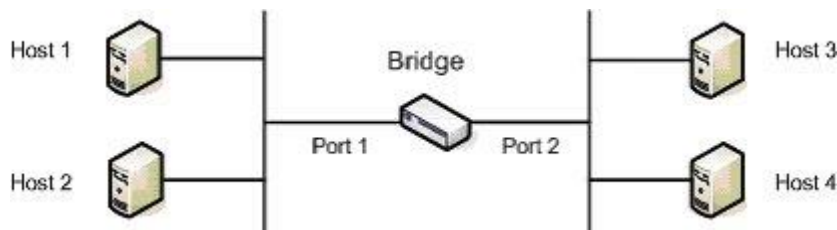
- All switch go through the three stages (sometimes two stages) when powered up and during operation
  - Address Learning
  - Forward/Filter decisions
  - Loop Avoidance (Optional)





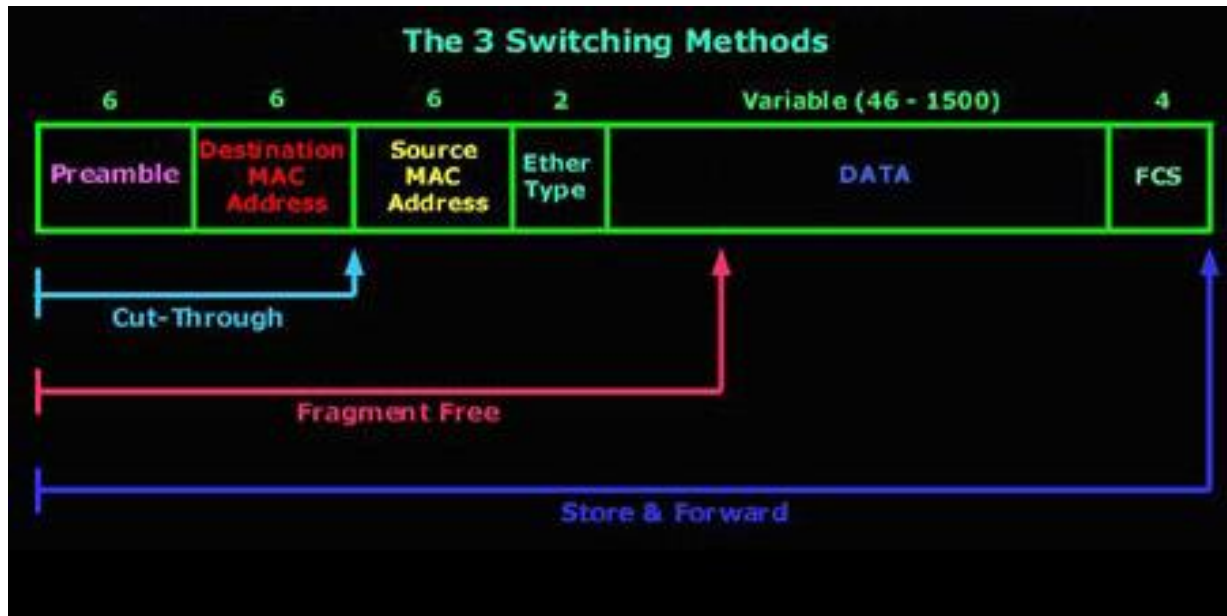
# Switch v/s Bridge

- Every port of **bridge** is connected to a shared common memory. Frame handling is done in **software**.
- **Switch** performs the address recognition and frame forwarding functions in **hardware** as it uses Application Specific Integrated Circuits (ASIC's) chip to build and maintain filter tables.
- A **bridge** can typically only analyze and forward **one frame at a time**.
- A **switch** has multiple parallel data paths and can handle **multiple frames at a time**.
- A **bridge** uses **store-and-forward** operation.
- A **switch** provides both, **store-and-forward** and **cut-through** operations.
- **Bridges** can only have **one spanning-tree** instance per bridge
- **Switches** can have **many**.
- **Bridges** can only have up to **16 ports**
- a **switch** can have **hundreds**!



# Switch Types

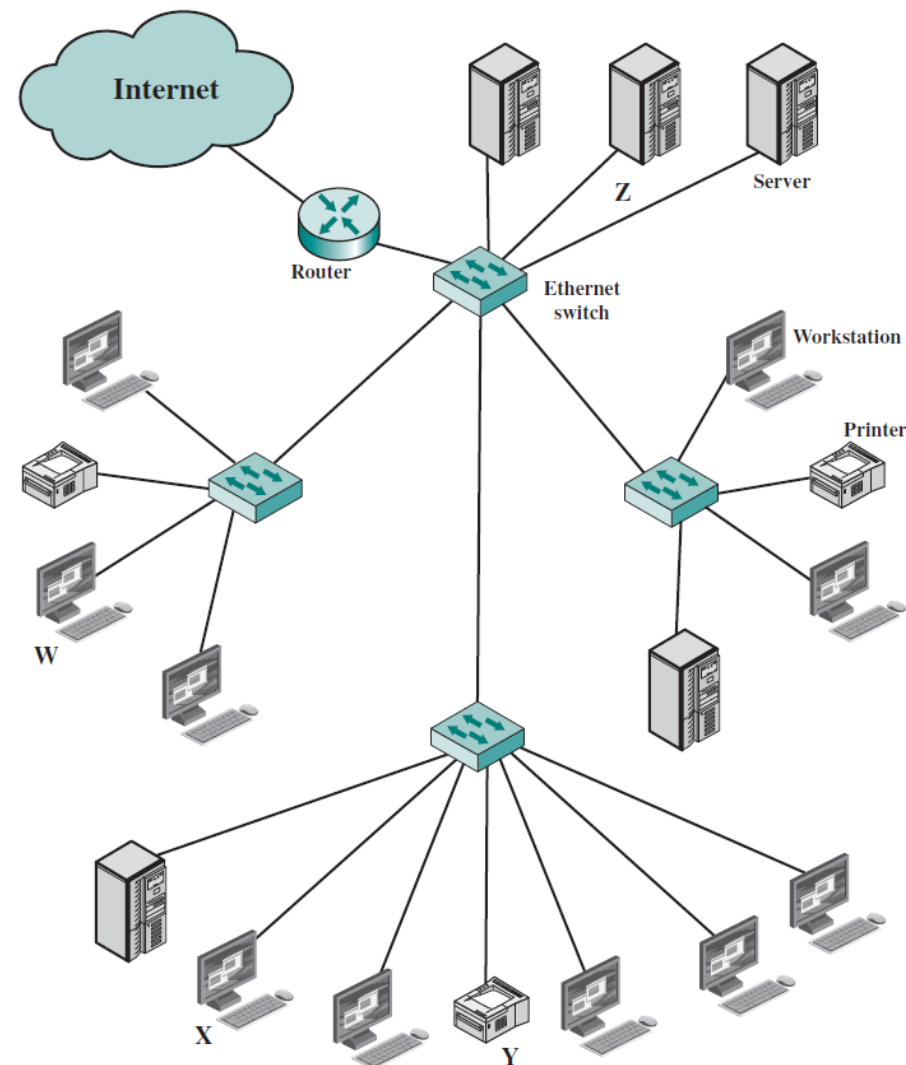
- **Store-and-forward switch:** The layer 2 switch accepts a frame on an input line, buffers it briefly, check error, and then routes it to the appropriate output line.
- **Cut-through (real-time) switch:** The layer 2 switch takes advantage of the fact that the **destination address appears at the beginning of the MAC frame**. The layer 2 switch **begins repeating** the incoming frame onto the appropriate output line as soon as the layer 2 switch recognizes the destination address.



- **Fragment free:** This method is a hybrid of the two other switching methods. The frame's first 64 bytes are only checked before forwarding the frame out the designated port.

# Virtual LAN

# Multiple Groups of LAN Devices



- Let the devices on the LAN be organized into **four groups**, each served by a LAN switch.
- Let a transmission from workstation X.
- Suppose the **destination** MAC address is Z
- the local switch routes the MAC frame through appropriate switches to the intended destination.
- It follows **unicast addressing**
- A MAC frame may also contain a **broadcast address** in which case all devices on the LAN should receive a copy of the frame.
- In many situations, **broadcast frame has information that is only useful to a particular department,**
- then transmission and computation **capacity is wasted** on the other portions of LAN and on the other switches

**How to avoid this wastage?**

Figure 11.12 A LAN Configuration

# Partition of LAN

- Simple solution:
- physically partition the LAN into separate broadcast domains
- We now have **four separate LANs** connected by a **router**
- **Drawback** to this approach
  - How to put a user into two broadcast domain?
  - Complex network formation with multiple routers.

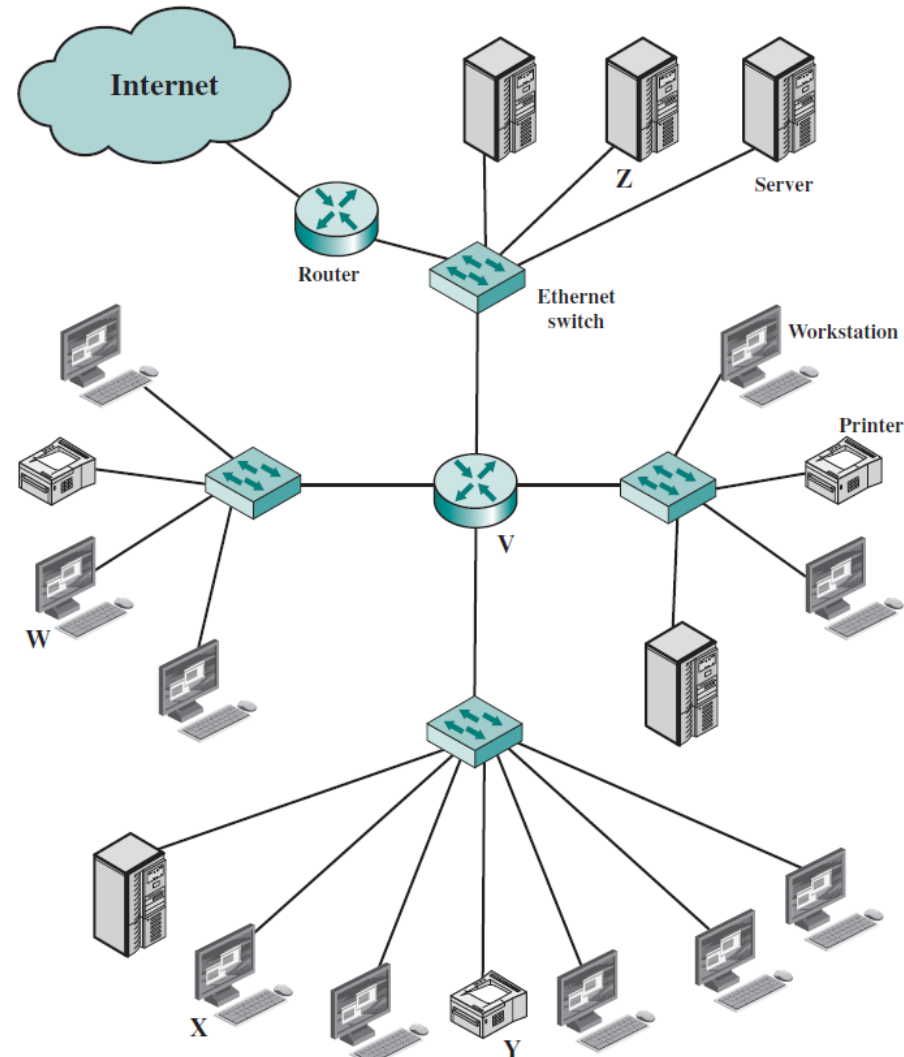


Figure 11.13 A Partitioned LAN

# Virtual LAN

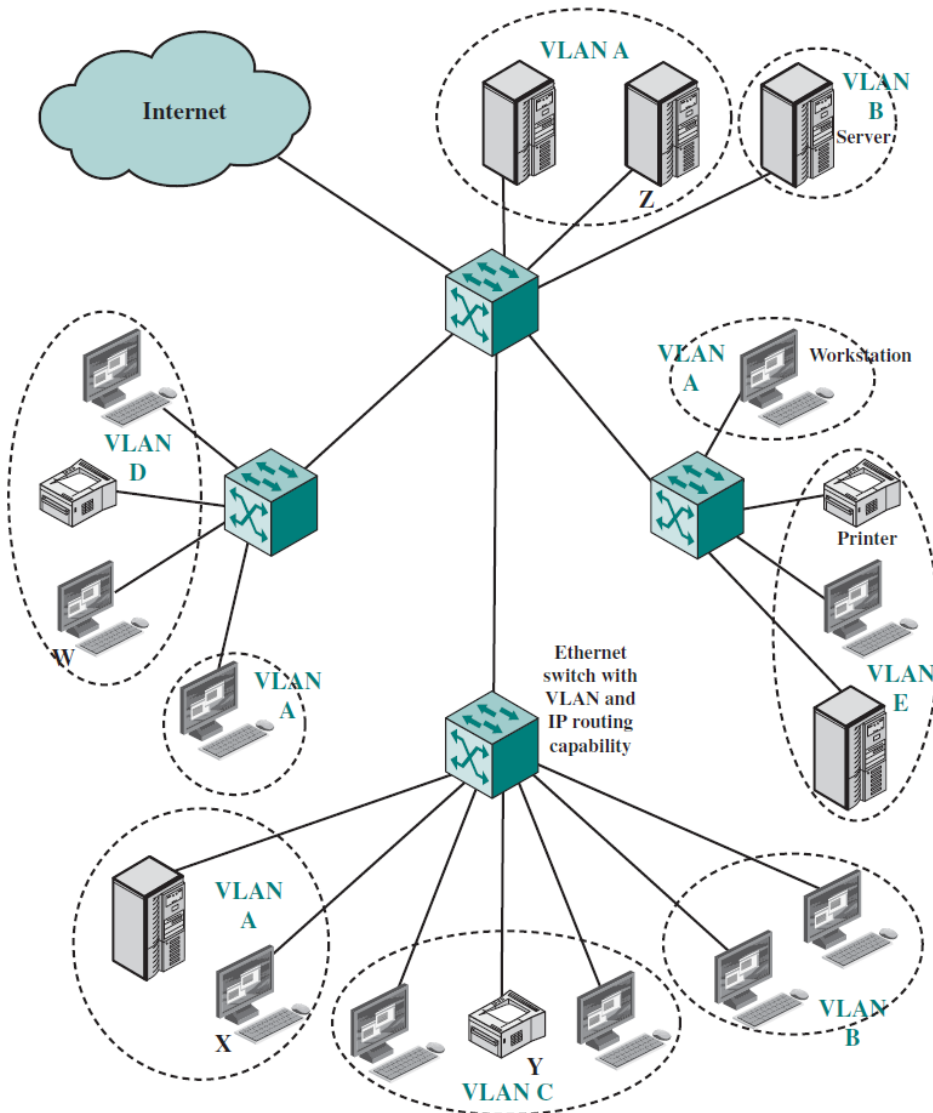


Figure 11.14 A VLAN Configuration

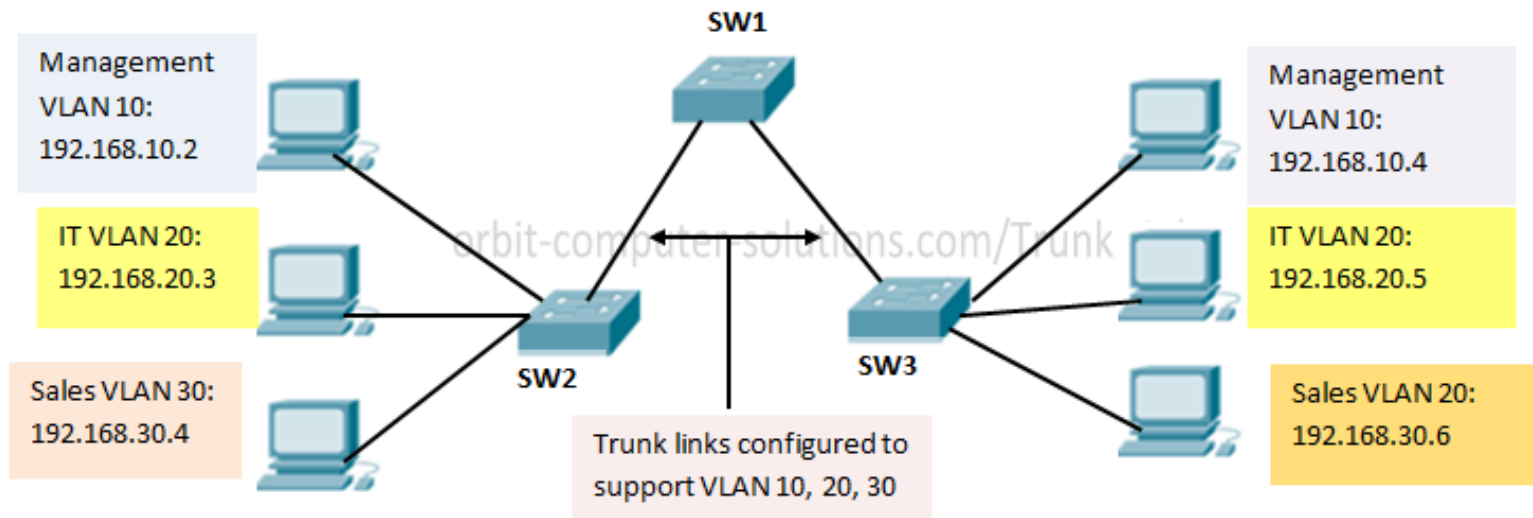
- More effective solution:
- creation of separate **virtual LAN** (VLAN) for each group.
- VLAN is a **logical subgroup** within a LAN
- It is created **by software** rather than by physically moving and separating devices
- It **combines** user stations and network devices **into a single broadcast domain** regardless of the physical LAN segment they are attached to
- The VLAN **logic is implemented** in LAN switches and **functions** at the MAC layer.

# Cont...

- Approaches for **defining membership** for VLAN configuration
  - by **MAC address**
  - by **port number**
  - by **protocol information** (e.g. IP address, TCP information)
- In brief, the **benefits of VLANs**:
  - simplification of moves, adds, and changes;
  - controlled broadcast activity;
  - workgroup and network security

# VLAN Trunks

- Large networks often contain **more than one switch**;
- if you want to span virtual LANs across two or more switches, a **VLAN trunk** can be used.
- A **trunk is a P2P link** between two network devices that carry more than one VLAN.
- Communicating VLAN Membership in Large network
  - Switches must have a **way of understanding VLAN membership** when network traffic **arrives from other switches**
    - A more common approach is **frame tagging** (IEEE 802.1q)
    - A **header** is inserted into each frame to uniquely identify to which VLAN a particular MAC-layer frame belongs

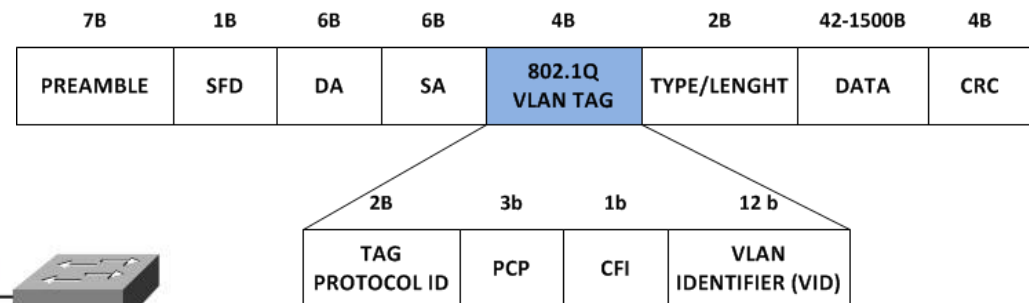
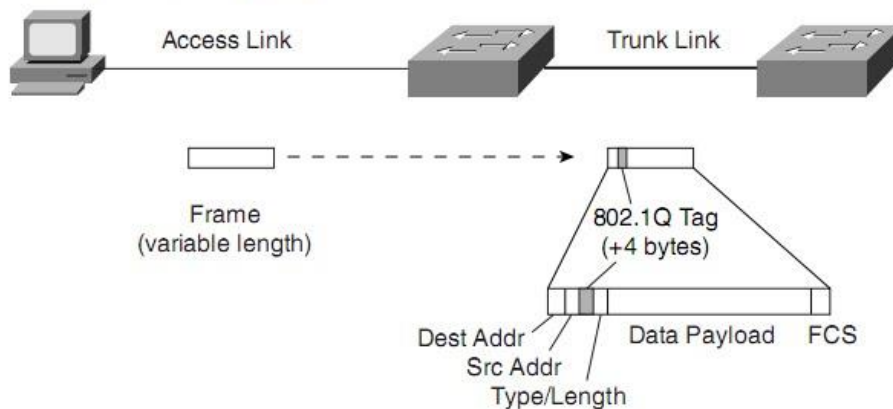




# VLAN Trunking Protocol

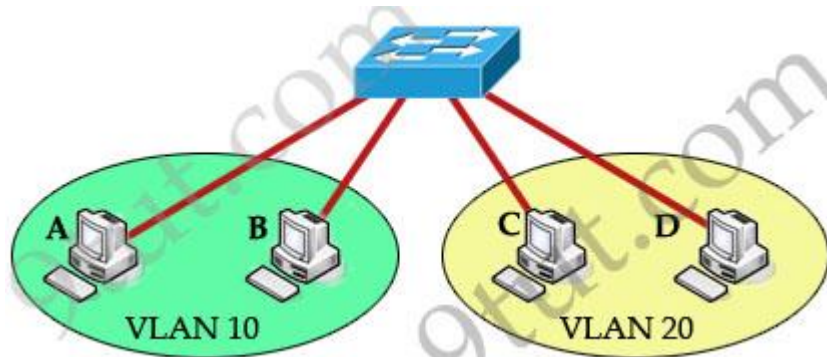
- Most Cisco switches support the IEEE 802.1Q used to coordinate trunks on FastEthernet and GigabitEthernet.
- To enable VLAN configured with trunk link to traffic frames between switches on the network, it made possible by a link protocol called **VLAN Trunking Protocol (VTP)**.
- VTP is a Cisco-proprietary link protocol, it provides a means by which Cisco switches can exchange VLAN configuration information. It enables the distribution of VLAN configuration among switches.

IEEE 802.1Q Frame-Tagging Standard

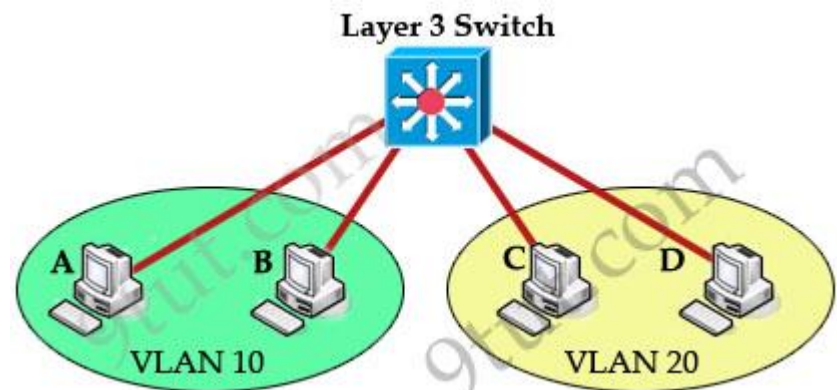
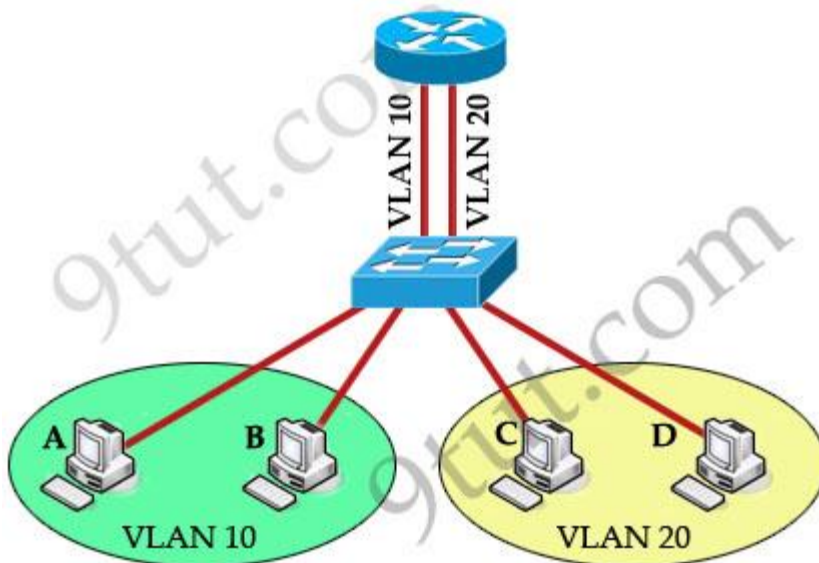


IEEE 802.1Q Frame Structure

# Inter-VLAN Routing

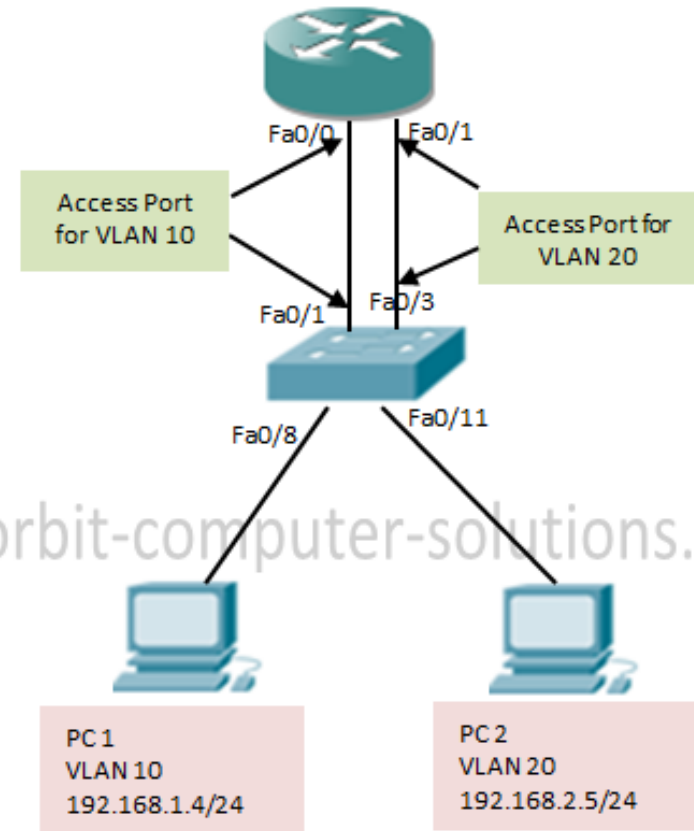


- Host A and B can communicate with each other as they are in the same VLAN 10;
- host C and D also can communicate as they are in the same VLAN 20
- But host A can't communicate with host C or D because they are in different VLANs.
- To allow hosts in different VLANs communicate with each other, we need a Layer 3 device (like a router) for routing.
- Routers can be implemented as separate devices OR the router logic can be implemented as part of the LAN Switch.



# Cont...

- **For example,**
- Let devices on VLAN 10 are configured to use IPv4 addresses in the 192.168.1.X IP space while devices on VLAN 20 are configured to use IPv4 addresses in the 192.168.2.x space.
- In addition to each device having its own IP address and subnet mask, a default gateway IP addresses is required.
- Every device in VLAN 10 will be configured to use the same default gateway IP address such as 192.168.1.1 and every device configured for VLAN 20 will use the gateway of 192.168.2.1.
- The default gateway IP address is a router interface (either physical or virtual) that is responsible for routing traffic to other IP networks.



# Thanks!

Figure and slide materials are taken from the following sources:

1. W. Stallings, (2017), [Data and Computer Communications, 10<sup>th</sup> Ed.](#)
2. [NPTL lecture](#) on Data Communication, by Prof. A. K. Pal, IIT Kharagpur
3. B. A. Forouzan, (2012), [Data Communication and Networking, 5<sup>th</sup> Ed.](#)