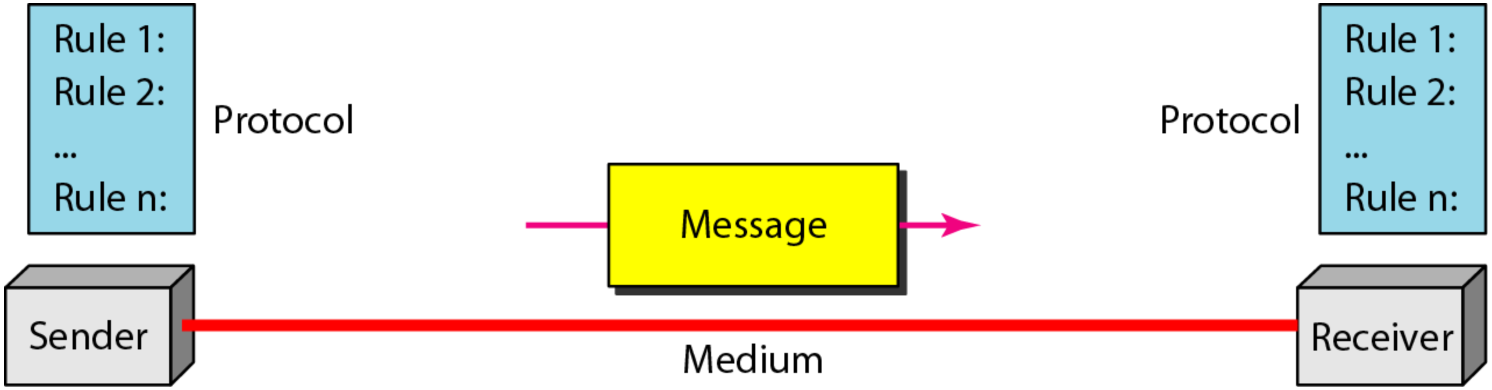
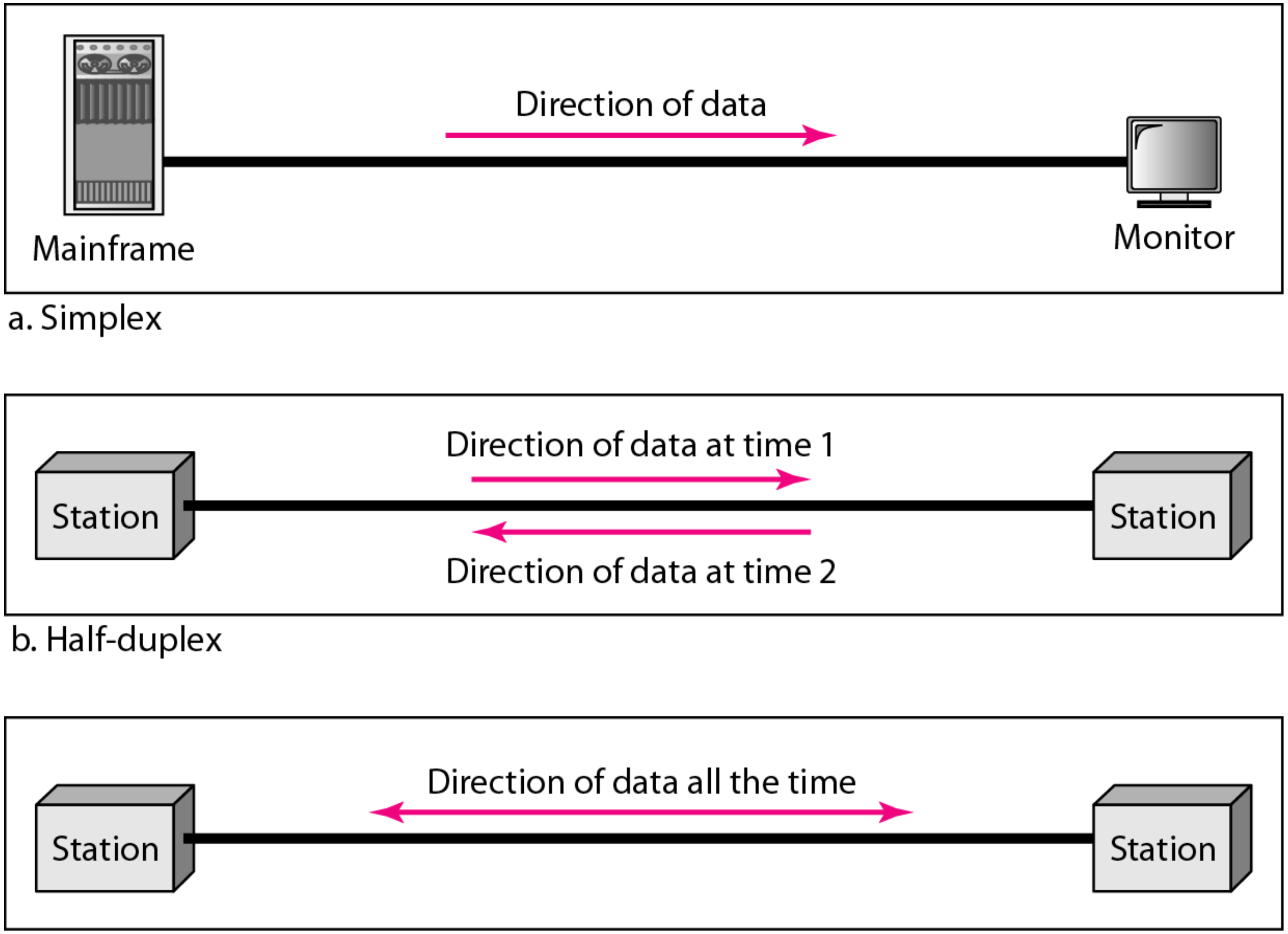
Unit 5: Overview of Data Communication Networking

Five Components of Data Communication



- Message:
  - text, number, images, audio, and video
- Sender and Receiver
  - devices that send/receive data message
  - Computer, workstation, telephone, TV, etc.
- Transmission medium
  - Physical path thru which the message travels
- Protocol
  - Set of rules governing data communications

Data flow (simplex, half-duplex, and full-duplex)


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

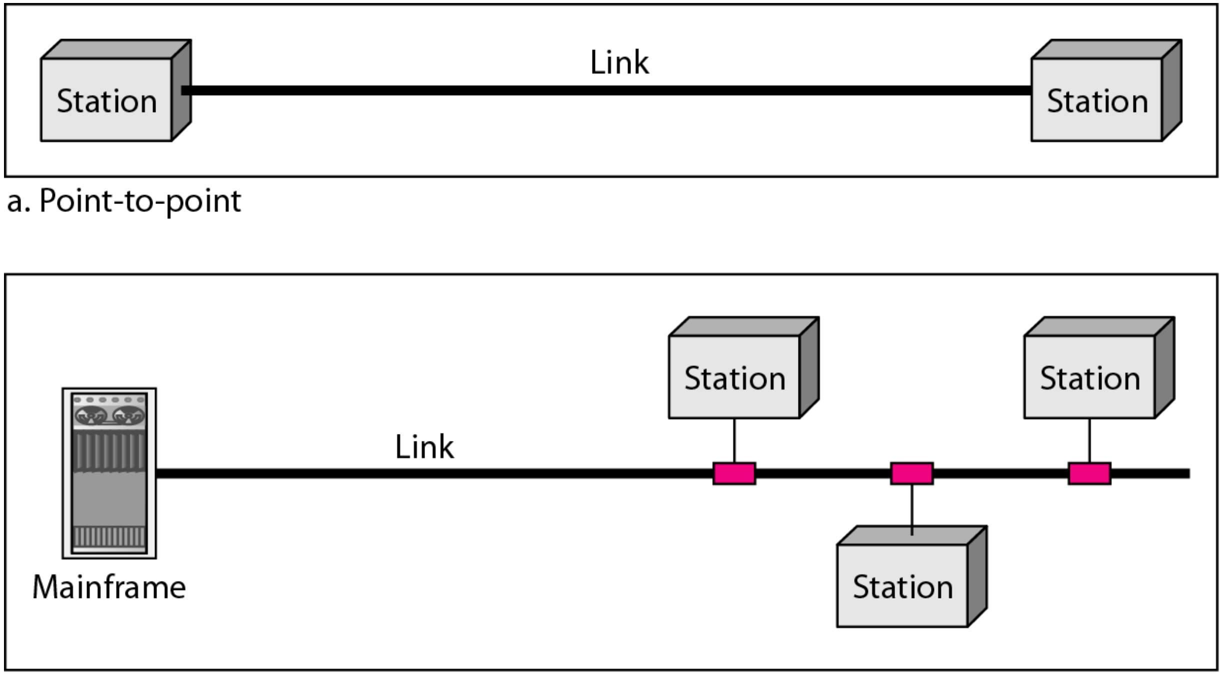
c. Full-duplex

NETWORKS

- A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- Network Criteria
  - Performance
    - Mostly measured by throughput and delay
  - Reliability
    - The frequency of failure
    - Recovery time from a failure
  - Security
    - Protecting data from
      - unauthorized access
      - Damage

Type of Connection

- Point-to-Point
- Multipoint (multi-drop)

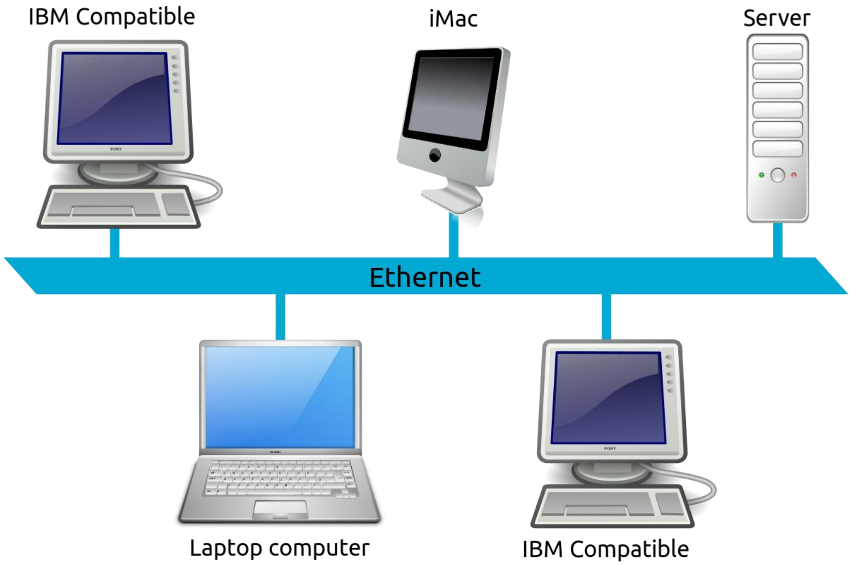


a. Point-to-point

b. Multipoint

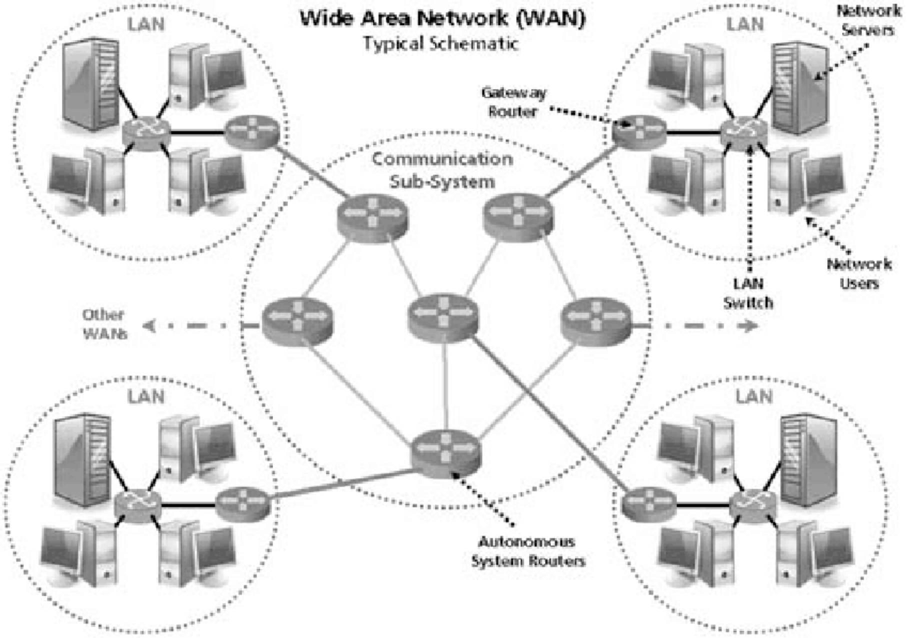
Common Network Types

- Local Area Network (LAN)
  - Contains printers, servers and computers
  - Systems are close to each other
  - Contained in one office or building
  - Organizations often have several LANS



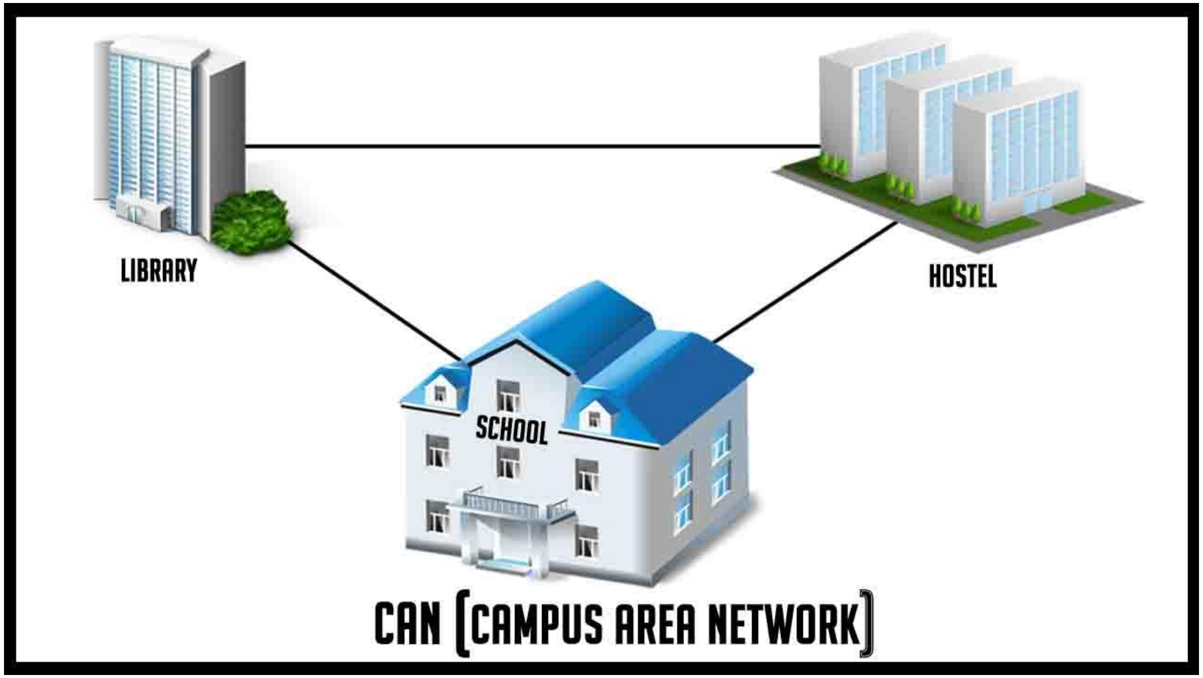
Common Network Types

- Wide Area Networks (WAN)
  - Two or more LANs connected
  - Over a large geographic area
  - Typically use public or leased lines
    - Phone lines
    - Satellite
  - The Internet is a WAN



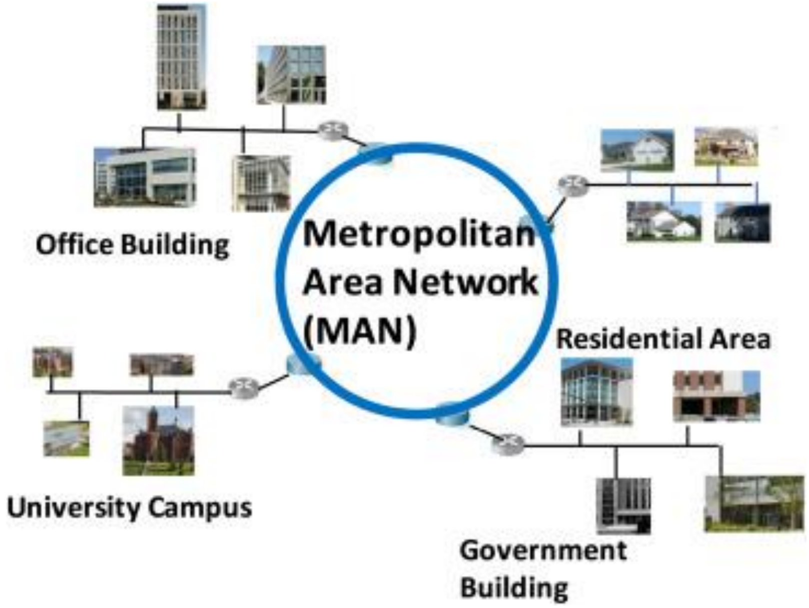
Hybrid Network Types

- Campus Area Networks (CAN)
  - A LAN in one large geographic area
  - Resources related to the same organization
  - Each department shares the LAN



Hybrid Network Types

- Metropolitan Area Network (MAN)
  - Large network that connects different organizations
  - Shares regional resources
  - A network provider sells time



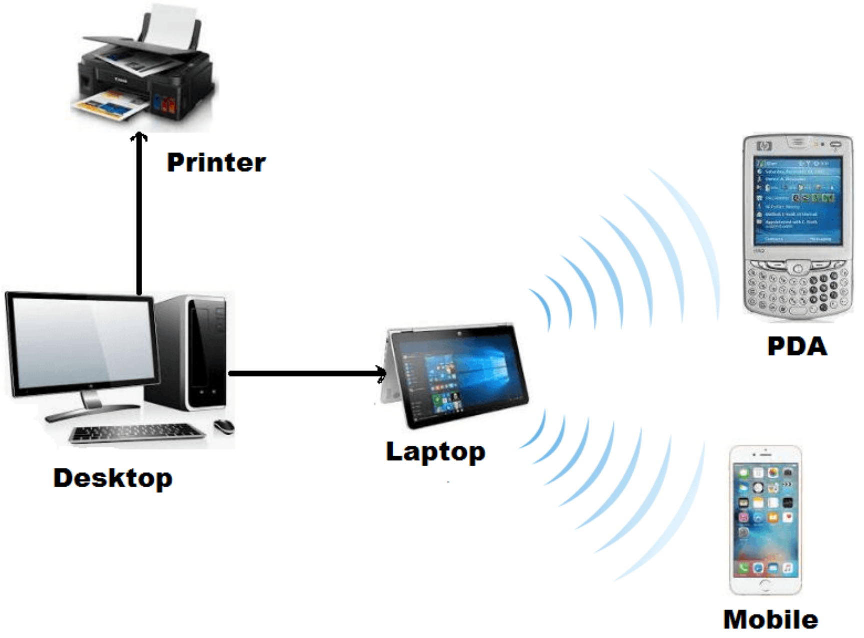
https://www.sciencedirect.com/topics/computer-science/metropolitan-area-networks

Hybrid Network Types

- Home Area Network (HAN)
  - Small scale network
  - Connects computers and entertainment appliances
  - Found mainly in the home

Hybrid Network Types

- Personal Area Network (PAN)
  - Very small scale network
  - Range is less than 2 meters
  - Cell phones, PDAs, MP3 players



Physical Topology

- Mesh topology
- Star topology
- Bus topology
- Ring topology
- Hybrid topology

LAN topologies

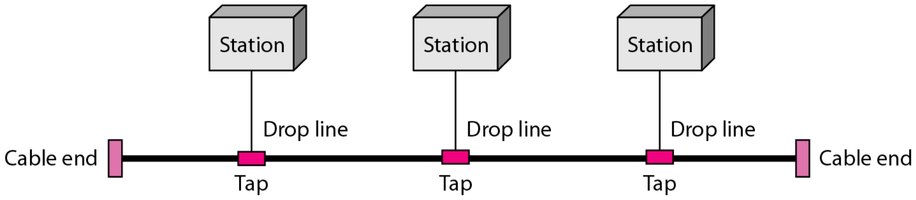
- Physical
  - Describes the geometric arrangement of components that make up the LAN
- Logical
  - Describes the possible connections between pairs of networked end-points that can communicate

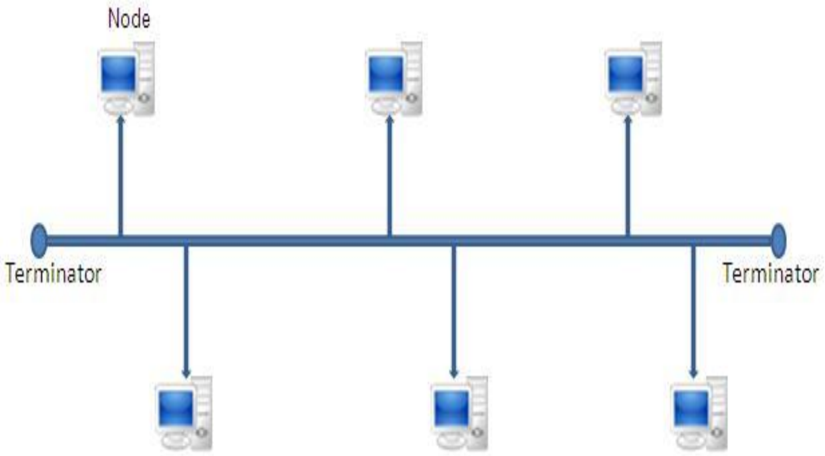
LAN Topologies(Physical)

1) Bus
2) Star
3) Ring
4) Switched
5) Daisy chains
6) Hierarchies

Bus topology

- All networked nodes are interconnected, peer to peer, using a single, open-ended cable
- Both ends of the bus must be terminated with a terminating resistor to prevent signal bounce





Advantages of Bus topology

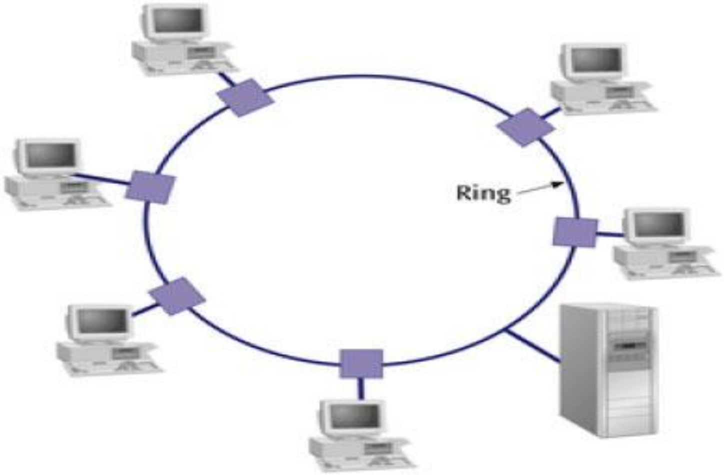
1) Easy to implement and extend
2) Well suited for temporary networks that must be set up in a hurry
3) Typically the least cheapest topology to implement
4) Failure of one station does not affect others

Disadvantages of Bus topology

1) Difficult to administer/troubleshoot
2) Limited cable length and number of stations
3) A cable break can disable the entire network; no redundancy
4) Maintenance costs may be higher in the long run
5) Performance degrades as additional computers are added

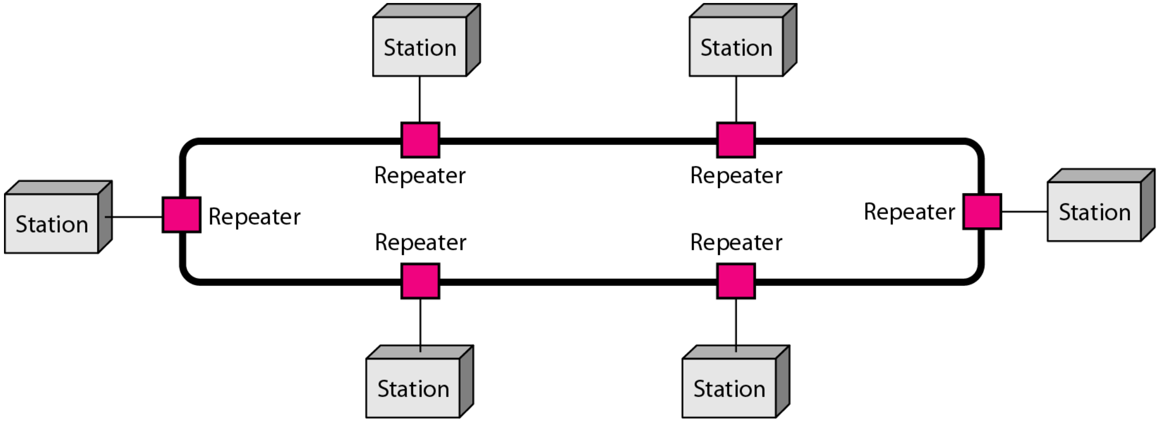
Ring topology

- started out as a simple peer-to-peer LAN topology
- Each networked workstation had two connections: one to each of its nearest neighbors
- Data was transmitted unidirectionally around the ring
- Sending and receiving of data takes place by the help of TOKEN



Token Passing

- Token contains a piece of information which along with data is sent by the source computer
- This token then passes to next node, which checks if the signal is intended to it
  - If yes, it receives it and passes the empty to into the network
  - otherwise passes token along with the data to next node
- IEEE 802.5 Token Ring, MAN



Advantages of Ring topology

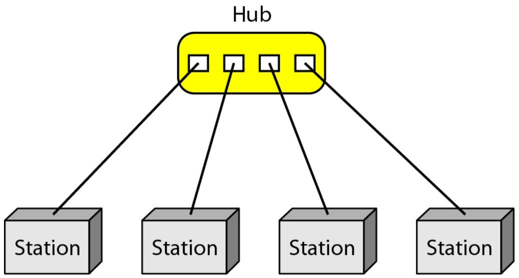
1) This type of network topology is very organized
2) Performance is better than that of Bus topology
3) No need for network server to control the connectivity between workstations
4) Additional components do not affect the performance of network
5) Each computer has equal access to resources

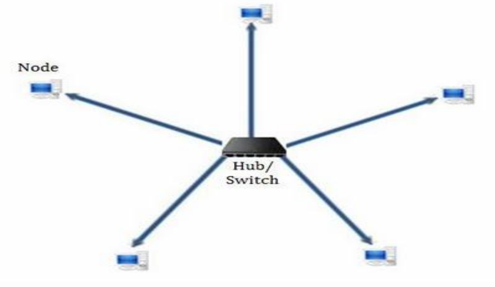
Disadvantages of Ring topology

1) Each packet of data must pass through all the computers between source and destination, slower than star topology
2) If one workstation or port goes down, the entire network gets affected
3) Network is highly dependent on the wire which connects different components

Star topology

- Have connections to networked devices that "radiate" out form a common point
- Each networked device in star topology can access the media independently
- Have become the dominant topology type in contemporary LANs
- Stars have made buses and rings obsolete in LAN topologies
- High speed LAN





Advantages of star topology

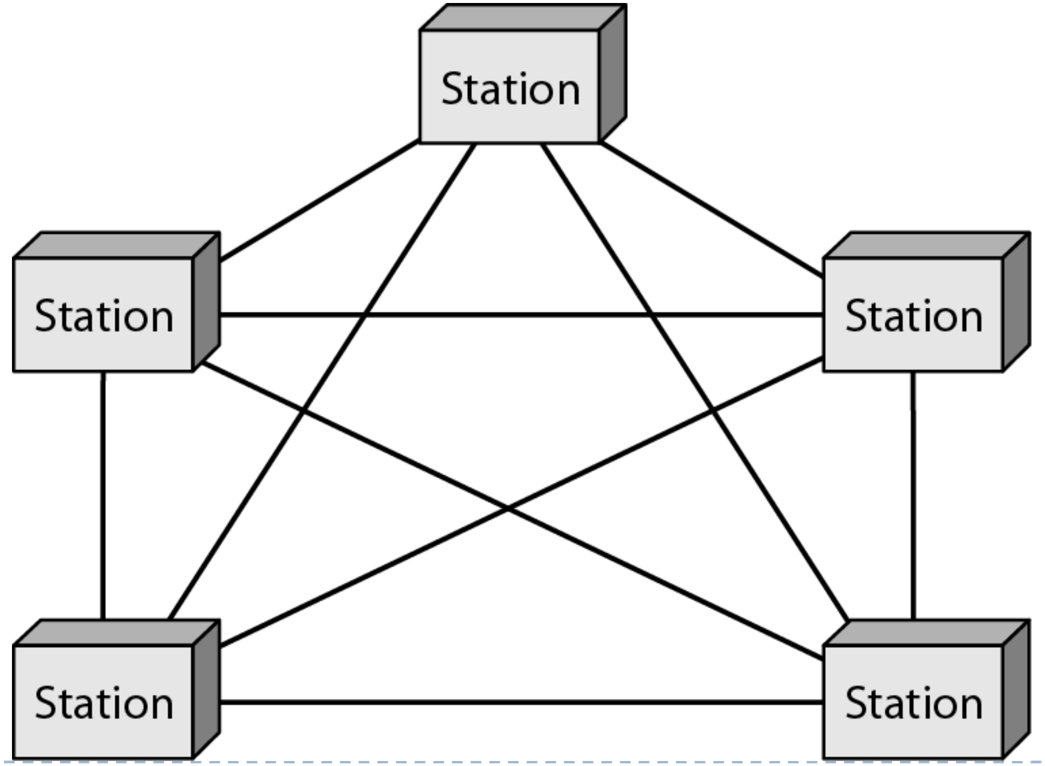
1) Compared to Bus topology it gives far much better performance
2) Easy to connect new nodes or devices
3) Centralized management. It helps in monitoring the network
4) Failure of one node or link doesn’t affect the rest of network

Disadvantages of star topology

1) If central device fails whole network goes down
2) The use of hub, a router or a switch as central device increases the overall cost of the network
3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

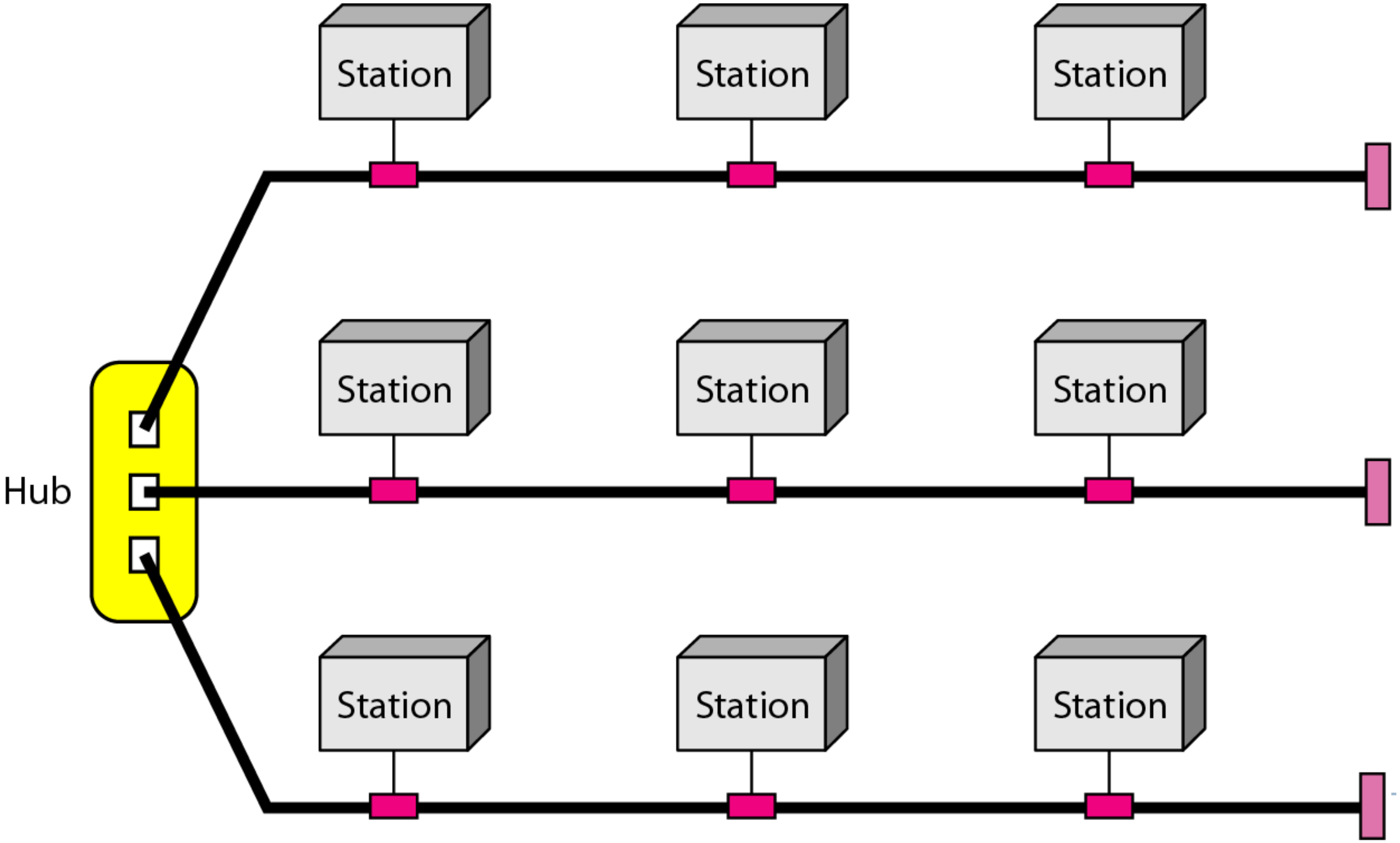
Mesh Topology

- Advantage v. Disadvantage
- Connection of telephone regional offices



Hybrid Topology

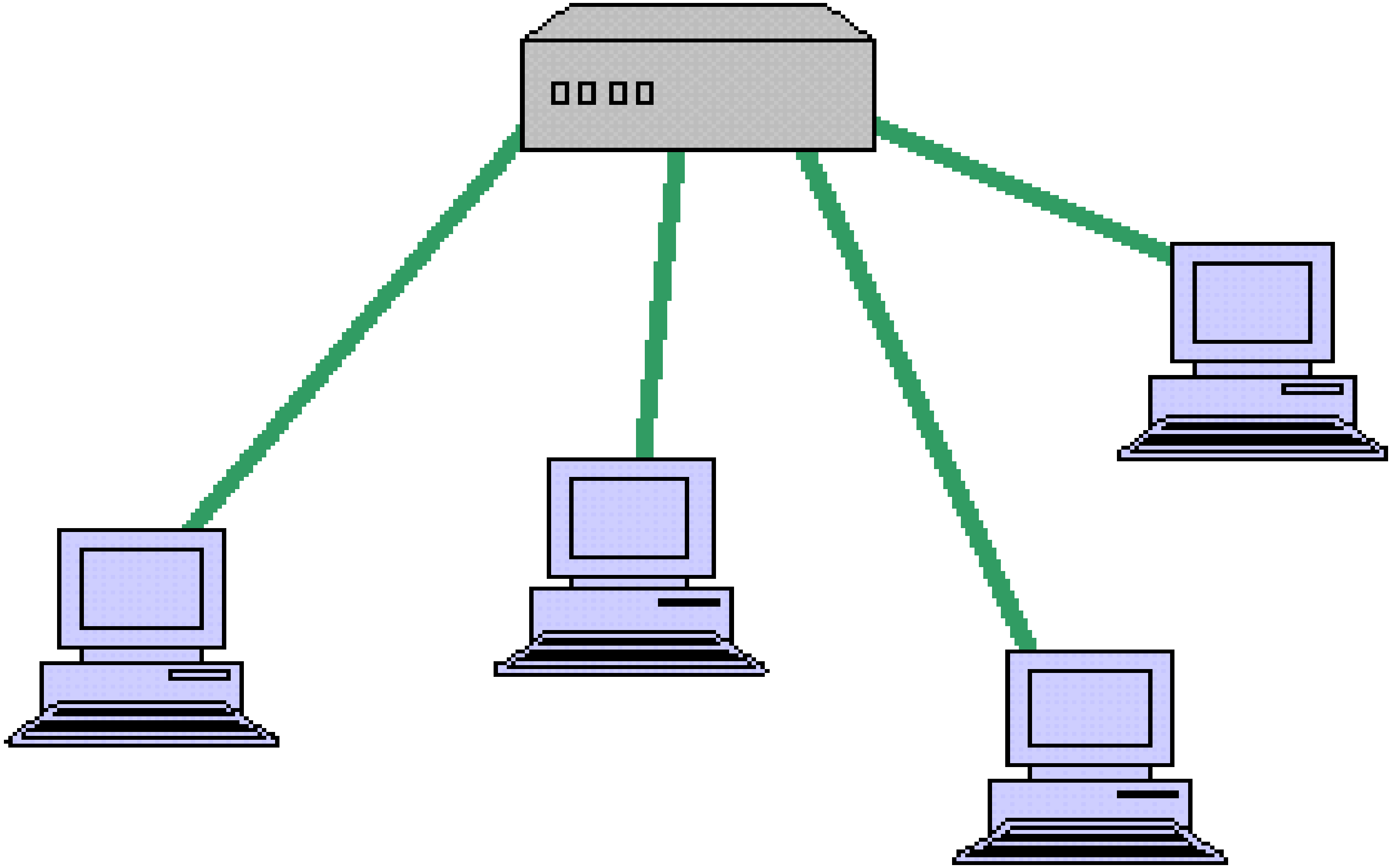
- Combination of two or more network topology



Switched topology

- A switch is a multiport, Data Link Layer device
- A switch "learns" Media Access Control addresses and stores them in an internal lookup table
- Temporary, switched paths are created between the frame's originator and its intended recipient, and the frames are forwarded along the temporary path
- Switched topology features multiple connections to a switching hub/Switch
- Each port, and the device to which it connects, has its own dedicated bandwidth

Switched topology



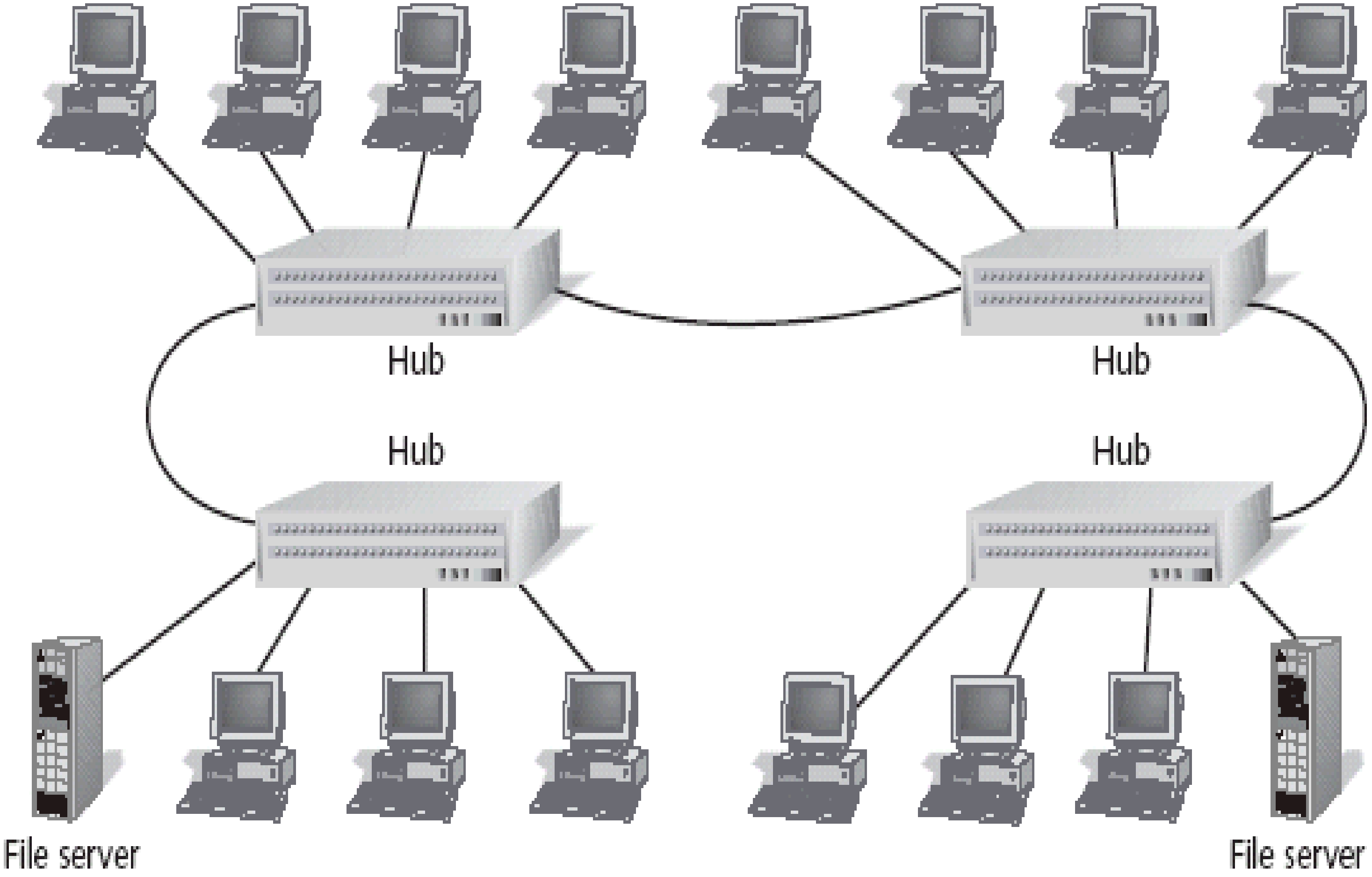
Advantages/Disadvantages of a Switched topology

- Advantage:
  - Can improve LAN performance:
    - increase the aggregate bandwidth available throughout the network
    - reducing the number of devices forced to share each segment of bandwidth
- Disadvantage:
  - Large switched implementations do not isolate broadcasts

Daisy chains

- Developed by serially interconnecting all the hubs of a network
- This simple approach uses ports on existing hubs for interconnecting the hubs
- Daisy chains are easily built and don’t require any special administrative skills
- Daisy chains were, historically, the interconnection method of choice for emerging, first-generation LANs

Daisy chains



Disadvantage of Daisy chain

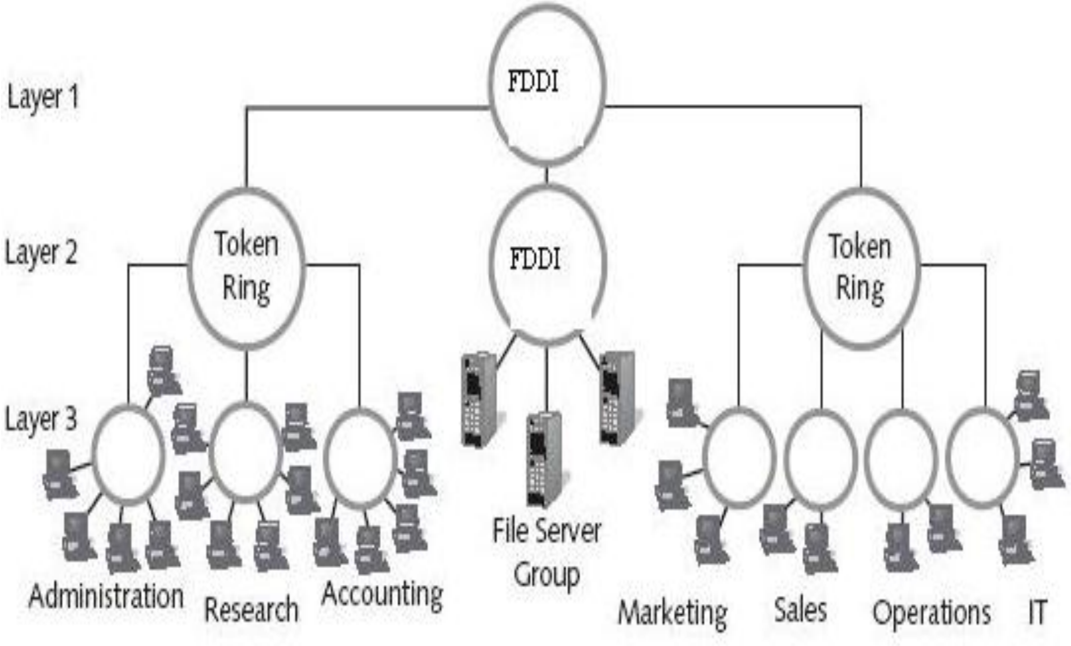
- Increases the number of connections, and therefore the number of devices, on a LAN. Too many devices competing for the same amount of bandwidth can create collisions and quickly incapacitate a LAN

Hierarchies

- Hierarchical topologies consist of more than one layer of hubs. Each layer serves a different network function
- The bottom tier is reserved for user station and server connectivity. Higher-level tiers provide aggregation of the user-level tier
- A hierarchical arrangement is best suited for medium-to-large-sized LANs that must be concerned with scalability of the network and with traffic aggregation

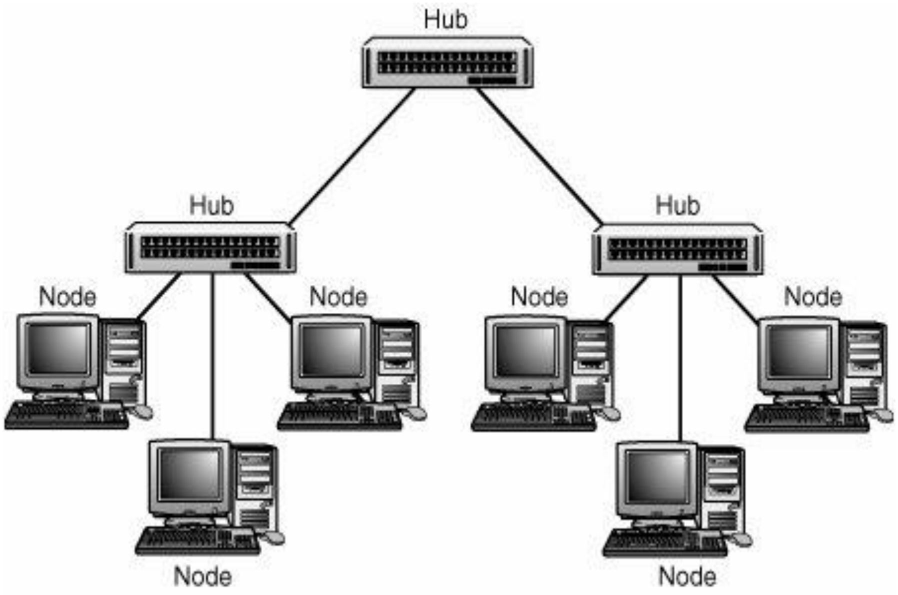
Hierarchical rings

- Ring networks can be scaled up by interconnecting multiple rings in a hierarchical fashion
- User station and server connectivity can be provided by as many limited size rings as are necessary to provide the required level of performance
- A second-tier ring, either Token Ring or Fiber Distributed Data Interface (FDDI), can be used to interconnect all the user level rings and to provide aggregated access to the Wide Area Network (WAN)



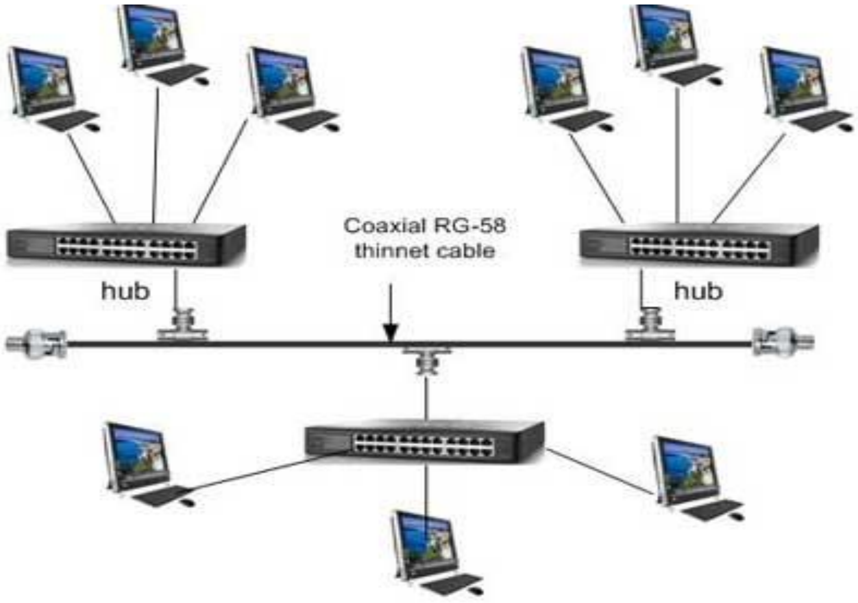
Hierarchical stars

- Star topologies, can be implemented in hierarchical arrangements of multiple stars
- Hierarchical stars can be implemented as a single collision domain or segmented into multiple collision domains using switches, routers or bridges

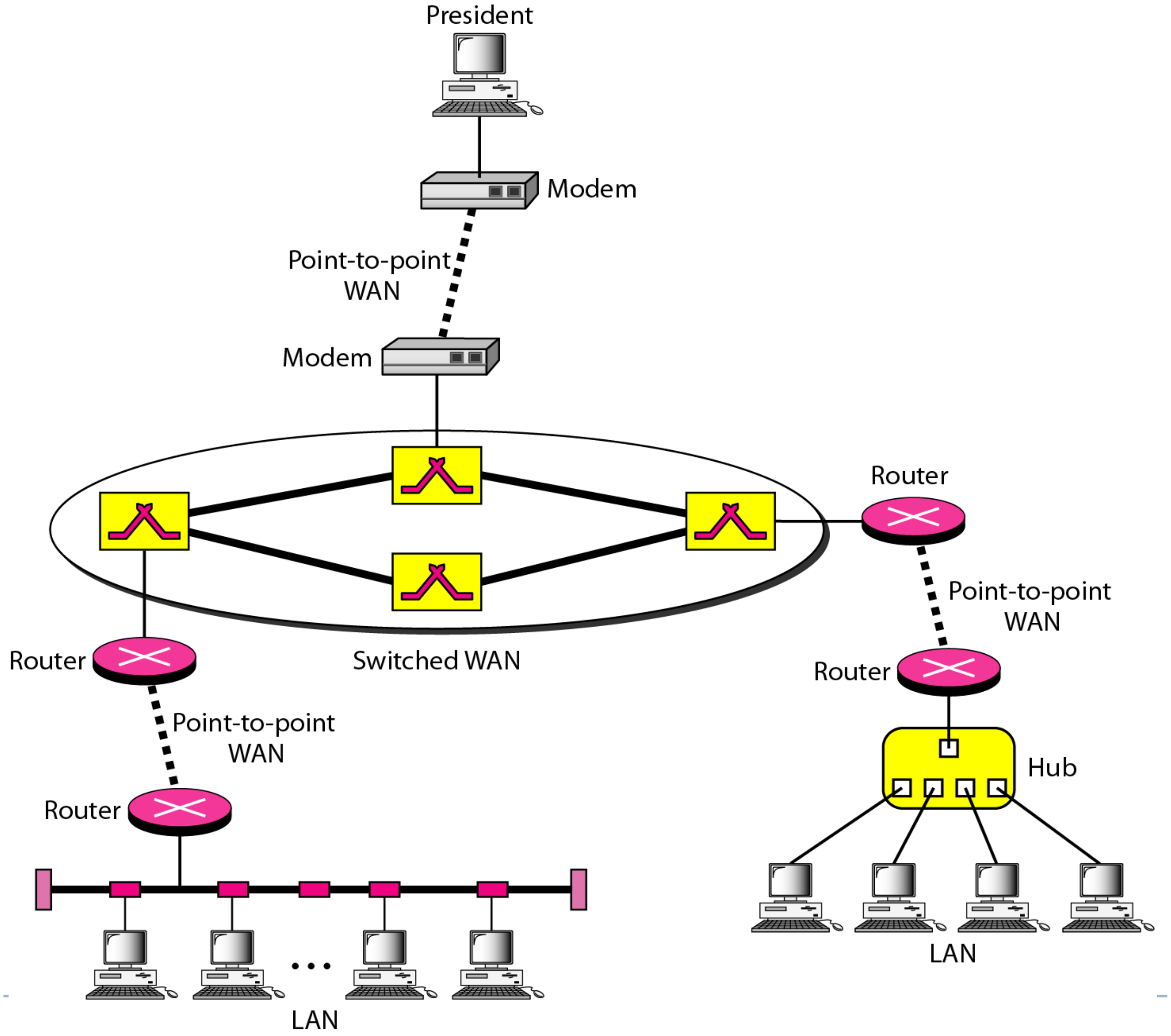


Hierarchical combinations

- Overall network performance can be enhanced by not force-fitting all the functional requirements of the LAN into a single solution
- Today’s high-end switching hubs enable you to mix multiple technologies



Heterogeneous Network



WAN Topologies

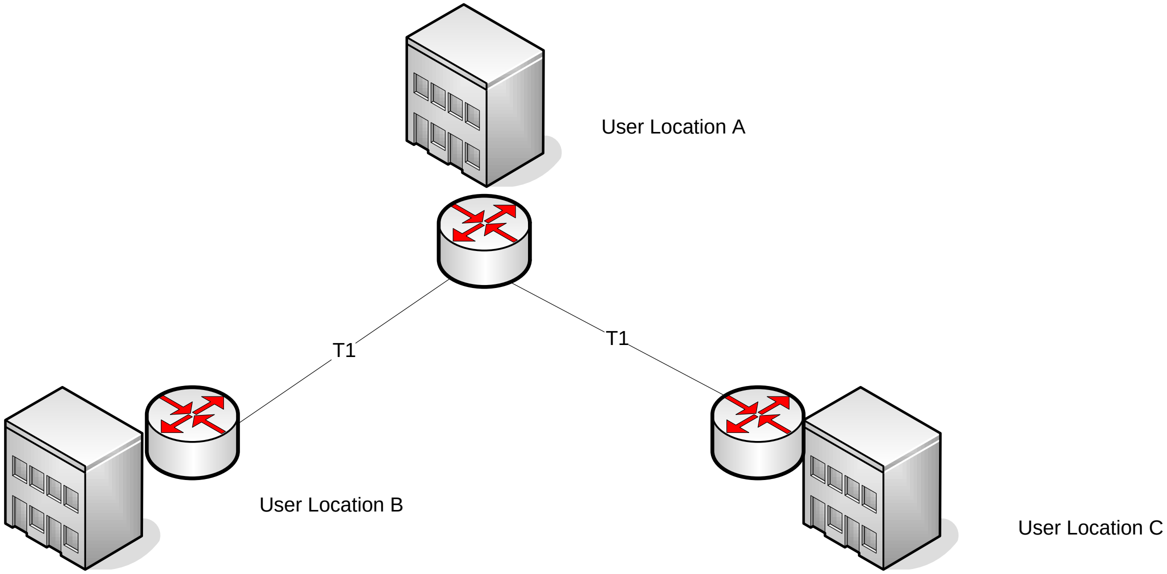
- The topology of a WAN describes the way the transmission facilities are arranged relative to the locations that they interconnect
- Numerous topologies are possible, each one offering a different mix of cost, performance and scalability

WAN Topologies

1) Peer-to-peer WANs
2) Ring WANs
3) Star WANs
4) Full-mesh WANs
5) Partial-mesh WANs
6) Two-tiered
7) Three-tiered
8) Hybrids

Peer-to-peer topology

- A peer-to-peer WAN can be developed using leased private lines or any other transmission facility
- This WAN topology is a relatively simple way of interconnecting a small number of sites
- Represents the least-cost solution for WANs that contain a small number of internetworked locations

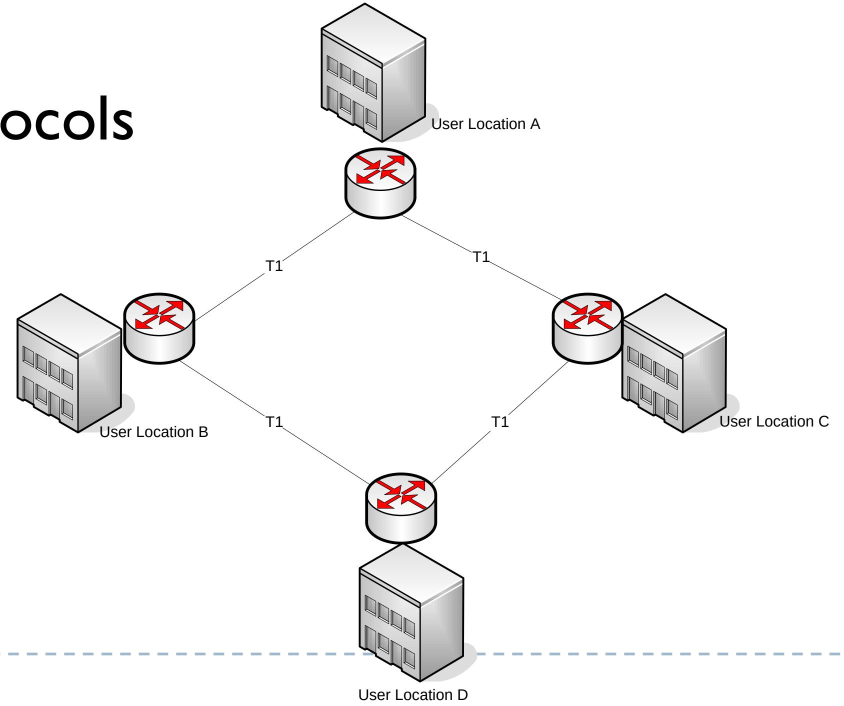


Advantage/Disadvantage of Peer-to-peer

- Advantage:
  - It is inexpensive relative to other options
- Disadvantages:
  - They don’t scale very well. As additional locations are introduced to the WAN, the number of hops between any given pair of locations remains highly inconsistent and has an upward trend
  - An equipment or facility failure anywhere in a peer-to-peer WAN can split the WAN

Ring topology

- Can be developed fairly easily from a peer-to-peer network by adding one transmission facility and an extra port on two routers
- A ring-shaped WAN constructed with point-to-point transmission facilities can be used to interconnect a small number of sites and provide route redundancy at a potentially minimal incremental cost
- Can use dynamic routing protocols

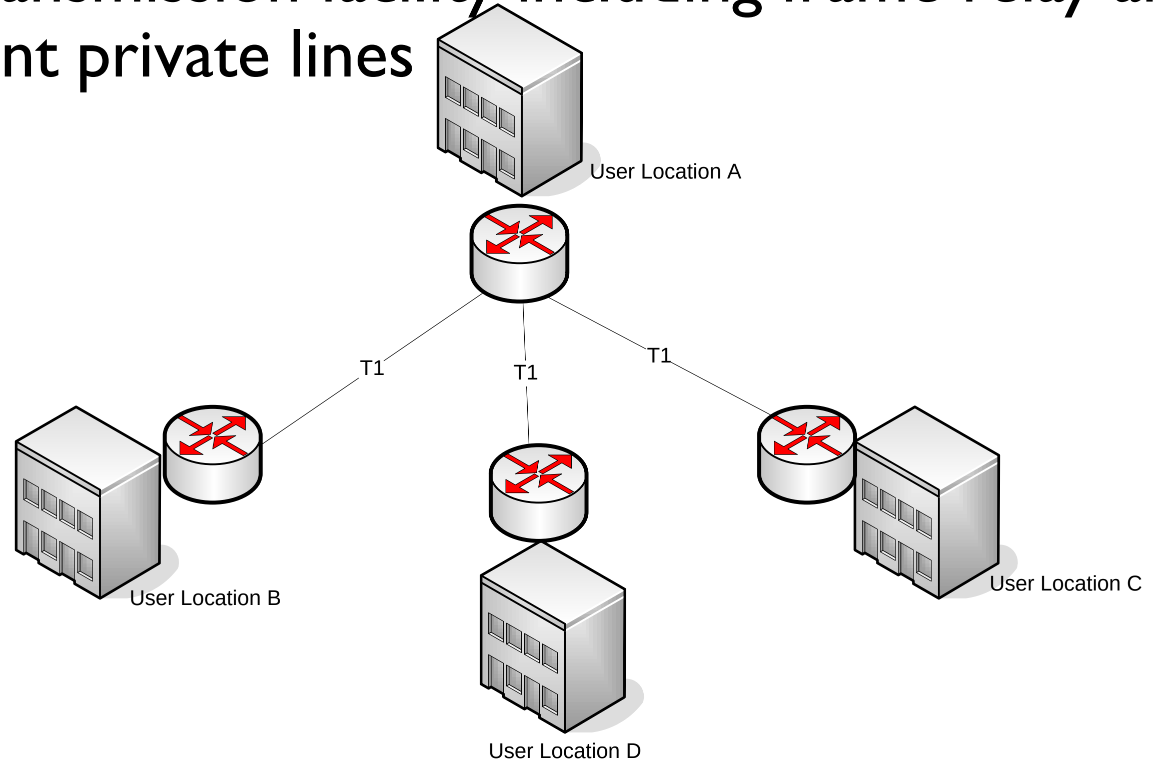


Advantages/Disadvantages of Ring topology

- Advantages:
  - It provides alternative routes
  - It is less expensive than all but the peer-to-peer WAN
- Disadvantages:
  - Depending on the geographic dispersion of the locations, adding an extra transmission facility to complete the ring may be cost prohibitive
  - Rings are not very scalable

Star network Topology

- constructed by homing all locations into a common location
- The star topology can be constructed using almost any dedicated transmission facility including frame relay and point-to-point private lines



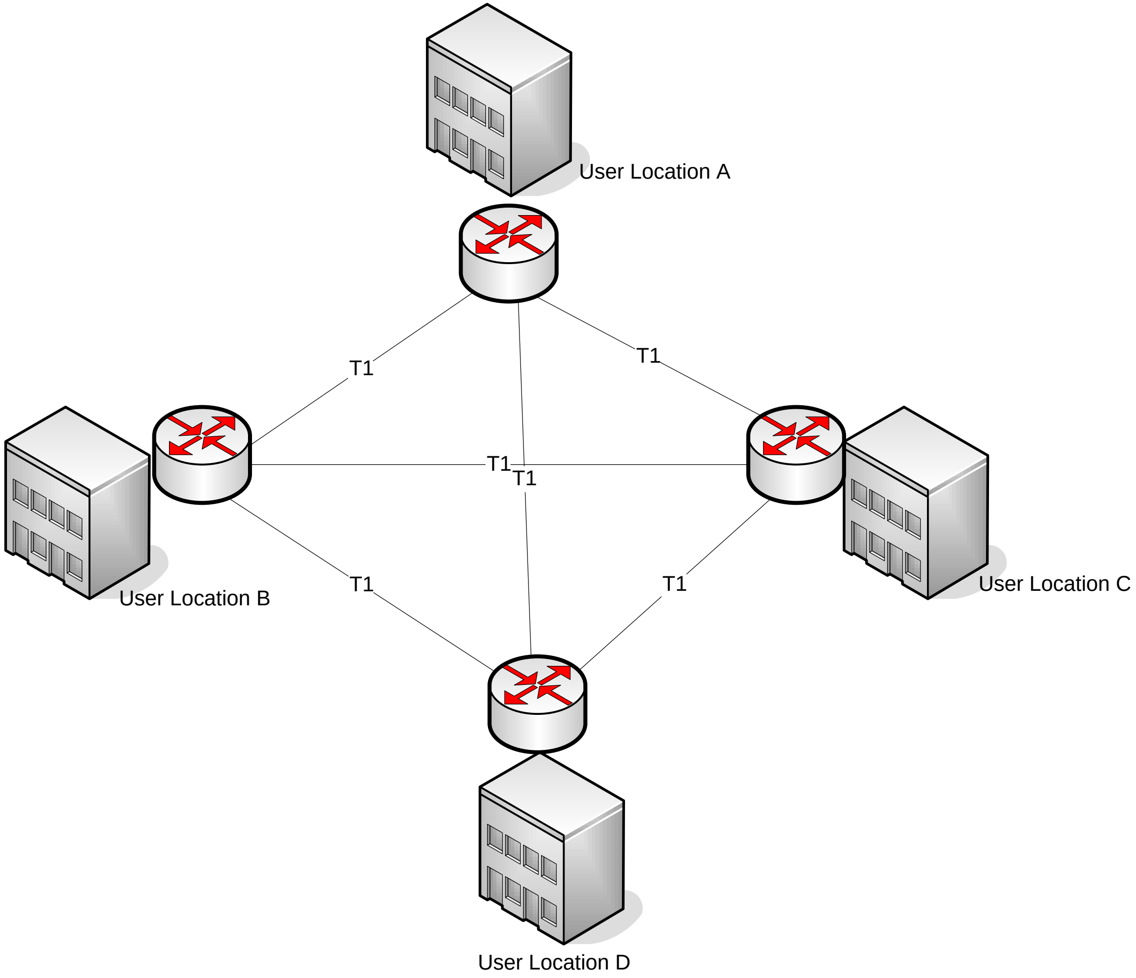
Advantages/Disadvantages of star topology

- Advantages:
  - More scalable than a peer-to-peer or ring network
  - Improved network performance. Hop count of three
- Disadvantages:
  - It creates a single point of failure
  - There is no route redundancy

Full-mesh topology

- This topology features the ultimate reliability and fault tolerance
- Every networked node is directly connected to every other networked node
- Redundant routes to each location are plentiful, hence static routing impractical.
- Use dynamic routing protocols
- One application would be to provide interconnectivity for a limited number of routers that require high network availability
- Another potential application is to fully mesh just parts of the WAN, such as the backbone of a multitiered WAN or tightly coupled work centers

Full-mesh topology

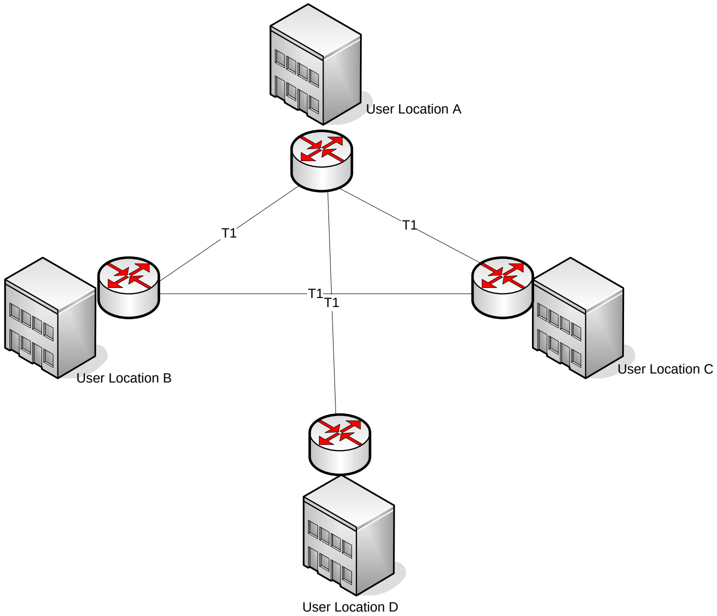


Advantages/Disadvantages of full-mesh

- Advantages:
  - Minimizes the number of hops between any two network-connected machines
  - Can be built with virtually any transmission technology
- Disadvantages:
  - These WANs can be fairly expensive to build
  - A finite (although substantial) limit on the scalability of the network

Partial-mesh topology

- Partial meshes are highly flexible topologies that can take a variety of very different configurations
- The routers are much more tightly coupled than any of the basic topologies but are not fully interconnected, as would be the case in a fully meshed network
- A partially meshed WAN topology is readily identified by the almost complete interconnection of every node with every other node in the network

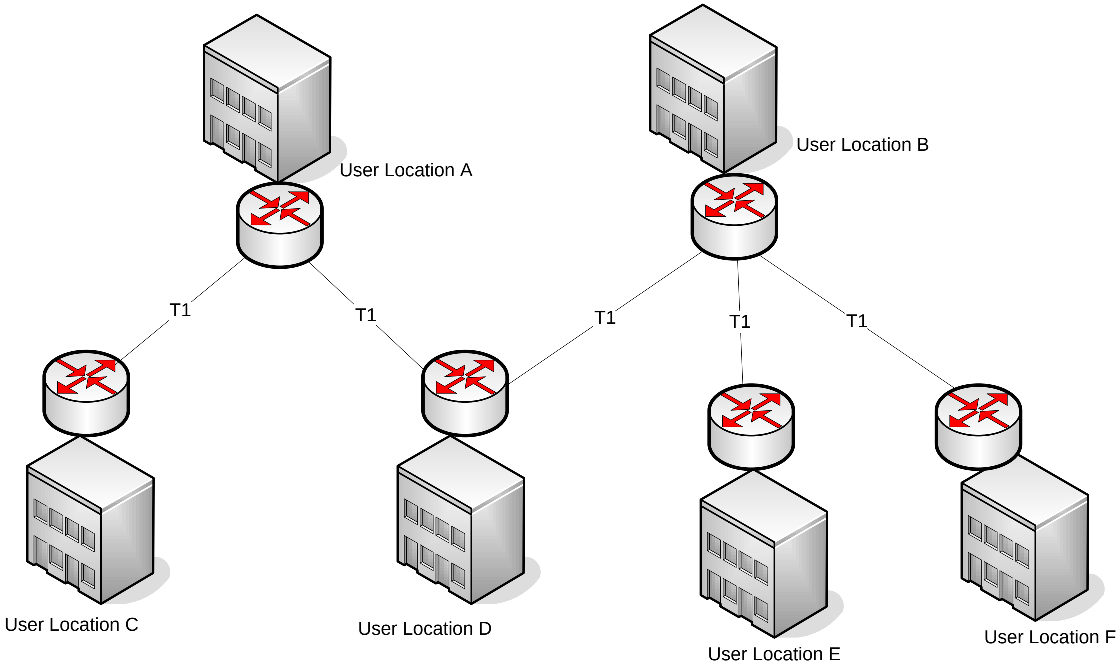


Advantages of partial-mesh

- Partial meshes offer the capability to minimize hops for the bulk of the WAN's users
- Unlike fully meshed networks, a partial mesh can reduce the startup and operational expenses by not interconnecting low-traffic segments of the WAN, hence more affordable and scalable

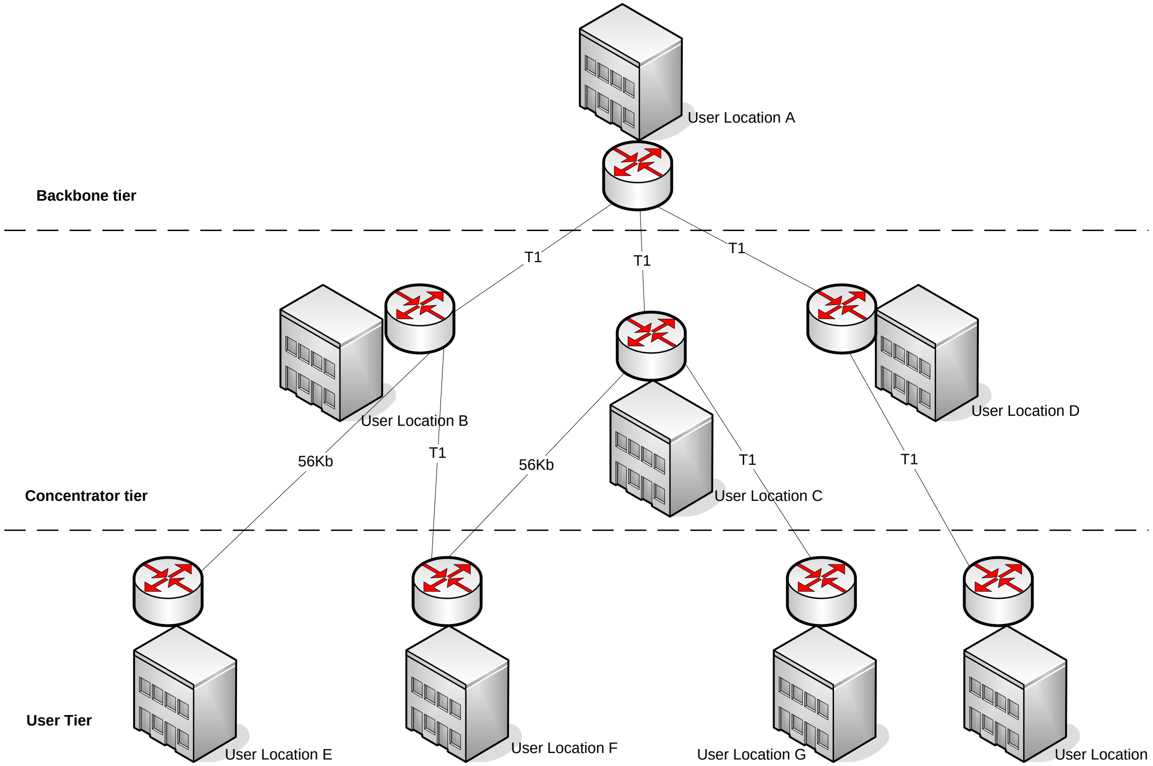
Two-tiered topology

- A two-tiered topology is a modified version of the basic star topology. Rather than single concentrator routers, two or more routers are used
- A two-tiered WAN constructed with dedicated facilities offers improved fault tolerance over the simple star topology without compromising scalability



Three-tiered topology

- WANs that need to interconnect a very large number of sites, or are built using smaller routers that can support only a few serial connections, may find the two-tiered architecture insufficiently scalable.
- Therefore, adding a third tier may well provide the additional scalability they require

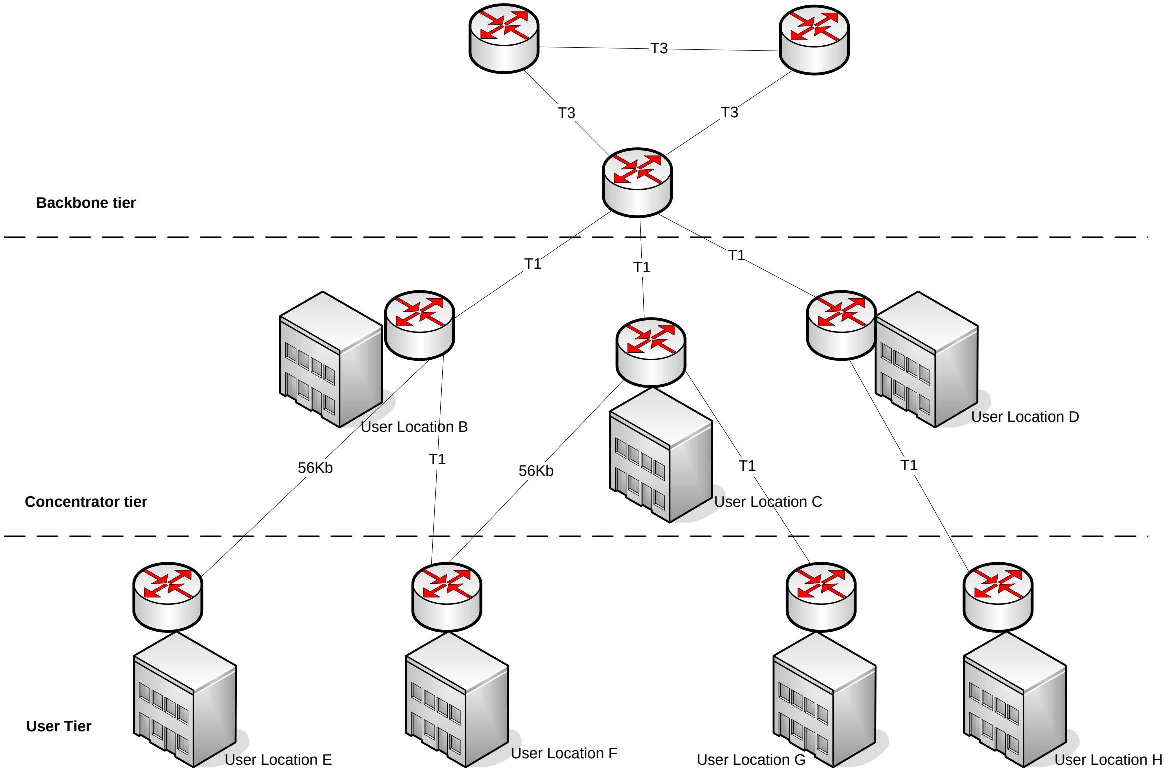


Advantage/Disadvantage of three-tiered

- Advantage:
  - A three-tiered WAN constructed with dedicated facilities offers even greater fault tolerance and scalability than the two-tiered topology
- Disadvantage:
  - Three-tiered networks are expensive to build, operate and maintain

Hybrid topologies

- Hybridization of multiple topologies is useful in larger, more complex networks
- Multitiered networks, in particular, lend themselves to hybridization. A multitiered WAN can be hybridized by fully or partially meshing the backbone tier of routers
- An effective hybrid topology may be developed in a multitiered WAN by using a fully meshed topology for the backbone nodes only



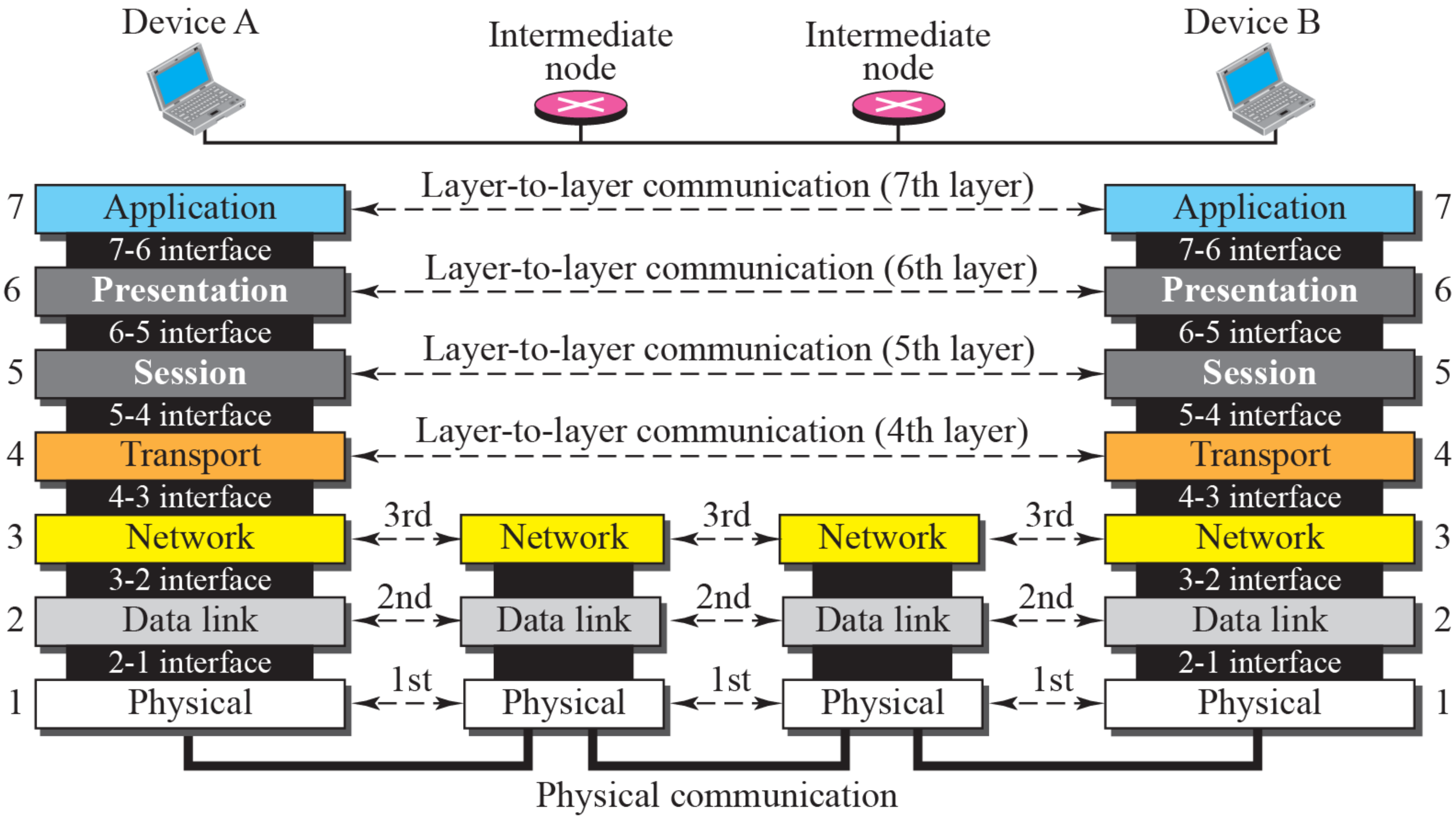
The Internet

- The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

PROTOCOLS AND STANDARDS

- Protocols
  - A set of rules to define
    - What is communicated
    - How it is communicated
    - When it is communicated
- Standards
  - To guarantee national/international interoperatibility of data and telecommunication technology
  - Regardless of equipment manufacturers
  - ISO, ITU, ANSI, IEEE, …
  - Internet standards are maintained by IETF for publishing RFC (Request for Comments)
    - http://www.ietf.org/rfc.html

OSI layers


Device A
Intermediate node
Intermediate node
Device B
Layer-to-layer communication (7th layer)
Layer-to-layer communication (6th layer)
Layer-to-layer communication (5th layer)
Layer-to-layer communication (4th layer)
7 Application 7
7-6 interface
6 Presentation 6
6-5 interface
5 Session 5
5-4 interface
4 Transport 4
4-3 interface
3 Network 3
3-2 interface
2 Data link 2
2-1 interface
1 Physical 1
3rd
2nd
1st
Network
Data link
Physical
Physical communication

Physical layer

- defines the procedures and functions that physical devices and interfaces have to perform for transmission occur.
- The physical layer is concerned with the following:
  - Physical characteristics of interfaces and media:
  - Representation of the bits
  - Data rate, the number of bits sent each second.
  - Line configuration, Point to point or multipoint configuration.
  - Physical topology
  - Transmission Mode : Simplex, half duplex or full duplex

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery.
- The Data Link layer is concerned with the following:
  - Framing.
  - Physical addressing, each node has its unique address.
  - Flow Control.
  - Access Control.
  - Error control, normally achieved through a trailer to the end of the frame.

Network Layer

- Is responsible for the source-to-destination delivery of a **packet** possible **across multiple networks.**
- Functions:
  - Logical addressing.
  - Routing, It determines which path the data should take based on network conditions, priority of service, and other factors.

Transport Layer

- The transport layer is responsible for process-to-process delivery of the entire message.

- Makes sure that the data arrives without errors, in the proper sequence and in a reliable condition.

- Functions:
  - Port addressing,The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
  - Segmentation and reassembly: a message is divided into transmittable segments, each having a sequence number
  - Connection control:The transport layer can be either connectionless or connection-oriented.
  - Flow control
  - Error control

Session Layer

- the *session layer*, allows two applications on different computers to open, use, and close a connection called a *session*.
  - (A session is a highly structured dialog between two workstations.)

- Functions:
  - **Dialog control**
    - It also makes sure the session is orderly, establishing which node transmits first, how long it can transmit, and what to do in case of an error.
    - It performs name-recognition and other functions, such as security, that are needed to allow two applications to communicate over the network.
  - **Synchronization**
    - The session layer synchronizes user tasks by placing **checkpoints** in the data stream.
    - The checkpoints break the data into smaller groups for error detection. It allows information of different streams, perhaps originating from different sources, to be properly combined or synchronized.
      - □ An example application is web conferencing, in which the streams of audio and video must be synchronous to avoid so-called lip synch problems. It ensures that the person displayed on screen is the current speaker.

presentation layer

- The presentation layer is responsible for translation, compression, and encryption.
- **Deals with the actual formatting of the data.**
  - For example, data might be converted from EBCDIC to ASCII formatting so that the receiving node can understand it.

Application Layer

- This layer relates to the services that directly provide user interfaces support user applications or services, such as software for file transfers, database access, and e-mail.
- In other words, it serves as a window through which application processes can access network services.
- The application layer enables the user to access the network.
- This would be the layer that a programmer uses to allow his application to access a network service, such as linking into a database.

Summary of OSI Layers

Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

Need For Protocol Architecture

- data exchange can involve complex procedures, cf. file transfer example
- better if task broken into subtasks
- implemented separately in layers in stack
  - each layer provides functions needed to perform comms for layers above
  - using functions provided by layers below
- peer layers communicate with a protocol

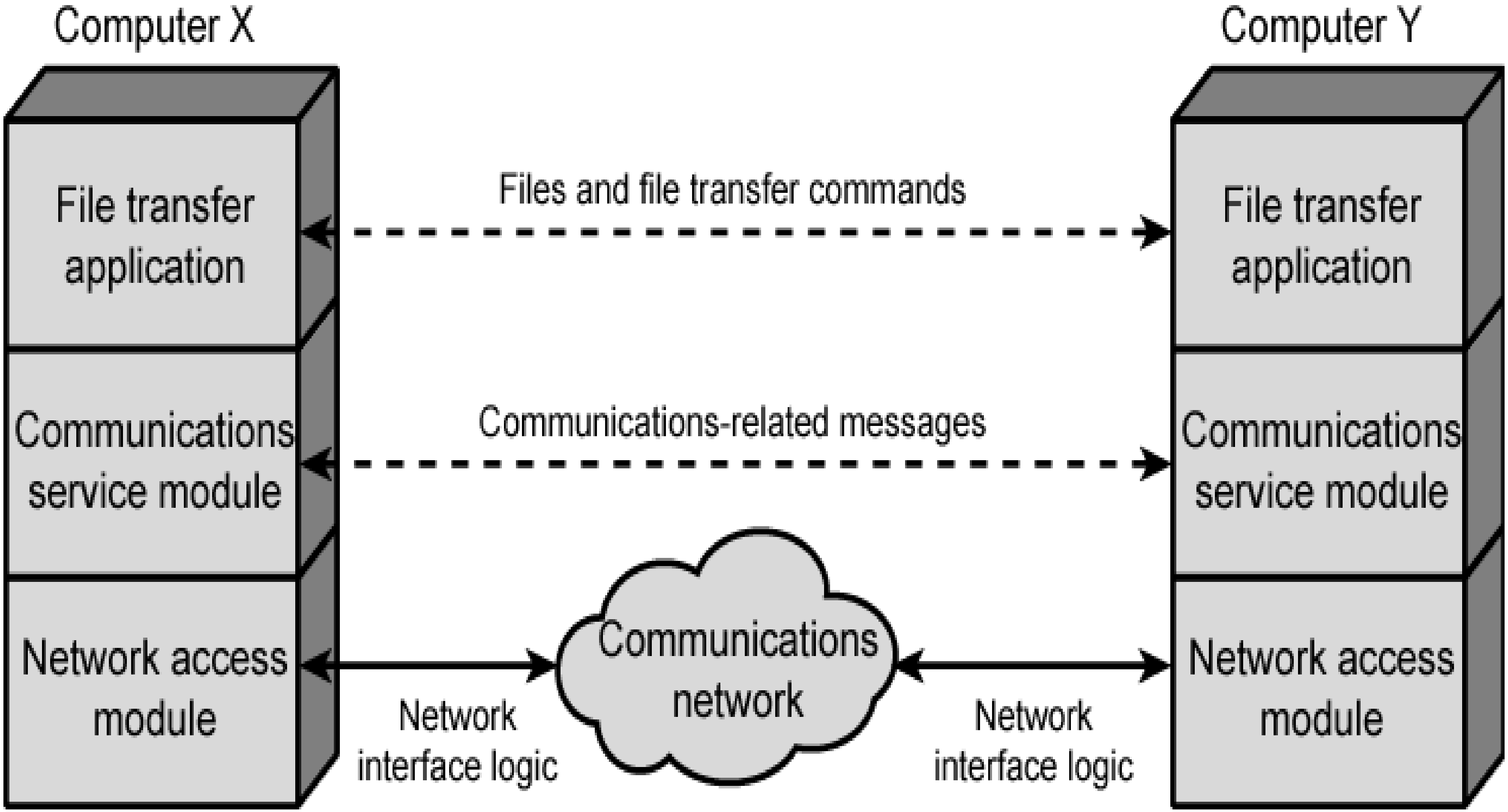
Key Elements of a Protocol

- syntax - data format
- semantics - control info & error handling
- timing - speed matching & sequencing

TCP/IP Protocol Architecture

- developed by US Defense Advanced Research Project Agency (DARPA)
- for ARPANET packet switched network
- used by the global Internet
- protocol suite comprises a large collection of standardized protocols

Simplified Network Architecture


Computer X
Computer Y
File transfer application
Files and file transfer commands
File transfer application
Communications service module
Communications-related messages
Communications service module
Network access module
Communications network
Network access module
Network interface logic
Network interface logic

TCP/IP Layers

- no official model but a working one
  - Application layer
  - Host-to-host, or transport layer
  - Internet layer
  - Network access layer
  - Physical layer

Physical Layer

- concerned with physical interface between computer and network
- concerned with issues like:
  - characteristics of transmission medium
  - signal levels
  - data rates
  - other related matters

Network Access Layer

- exchange of data between an end system and attached network
- concerned with issues like :
  - destination address provision
  - invoking specific services like priority
  - access to & routing data across a network link between two attached systems
- allows layers above to ignore link specifics

Internet Layer (IP)

- routing functions across multiple networks
- for systems attached to different networks
- using IP protocol
- implemented in end systems and routers
- routers connect two networks and relays data between them

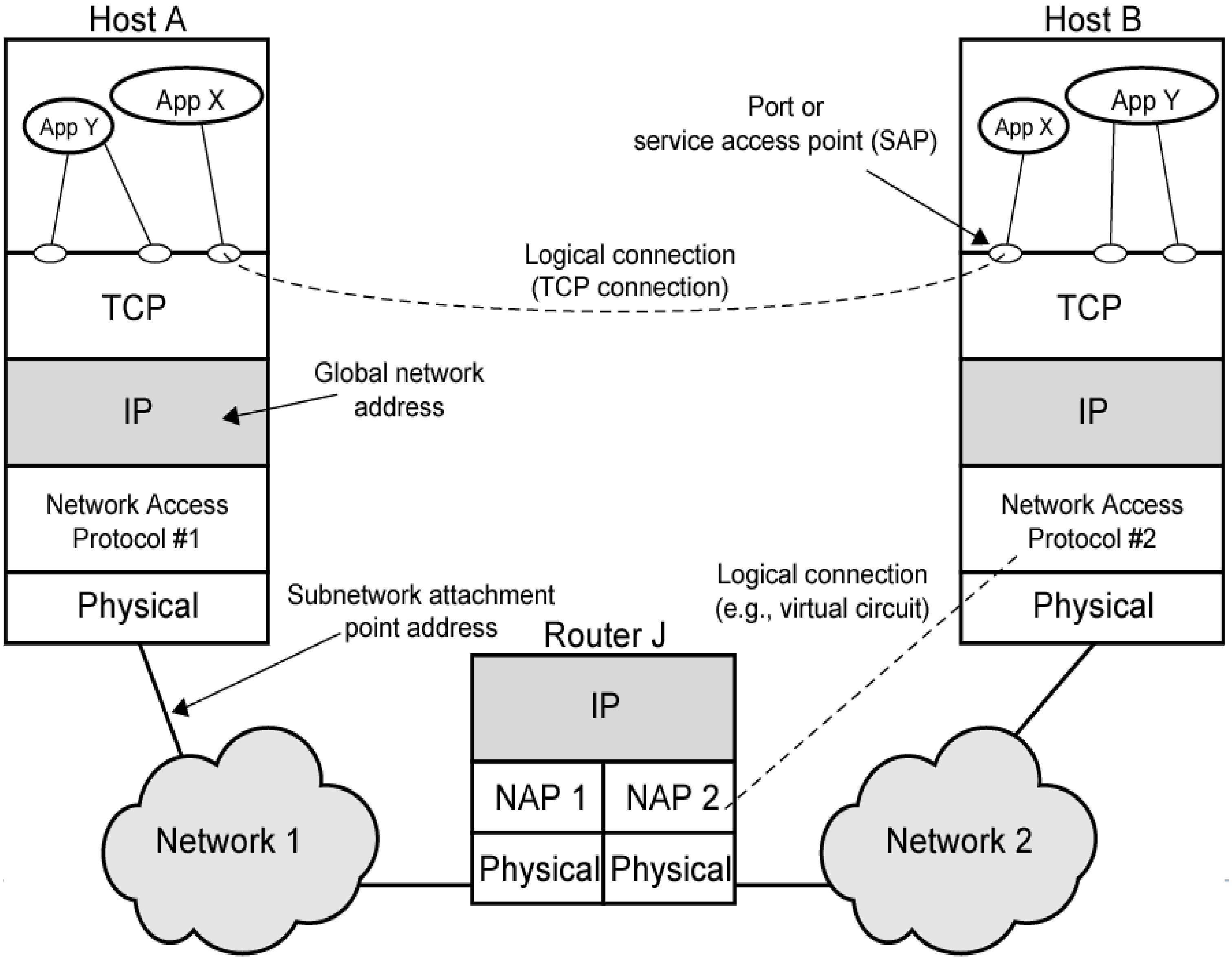
Transport Layer (TCP)

- **host-to-host layer**
- common layer shared by all applications
- provides reliable delivery of data
- in same order as sent
- commonly uses TCP

Application Layer

- provide support for user applications
- need a separate module for each type of application

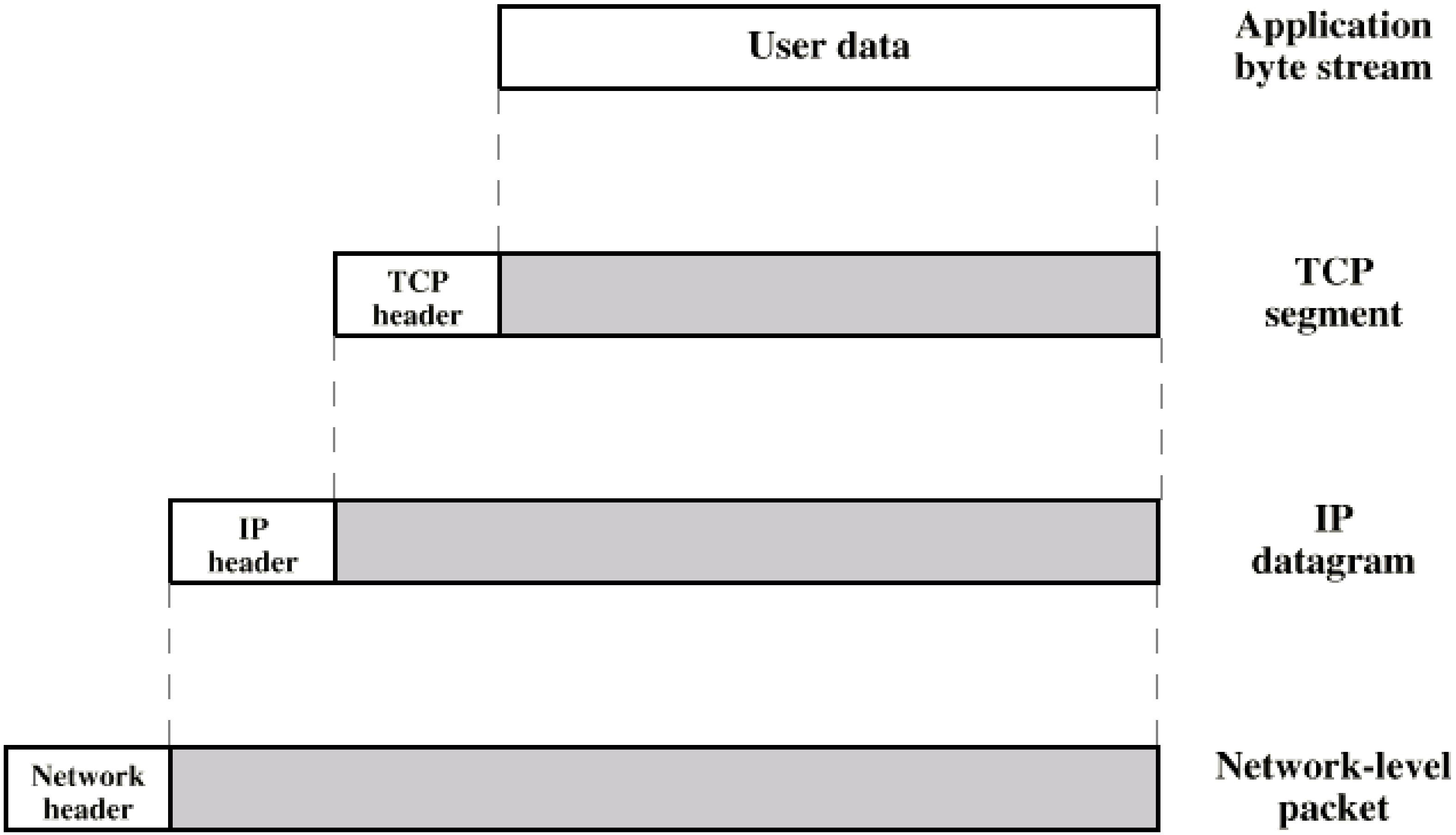
Operation of TCP and IP



Addressing Requirements

- two levels of addressing required
- each host on a subnet needs a unique global network address
  - its IP address
- each application on a (multi-tasking) host needs a unique address within the host
  - known as a port

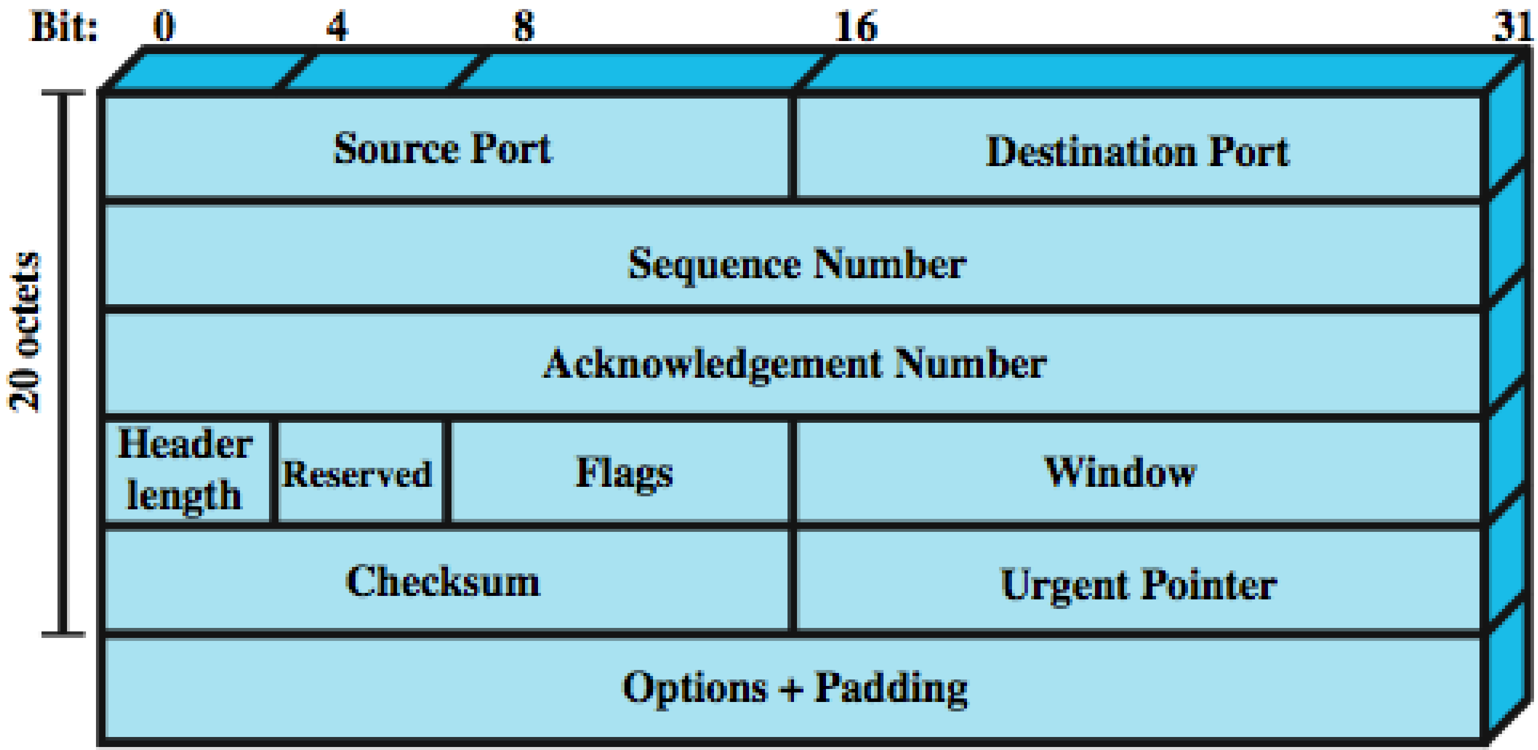
Operation of TCP/IP



Transmission Control Protocol (TCP)

- usual transport layer is (TCP)
- provides a reliable connection for transfer of data between applications
- a TCP segment is the basic protocol unit
- TCP tracks segments between entities for duration of each connection

TCP Header



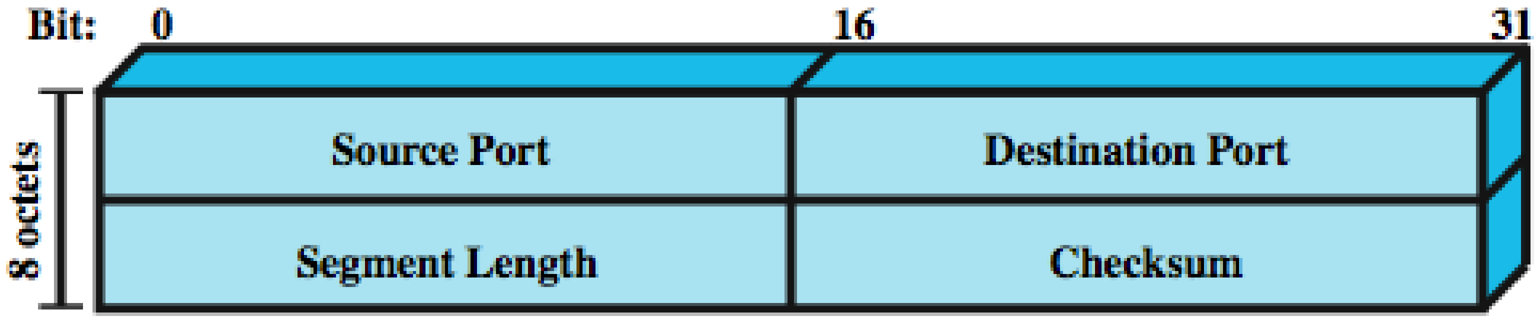
<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>Header length</td><td>Reserved</td><td>Flags</td><td>Window</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Options + Padding</td></tr>
</table>

(a) TCP Header

User Datagram Protocol (UDP)

- an alternative to TCP
- no guaranteed delivery
- no preservation of sequence
- no protection against duplication
- minimum overhead
- adds port addressing to IP

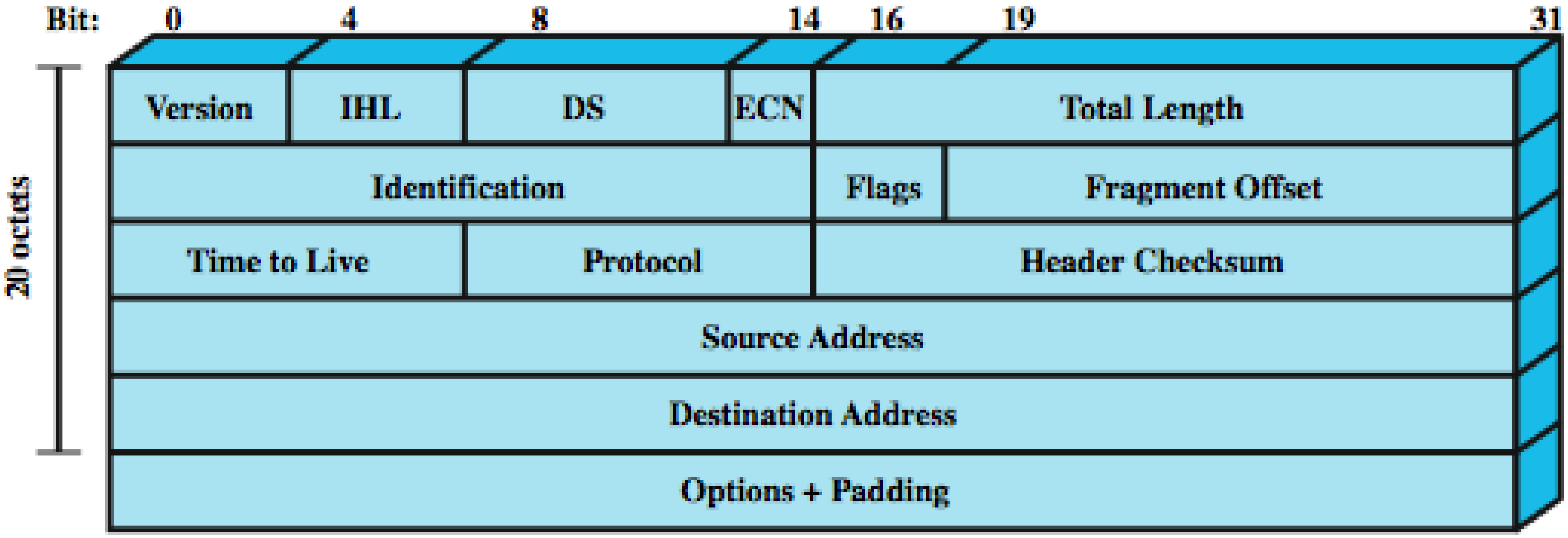
UDP Header



Bit: 0	16 31
Source Port	Destination Port
Segment Length	Checksum

(b) UDP Header

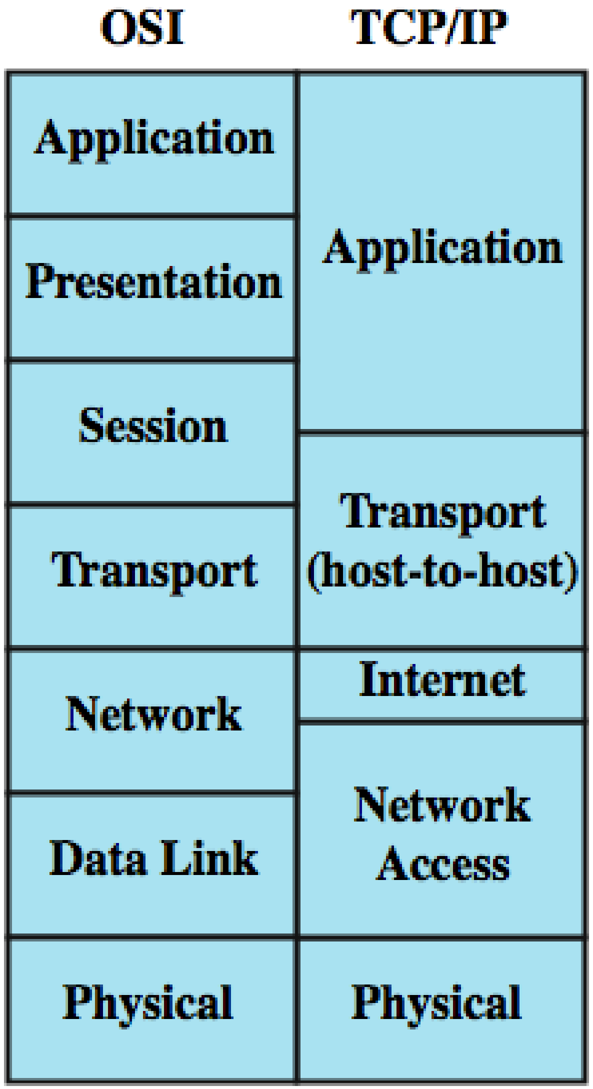
IP Header



(a) IPv4 Header

IPV4 uses a 32-bit address to specify a source or destination

OSI v TCP/IP



OSI

TCP/IP

Application

Presentation

Session

Transport

Network

Data Link

Physical

Application

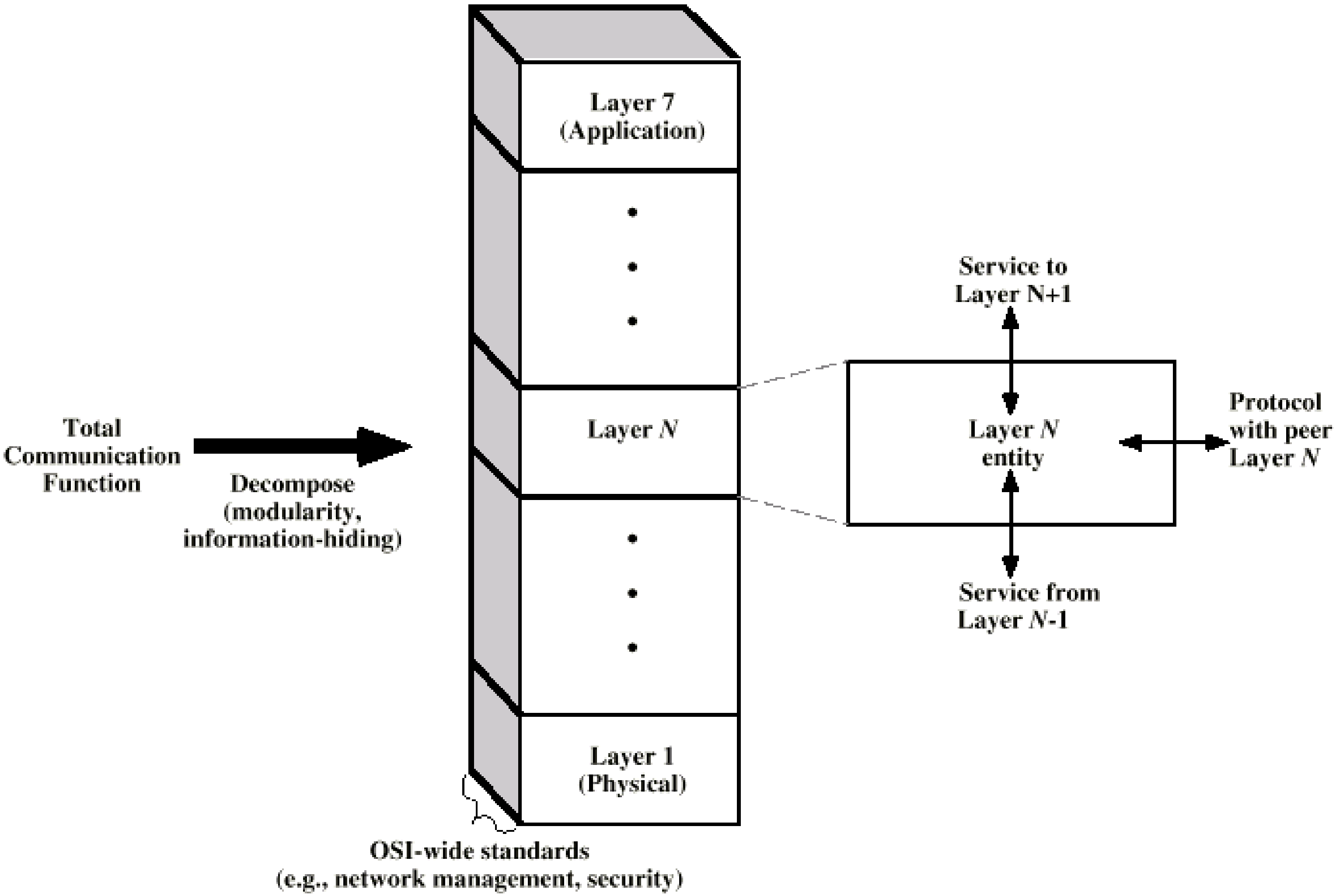
Transport (host-to-host)

Internet

Network Access

Physical

Standardized Protocol Architectures



LAN Protocol Architecture

- Layering of protocols that organize the structure of a LAN
- LAN protocol architectures are specified by IEEE 802 reference model
- In IEEE 802 reference model, there are two separate layers corresponding to data link layer of OSI model
  - MAC (Medium Access Control) layer
  - LLC (Logical Link Control) layer

LAN Topologies

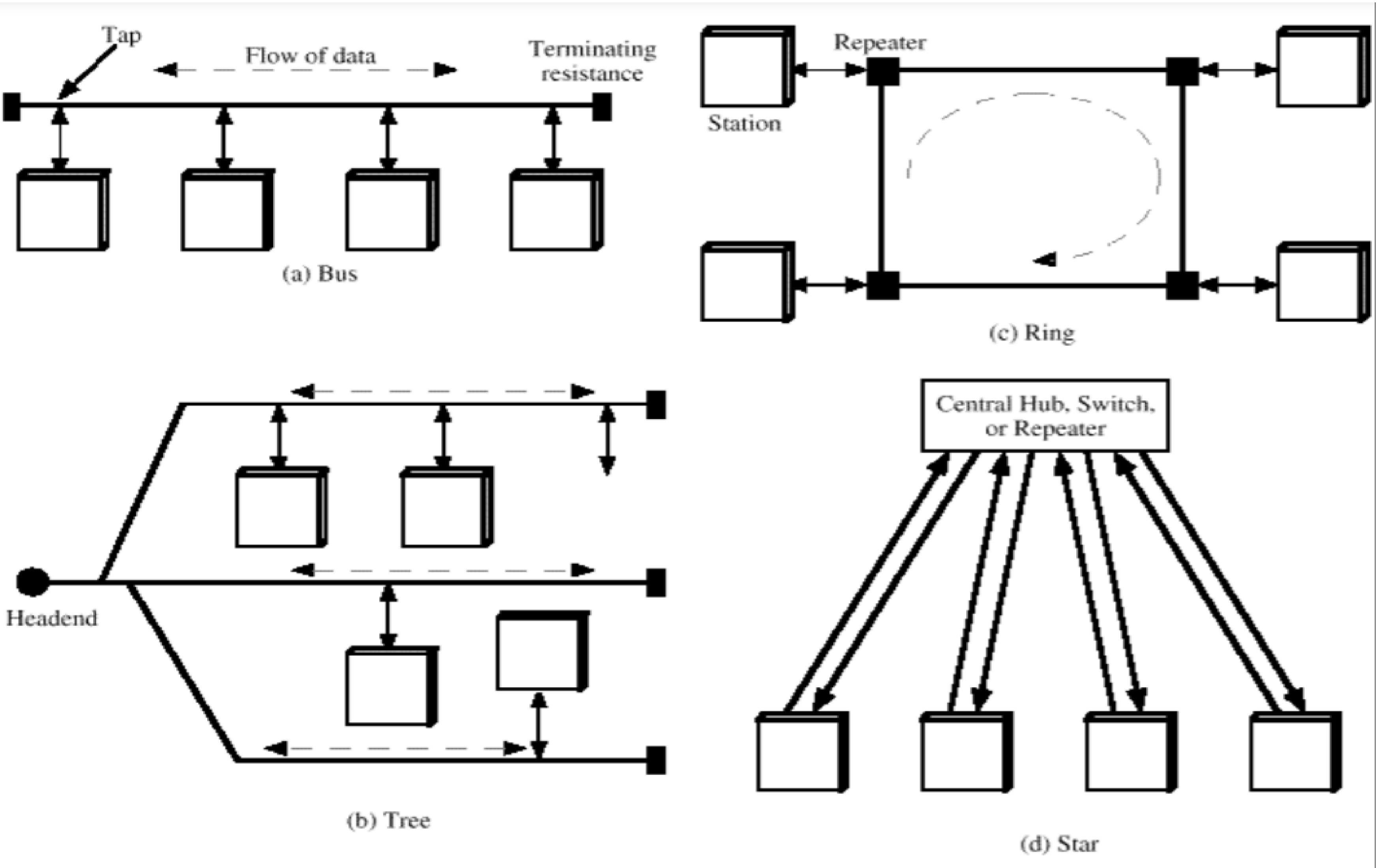


Figure 12.4 LAN/MAN Topologies

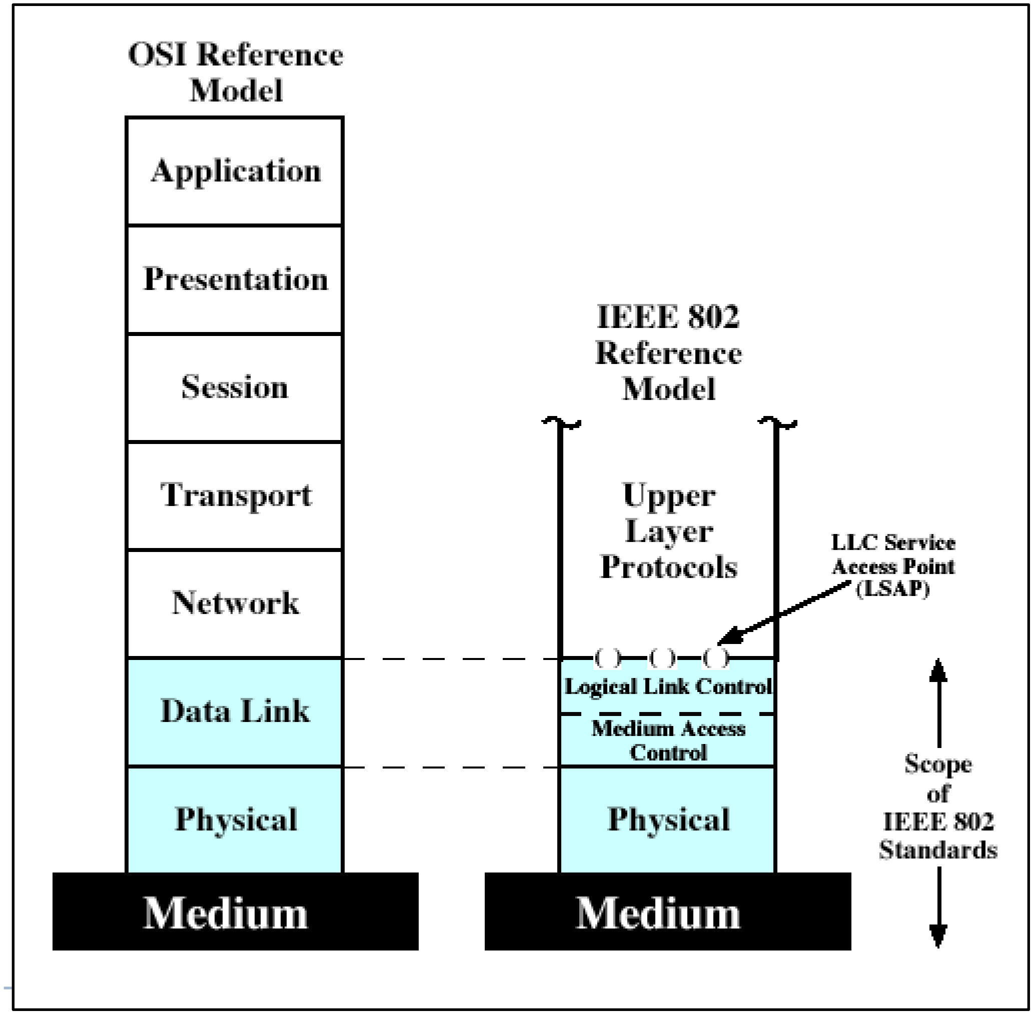
Advantages of Standards

- Assure sufficient volume to keep costs down
- Enable equipment from various sources to interconnect

IEEE 802 Reference Model

- IEEE 802 committee developed, revises, and extends standards
- Use a three-layer protocol hierarchy: physical, medium access control (MAC), and logical link control (LLC)

IEEE 802 Protocol Models Compared to OSI Model



- LLC Layer
  - Provide an interface to higher layers
  - Flow and error control
- MAC Layer
  - Interface to physical layer
  - Govern access to LAN transmission system
  - Sending/receiving frames
  - Frame synchronization
  - Error detection
- Physical Layer
  - Specification of the transmission medium and the topology
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception

Physical Layer

- Encoding/decoding of signals and bit transmission/reception
- Specification of the transmission medium.
- Generally considered "below" the lowest layer of the OSI model. However, the choice of transmission medium is critical in LAN design, and so a specification of the medium is included

Logical Link Control

- Specifies method of addressing and controls exchange of data
- Independent of topology, medium, and medium access control
- Unacknowledged connectionless service (higher layers handle error/flow control, or simple apps)
- Connection-mode service (devices without higher-level software)
- Acknowledged connectionless service (no prior connection necessary)

Medium Access Control

- LLC frames data in a PDU (protocol data unit)
- MAC layer frames data again
  - MAC control (e.g. priority level)
  - Destination MAC address
  - Source MAC address
  - LLC PDU
  - CRC (Cyclic Redundancy Check)

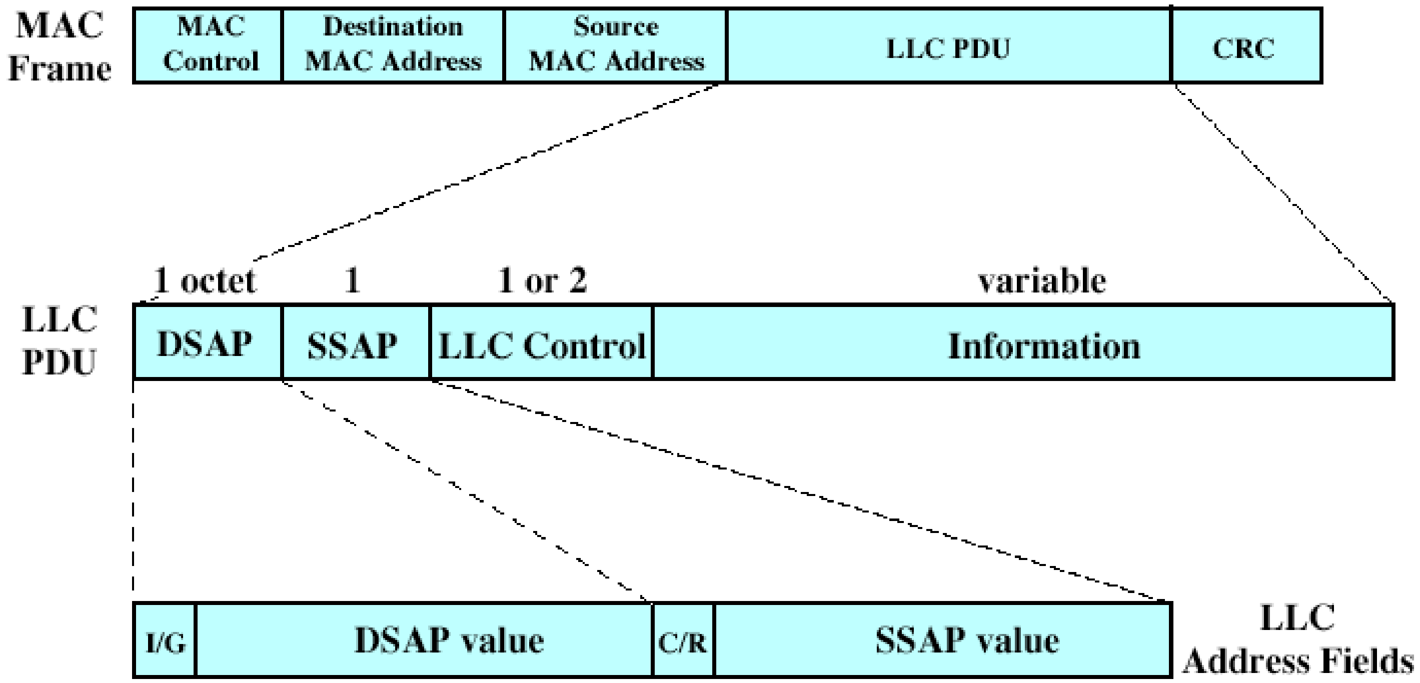
Medium Access Control

- Some means of controlling access to the shared transmission medium is needed to provide for an orderly and efficient use of the network's transmission capacity ⇒ MAC protocol
- Major issues are: WHERE and HOW
  - WHERE: either Centralized or Distributed
  - HOW: Synchronous or Asynchronous
    - Synchronous: FDM, synchronous TDM ⇒ not well used
    - Asynchronous: Round Robin, Reservation, Contention
- Centralized vs. distributed access control
  - Advantages of centralized control
    - Easier to provide centralized control with priorities, etc.
    - Individual station logic is simple
    - Avoids problem of group coordination
  - Disadvantages
    - Less reliable
    - May become bottleneck and reduce efficiency
    - Overheads may be higher if propagation delay is high

- Access Control Mechanisms
  - Round-Robin
    - Each station, in turn, is given opportunity to transmit. Either a central controller polls a station to permit to go, or stations can coordinate among themselves. “Token” is passed. Simple but overhead may be high when traffic
  - Reservation
    - Station wishing to transmit makes “reservations” for time slots in advance. Central or distributed.
  - Contention (Random Access)
    - No control on who tries; If “collision” occurs, retransmission after random timeout is attempted.

- MAC Frame Format
  - MAC control
    - Contains any protocol control information needed for the functioning of the MAC protocol. e.g., priority level.
  - Destination/Source MAC address
    - Destination/source physical attachment point on the LAN for this frame
  - LLC PDU
    - LLC data
  - CRC
    - Error detecting code

LLC PDU in a MAC Frame



I/G = Individual/Group
C/R = Command/Response

DSAP (Destination Service Access Point)
SSAP (Source Service Access Point)

LLC Services/Protocols

- Unacknowledged connectionless service (Type 1)
  - Datagram style service. No flow and error control mechanisms. Delivery of data is not guaranteed.
  - Unnumbered information PDU is used to transfer user data
- Connection-mode service (Type 2)
  - A logical connection is setup, and flow and error control are provided.
  - The connection is uniquely identified by the pair of SAPs.
  - Information PDUs include send and receive sequence numbers for for sequencing and flow control. Supervisory PDUs are used for flow and error control.
- Acknowledgement connectionless service
  - Acknowledged datagrams, but no prior logical connection is setup.
  - Each transmitted PDU is acknowledged. To guard against lost PDUs, 1-bit sequence number is used.

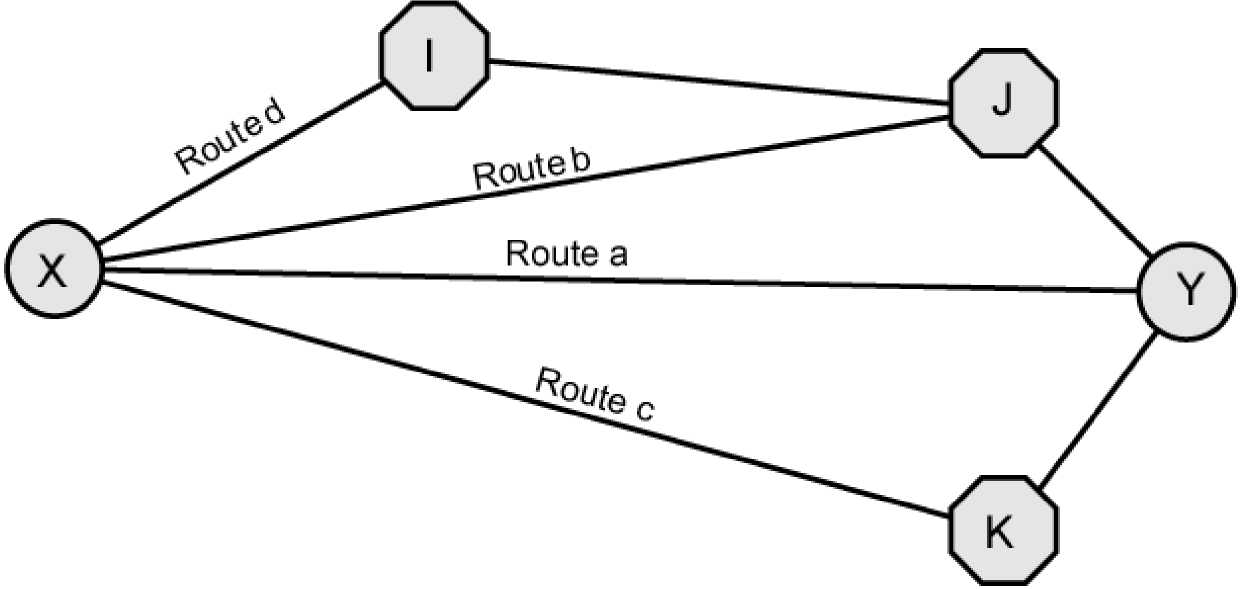
Routing in Circuit Switched Network

- Many connections will need paths through more than one switch
- Need to find a route
  - Efficiency
  - Resilience
- Public telephone switches are a tree structure
  - Static routing uses the same approach all the time
- Dynamic routing allows for changes in routing depending on traffic
  - Uses a peer structure for nodes

Alternate Routing

- Possible routes between end offices predefined
- Originating switch selects appropriate route
- Routes listed in preference order
- Different sets of routes may be used at different times

Alternate Routing Diagram



Route a: X® Y
Route b: X® J® Y
Route c: X® K ® Y
Route d: X® I ® J® Y

○ = end office

⯃ = intermediate switching node

(a) Topology

Time Period	First route	Second route	Third route	Fourth and final route
Morning	a	b	c	d
Afternoon	a	d	b	c
Evening	a	d	c	b
Weekend	a	c	b	d

(b) Routing table

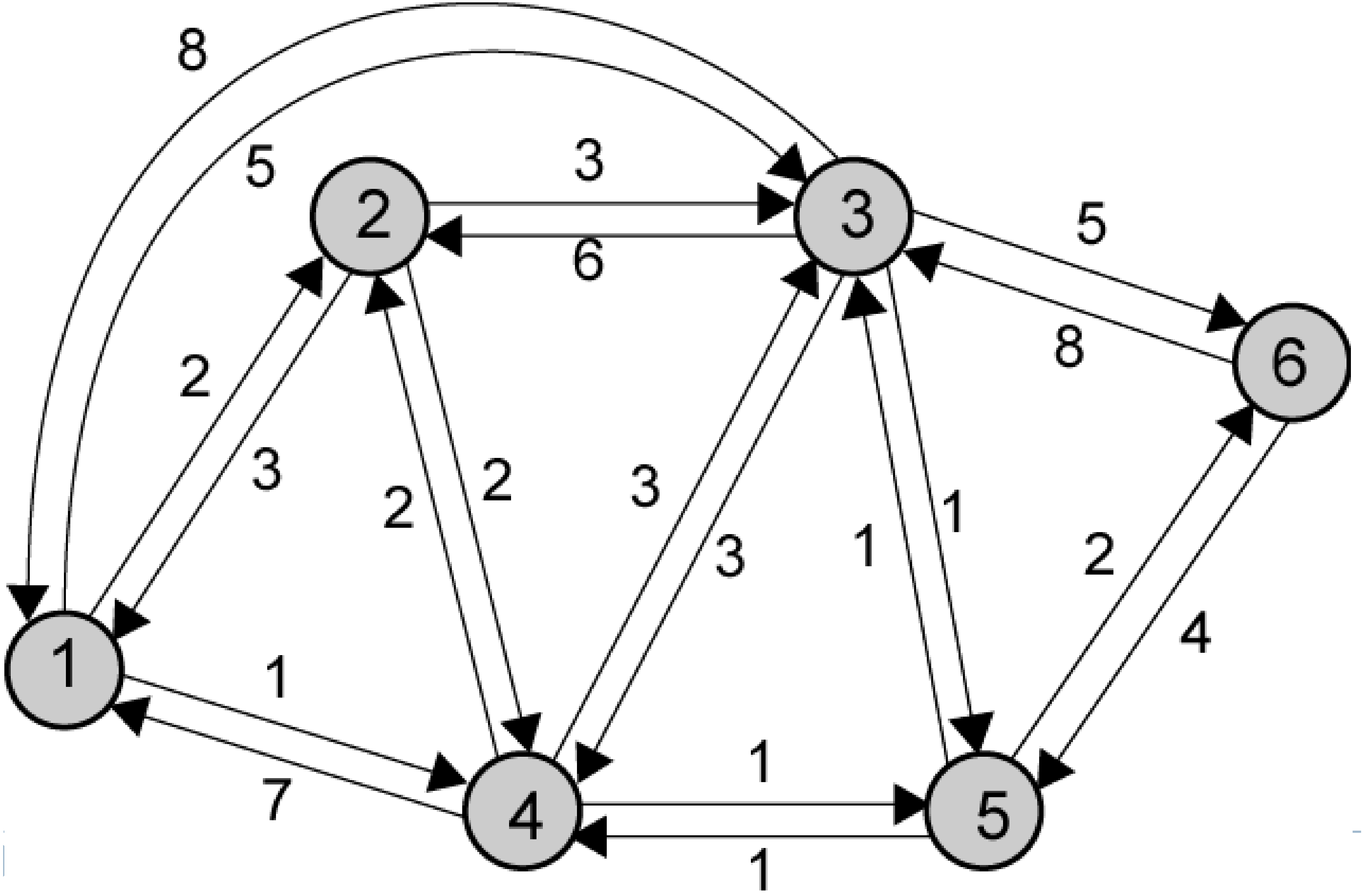
Routing in Packet Switched Network

- Complex, crucial aspect of packet switched networks
- Characteristics required
    - Correctness
    - Simplicity
    - Robustness
    - Stability
    - Fairness
    - Optimality
    - Efficiency

Performance Criteria

- Used for selection of route
- Minimum hop
- Least cost

Example Packet Switched Network



Decision Time and Place

- Time
  - Packet or virtual circuit basis
- Place
  - Distributed
    - Made by each node
  - Centralized
  - Source

Network Information Source and Update Timing

- Routing decisions usually based on knowledge of network (not always)
- Distributed routing
  - Nodes use local knowledge
  - May collect info from adjacent nodes
  - May collect info from all nodes on a potential route
- Central routing
  - Collect info from all nodes
- Update timing
  - When is network info held by nodes updated
  - Fixed - never updated
  - Adaptive - regular updates

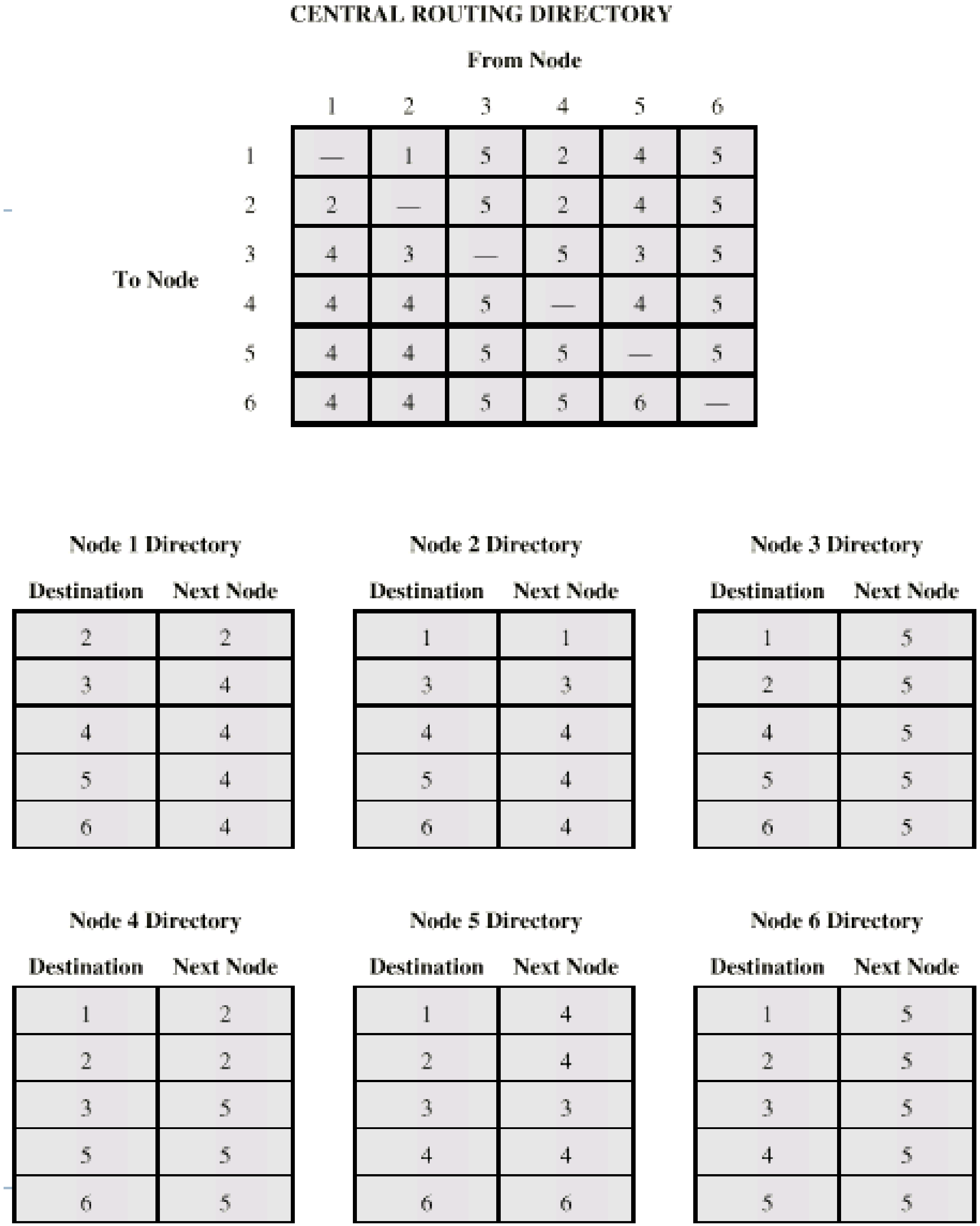
Routing Strategies

- Fixed
- Flooding
- Random
- Adaptive

Fixed Routing

- Single permanent route for each source to destination pair
- Determine routes using a least cost algorithm
- Route fixed, at least until a change in network topology

Fixed Routing Tables



CENTRAL ROUTING DIRECTORY

To Node \ From Node	1	2	3	4	5	6
1	—	1	5	2	4	5
2	2	—	5	2	4	5
3	4	3	—	5	3	5
4	4	4	5	—	4	5
5	4	4	5	5	—	5
6	4	4	5	5	6	—

Node 1 Directory

Destination	Next Node
2	2
3	4
4	4
5	4
6	4

Node 2 Directory

Destination	Next Node
1	1
3	3
4	4
5	4
6	4

Node 3 Directory

Destination	Next Node
1	5
2	5
4	5
5	5
6	5

Node 4 Directory

Destination	Next Node
1	2
2	2
3	5
5	5
6	5

Node 5 Directory

Destination	Next Node
1	4
2	4
3	3
4	4
6	6

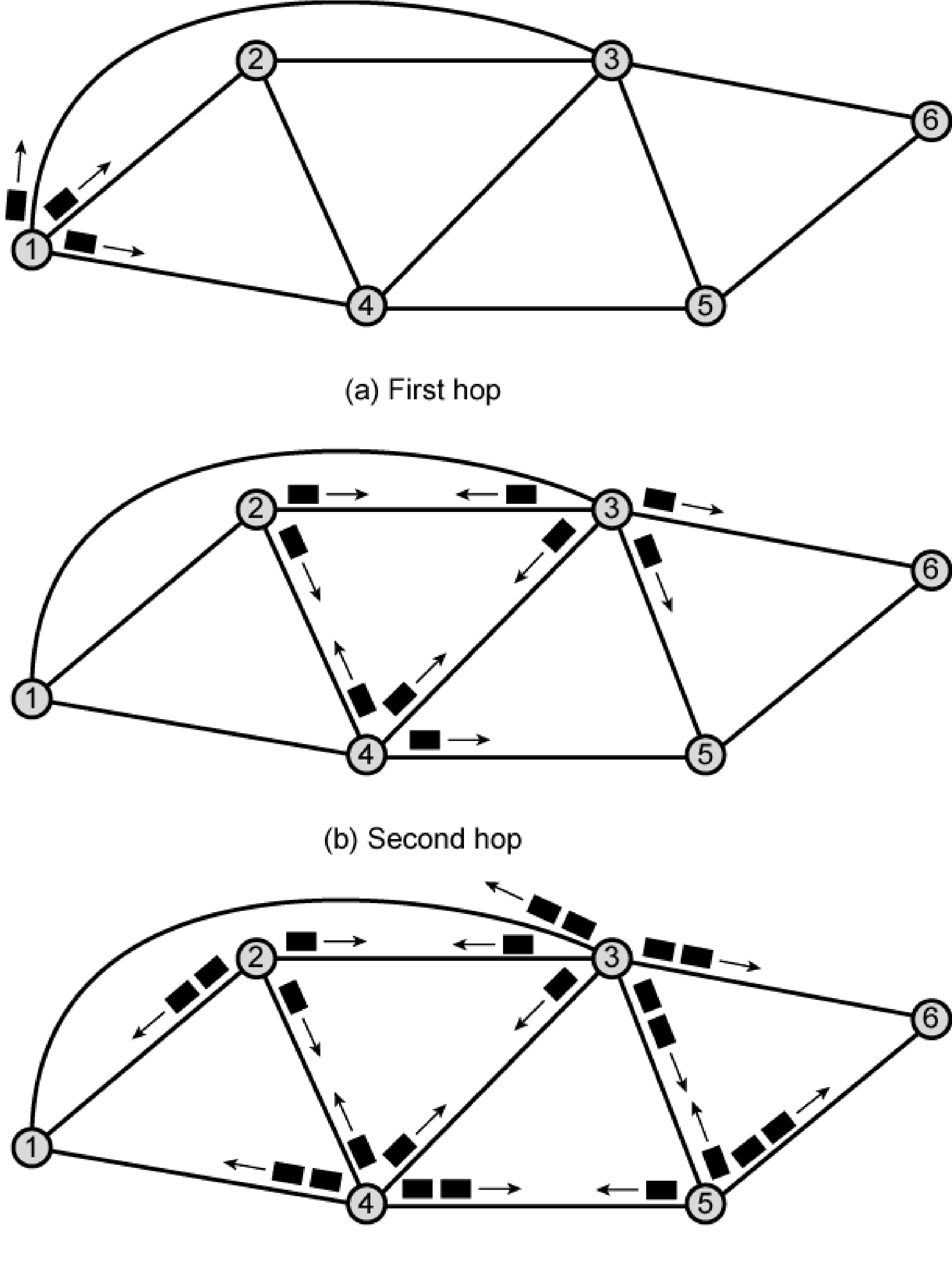
Node 6 Directory

Destination	Next Node
1	5
2	5
3	5
4	5
5	5

Flooding

- No network info required
- Packet sent by node to every neighbor
- Incoming packets retransmitted on every link except incoming link
- Eventually a number of copies will arrive at destination
- Each packet is uniquely numbered so duplicates can be discarded
- Nodes can remember packets already forwarded to keep network load in bounds
- Can include a hop count in packets

Flooding Example



(a) First hop

(b) Second hop

(c) Third hop

Properties of Flooding

- All possible routes are tried
  - Very robust
- At least one packet will have taken minimum hop count route
  - Can be used to set up virtual circuit
- All nodes are visited
  - Useful to distribute information (e.g. routing)

Random Routing

- Node selects one outgoing path for retransmission of incoming packet
- Selection can be random or round robin
- Can select outgoing path based on probability calculation
- No network info needed
- Route is typically not least cost nor minimum hop

Adaptive Routing

- Used by almost all packet switching networks
- Routing decisions change as conditions on the network change
  - Failure
  - Congestion
- Requires info about network
- Decisions more complex
- Tradeoff between quality of network info and overhead
- Reacting too quickly can cause oscillation
- Too slowly to be relevant

Adaptive Routing - Advantages

- Improved performance
- Aid congestion control
- Complex system
  - May not realize theoretical benefits

Least Cost Algorithms

- Basis for routing decisions
  - Can minimize hop with each link cost 1
  - Can have link value inversely proportional to capacity
- Given network of nodes connected by bi-directional links
- Each link has a cost in each direction
- Define cost of path between two nodes as sum of costs of links traversed
- For each pair of nodes, find a path with the least cost
- Link costs in different directions may be different
  - E.g. length of packet queue

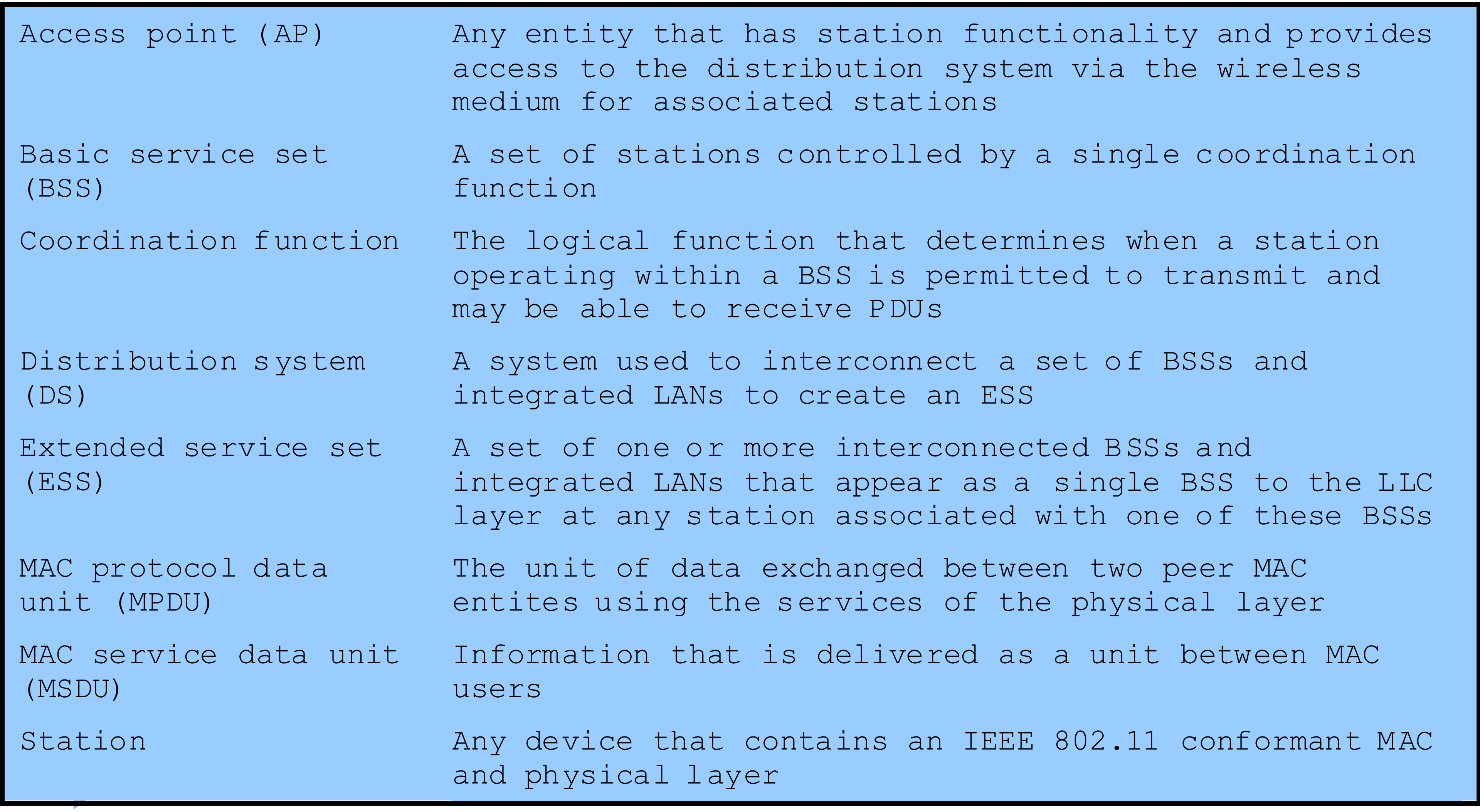
IEEE Standards

- IEEE 802 committee for LAN standards
- IEEE 802.11 formed in 1990's
  - charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- since then demand for WLANs, at different frequencies and data rates, has exploded
- hence seen ever-expanding list of standards issued

IEEE 802 Standards

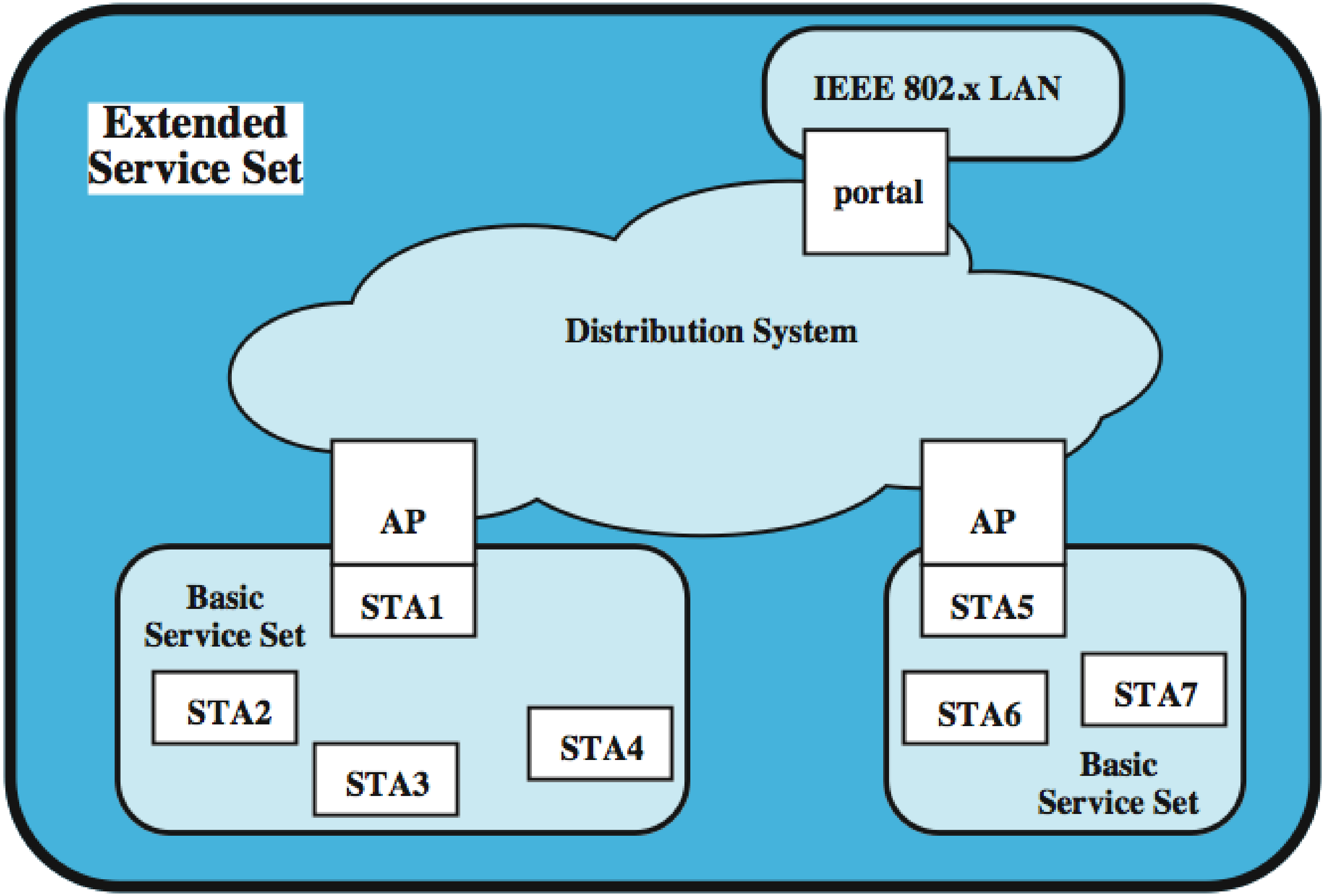
Standard	Scope
IEEE 802.11	Medium access control (MAC): One common MAC for WLAN applications
	Physical layer: Infrared at 1 and 2 Mbps
	Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
	Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	Bridge operation at 802.11 MAC layer
IEEE 802.11d	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	Recommended practices for multivendor access point interoperability
IEEE 802.11g	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
IEEE 802.11m	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
IEEE 802.11n	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	Physical/MAC: Wireless access in vehicular environments
IEEE 802.11r	Physical/MAC: Fast roaming (fast BSS transition)
IEEE 802.11s	Physical/MAC: ESS mesh networking
IEEE 802.11,2	Recommended practice for the Evaluation of 802.11 wireless performance
IEEE 802.11u	Physical/MAC: Interworking with external networks

IEEE 802 Terminology



Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

IEEE 802.11 Architecture



STA = station
AP = access point

Wi-Fi Alliance

- 802.11b first broadly accepted standard
- Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999
  - to assist interoperability of products
  - renamed Wi-Fi (Wireless Fidelity) Alliance
  - created a test suite to certify interoperability
  - initially for 802.11b, later extended to 802.11g
  - concerned with a range of WLANs markets, including enterprise, home, and hot spots

Ethernet (CSMA/CD)

- most widely used LAN standard
- developed by
  - Xerox - original Ethernet
  - IEEE 802.3
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - random / contention access to media

ALOHA

- developed for packet radio nets
- when station has frame, it sends
- then listens for a bit over max round trip time
  - if receive ACK then fine
  - if not, retransmit
  - if no ACK after repeated transmissions, give up
- frame may be damaged by noise or by another station transmitting at the same time (collision)
- any overlap of frames causes collision
- max utilization 18%

Slotted ALOHA

- time on channel based on uniform slots equal to frame transmission time
    - need central clock (or other sync mechanism)
- transmission begins at slot boundary
- frames either miss or overlap totally
- max utilization 37%
- both have poor utilization
- fail to use fact that propagation time is much less than frame transmission time

CSMA

- stations soon know transmission has started
- so first listen for clear medium (carrier sense)
- if medium idle, transmit
- if two stations start at the same instant, collision
  - wait reasonable time
  - if no ACK then retransmit
  - collisions occur at leading edge of frame
- max utilization depends on propagation time (medium length) and frame length

Nonpersistent CSMA

- Nonpersistent CSMA rules:
  1. if medium idle, transmit
  2. if medium busy, wait amount of time drawn from probability distribution (retransmission delay) & retry
- random delays reduces probability of collisions
- capacity is wasted because medium will remain idle following end of transmission
- nonpersistent stations are deferential

1-persistent CSMA

- 1-persistent CSMA avoids idle channel time
- 1-persistent CSMA rules:
  1. if medium idle, transmit;
  2. if medium busy, listen until idle; then transmit immediately
- 1-persistent stations are selfish
- if two or more stations waiting, a collision is guaranteed

P-persistent CSMA

- a compromise to try and reduce collisions and idle time
- p-persistent CSMA rules:
  1. if medium idle, transmit with probability p, and delay one time unit with probability (1–p)
  2. if medium busy, listen until idle and repeat step 1
  3. if transmission is delayed one time unit, repeat step 1
- issue of choosing effective value of p to avoid instability under heavy load

Value of p?

- have n stations waiting to send
- at end of tx, expected no of stations is np
  - if np>1 on average there will be a collision
- repeated tx attempts mean collisions likely
- eventually when all stations trying to send have continuous collisions hence zero throughput
- thus want np<1 for expected peaks of n
  - if heavy load expected, p small
  - but smaller p means stations wait longer

CSMA/CD Description

- with CSMA, collision occupies medium for duration of transmission
- better if stations listen whilst transmitting
- CSMA/CD rules:
  1. if medium idle, transmit
  2. if busy, listen for idle, then transmit
  3. if collision detected, jam and then cease transmission
  4. after jam, wait random time then retry

10Mbps Specification (Ethernet)

	10BASE5	10BASE2	10BASE-T	10BASE-FP
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 (mm)	10	5	0.4 to 0.6	62.5/125 µm

Datagram Packet Switching

- No call setup
- Each packet can travel across a different route from sender to receiver
- Delivery and order of packets cannot be guaranteed
- Most common implementation of datagram packet switching is Internet Protocol (IP)

Virtual Circuit Packet Switching

- Similar to standard circuit-switched networks
- Call Setup required to define the route between Sender and Receiver
- Each route is assigned a Virtual Circuit Identifier (VCI)
- All packets using the same VCI will travel the same route and will arrive in sequence
- Circuit is "virtual" because resources are not dedicated to a single call
- Most common forms of virtual circuit packet switching are X.25 and Frame Relay

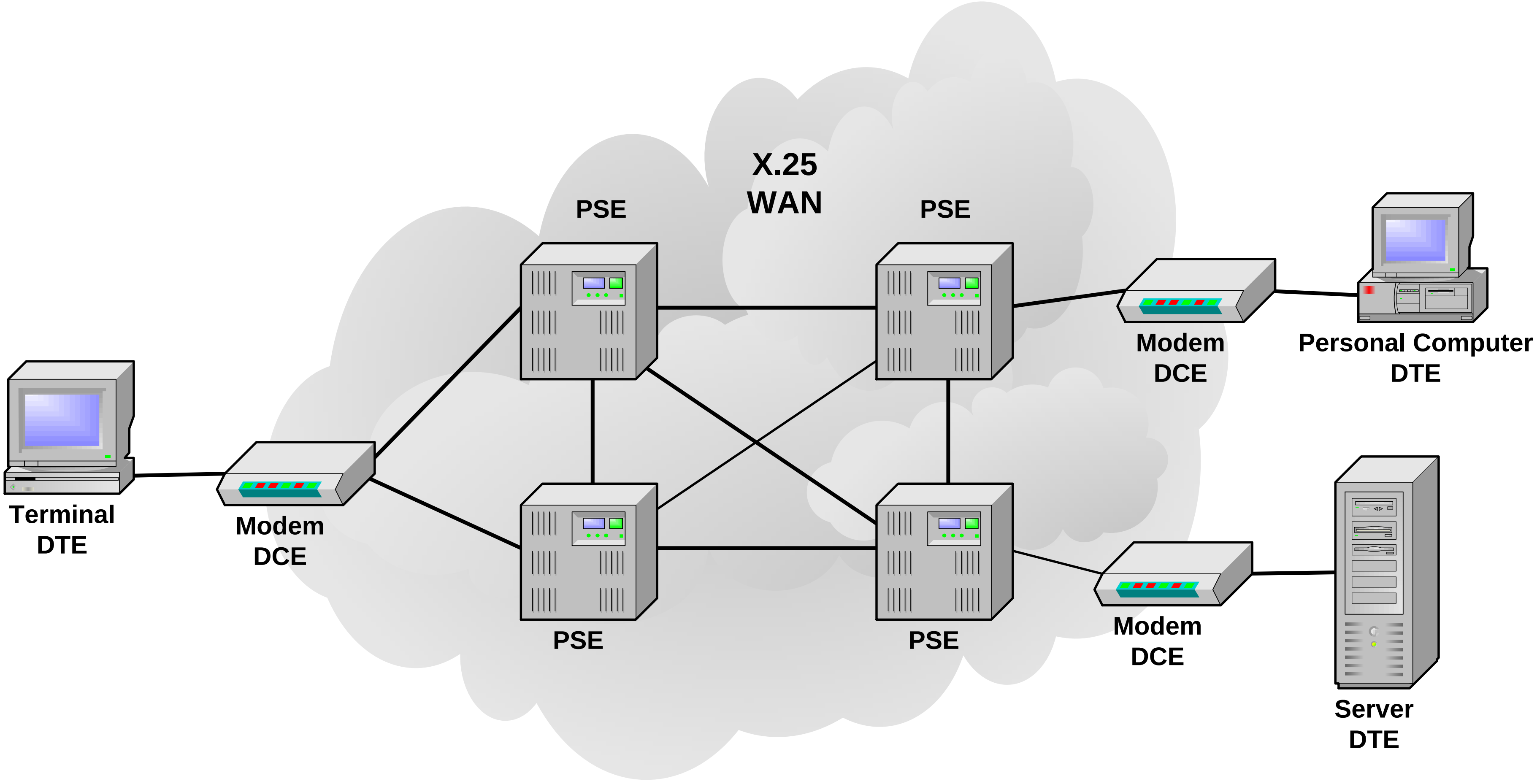
X.25 History and Overview

- Designed to provide a low cost alternative for data communication over public networks
  - Pay only for bandwidth actually used
- Ideal for "bursty" communication over low quality circuits
- Standard provides error detection and correction for reliable data transfer
- X.25 standard approved in 1976 by CCITT (now known as ITU)
- Can support speeds of 9.6 Kbps to 2 Mbps
- Can provide multiplexing of up to 4095 virtual circuits over on DTE-DCE link

X.25 Devices

- Data Terminal Equipment (DTE)
  - Terminals, personal computers, and network hosts
  - Located on premises of subscriber
- Data Circuit-terminating Equipment (DCE)
  - Modems and packet switches
  - Usually located at carrier facility
- Packet Switching Exchange (PSE)
  - Switches that make up the carrier network

Sample X.25 Network



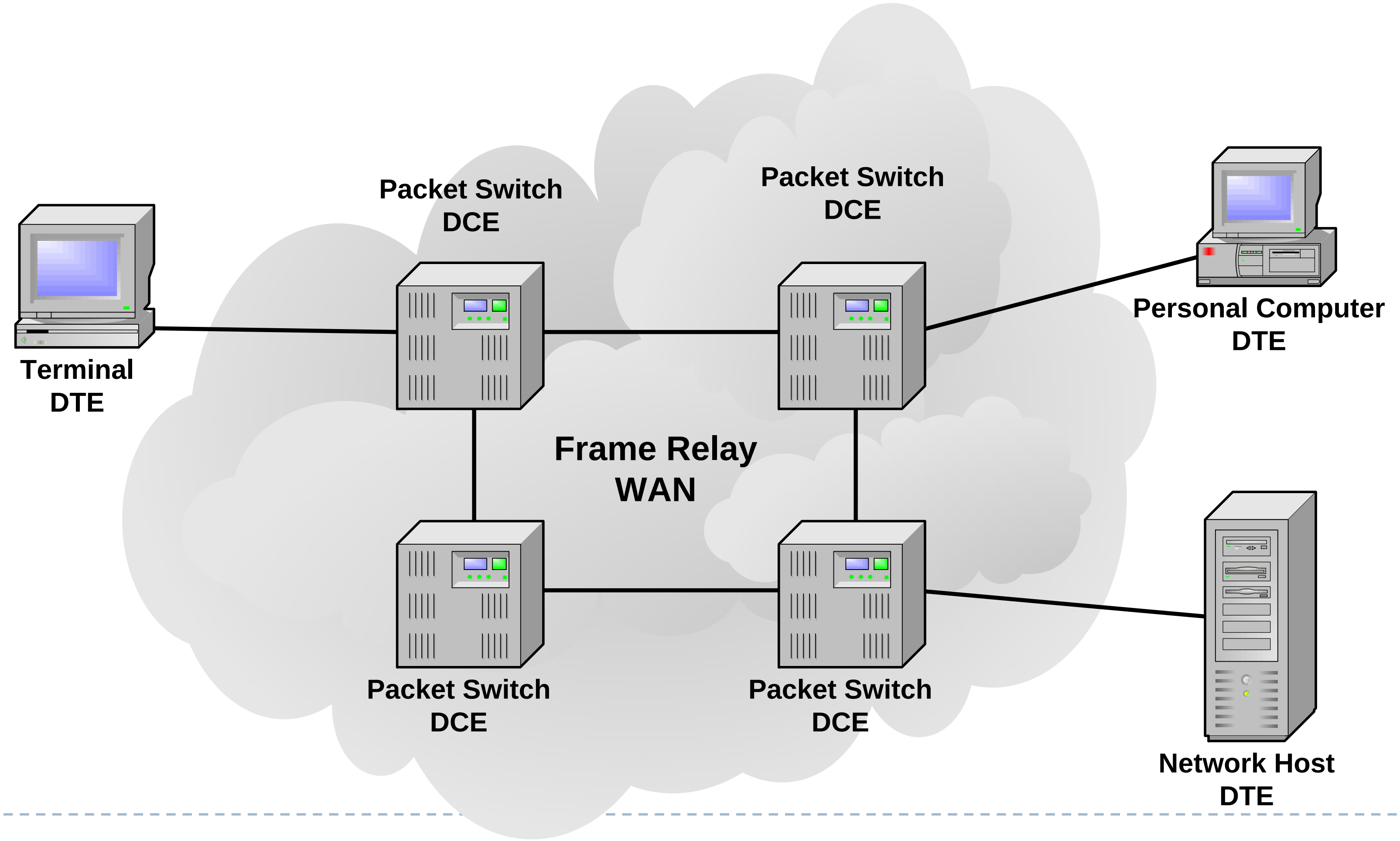
Frame Relay History and Overview

- Frame Relay was originally designed for use on Integrated Services Digital Network (ISDN)
- Usually considered a replacement for X.25 using more advanced digital and fiber optic connections
- Does not perform error correction at intermediate nodes making it faster than X.25
  - When an error is detected (FCS) the frame is discarded and correction is left up to higher layer protocols
- Original standard proposed in 1984 but widespread acceptance did not occur until the late 1980's
  - Service Description Standard (ITU-T I.233)
    - Overall service description and specifications, Connection Management
  - Core Aspects (ITU-T Q.922)
    - Frame Format, Field Functions, Congestion Control
  - Signaling (ITU-T Q.933)
    - Establishing and Releasing switched connections and status of permanent connections

Frame Relay Devices

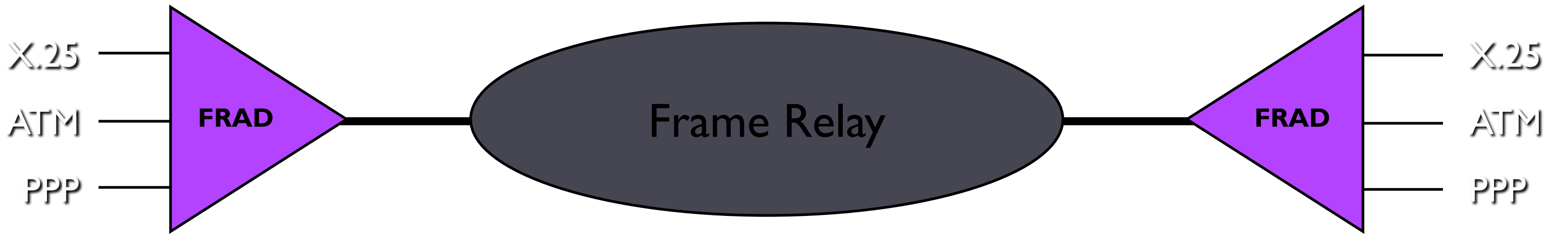
- Data Terminal Equipment (DTE)
  - Terminals, Personal Computers, routers, and bridges typically at the customer location
- Data Circuit-terminating Equipment (DCE)
  - Typically packet switches owned by the carrier that transmit data through the WAN

Sample Frame Relay Network



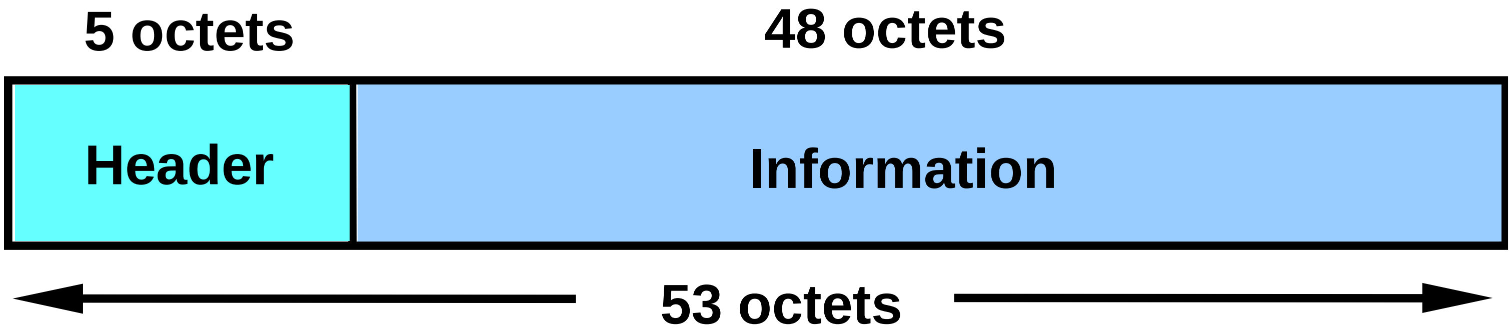
Frame Relay Assembler/Disassembler (FRAD)

- To handle frames from other protocols a FRAD is used to provide conversion to Frame Relay packets
- A FRAD can either be a separate device or part of a router/switch



What is Asynchronous Transfer Mode (ATM)?

- Asynchronous Transfer Mode (ATM) is a connection-oriented, high-speed, low-delay switching and transmission technology that uses short and fixed-size packets, called cells, to transport information.



- Using the cell switching technique, ATM combines the benefits of both circuit switching (low and constant delay, guaranteed capacity) and packet switching (flexibility, efficiency for bursty traffic) to support the transmission of multimedia traffic such as voice, video, image, and data over the same network.

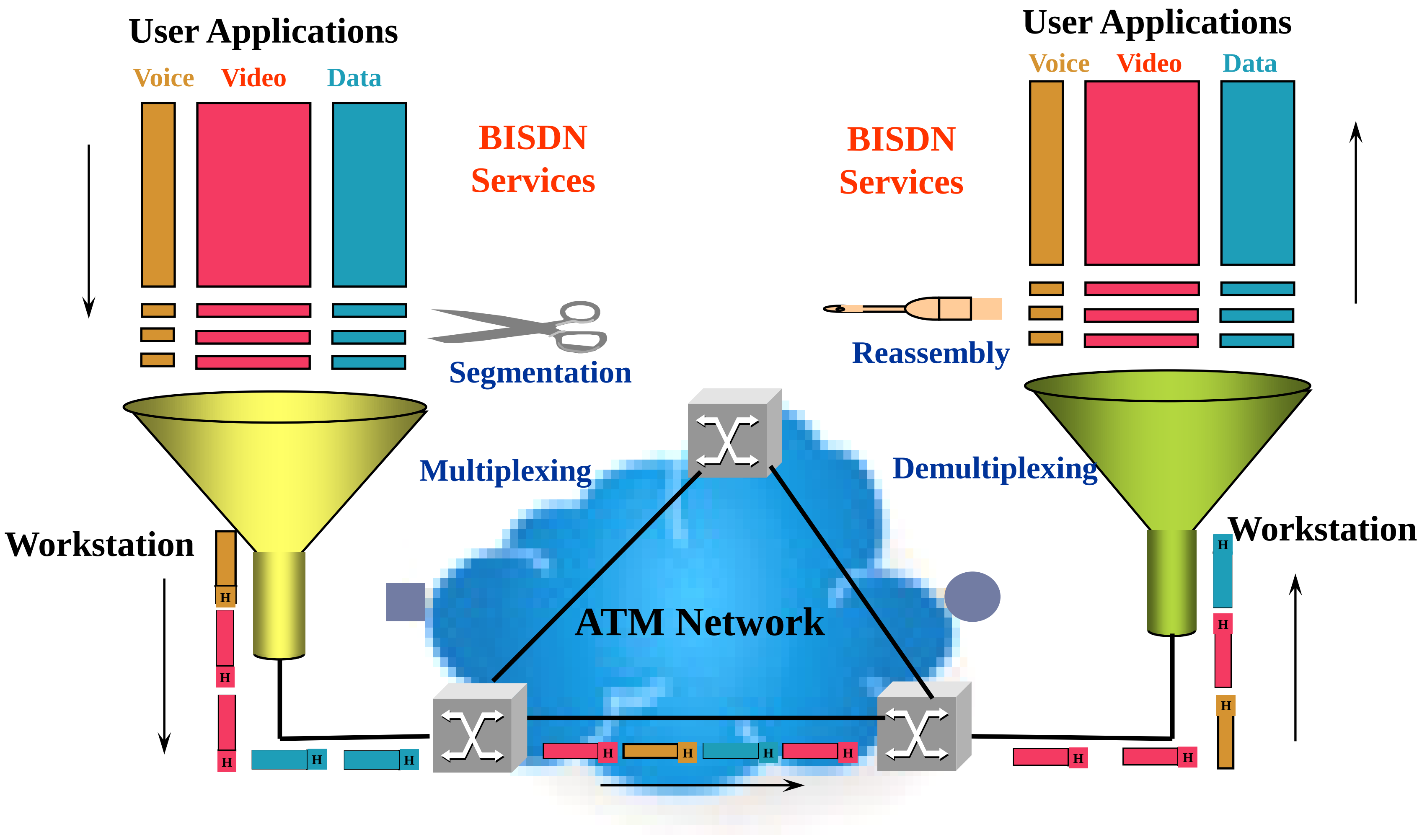
Goals of ATM

- ATM, also known as cell relay, involves the transfer of data in discrete chunks called cells. Multiple logical connections can be multiplexed over a single path. This is similar to packet switching except that the packets are variable sized and cells are of a fixed size.
- ATM is used in the WANs and is not constrained to a particular physical medium or data rate (155 Mbps, 622 Mbps, and 2.5 Gbps).
- ATM has minimal error and flow control capabilities to reduce the overhead of cells the overhead of protocol processing, enabling ATM to operate at high data rates.

Why ATM?

- International standard-based technology (for interoperability)
- Low network latency (for voice, video, and real-time applications)
- Low variance of delay (for voice and video transmission)
- Guaranteed quality of service
- High capacity switching (multi-giga bits per second)
- Bandwidth flexibility (dynamically assigned to users)
- Scalability (capacity may be increased on demand)
- Medium not shared for ATM LAN (no degradation in performance as traffic load or number of users increases)
- Supports a wide range of user access speeds
- Appropriate (seamless integration) for LANs, MANs, and WANs
- Supports audio, video, imagery, and data traffic (for integrated services)

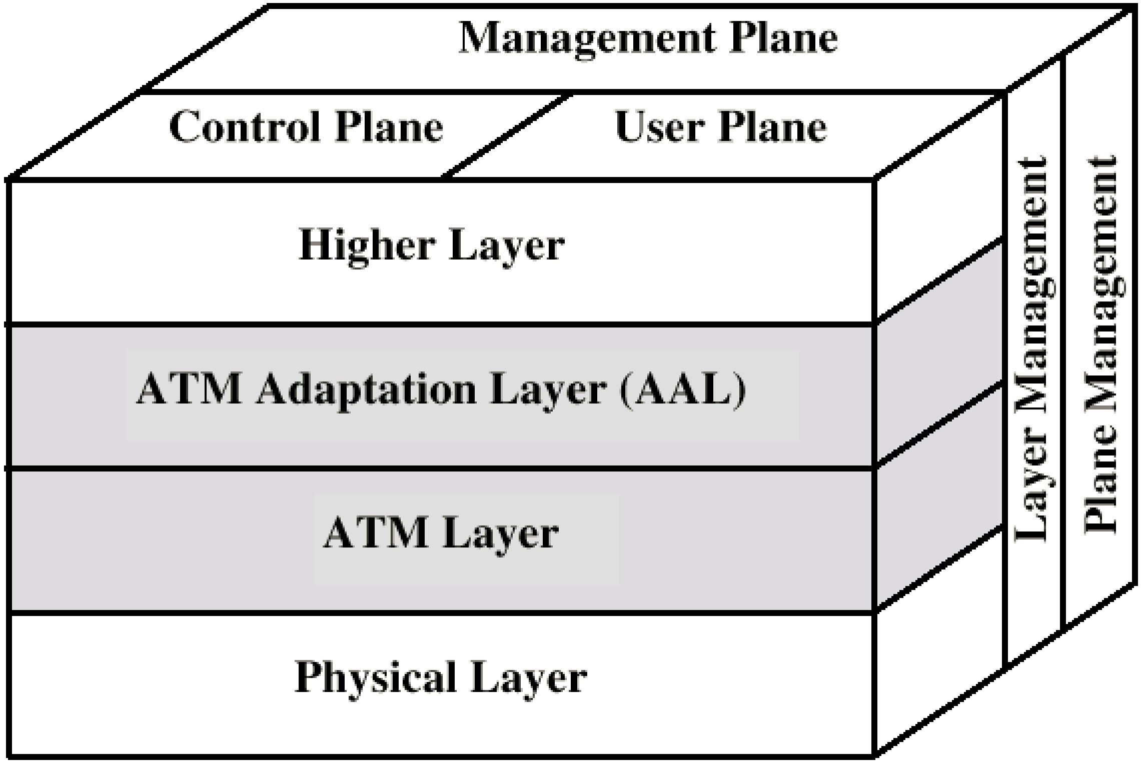
How Does ATM Work?



How Does ATM Work? (concluded)

- ATM is connection-oriented -- an end-to-end connection must be established and routing tables setup prior to cell transmission
- Once a connection is established, the ATM network will provide end-to-end Quality of Service (QoS) to the end users
- All traffic, whether voice, video, image, or data is divided into 53-octet cells and routed in sequence across the ATM network
- Routing information is carried in the header of each cell
- Routing decisions and switching are performed by hardware in ATM switches
- Cells are reassembled into voice, video, image, or data at the destination

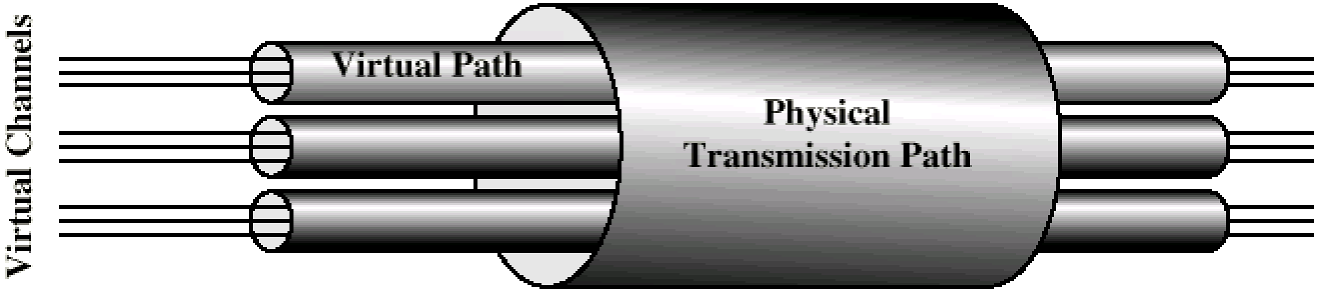
Protocol Architecture (diag)



Protocol Architecture

- Physical Layer
  - Concerned with specifications of the transmission medium and signal encoding . Data rates specified include 155 and 622 Mbps with other data rates possible.
- ATM Layer
  - Defines transmission of data in fixed size cells and also defines the logical connections (Virtual circuits and virtual paths).
- ATM Adaptation Layer (AAL)
  - Supports transfer protocols not based on ATM. It maps higher layer information into ATM cells to be transported over an ATM network, then collects information from ATM cells for delivery to higher layers (e.g. a IP packet can be mapped to ATM cells).
- There are 3 planes in the protocol architecture:
  - the User plane is for user traffic including flow and error control;
  - the Control plane is for connection control;
  - the Management plane manages the system as a whole and coordinates the planes and layers.

ATM Connection Relationships



Advantages of Virtual Paths

- Simplified network architecture
- Increased network performance and reliability
- Reduced processing
- Short connection setup time
- Enhanced network services

Virtual Channel Connection Uses

- Between end users
  - End to end user data
  - Control signals
  - VPC provides overall capacity
    - VCC organization done by users
- Between end user and network
  - Control signaling
- Between network entities
  - Network traffic management
  - Routing

VP/VC Characteristics

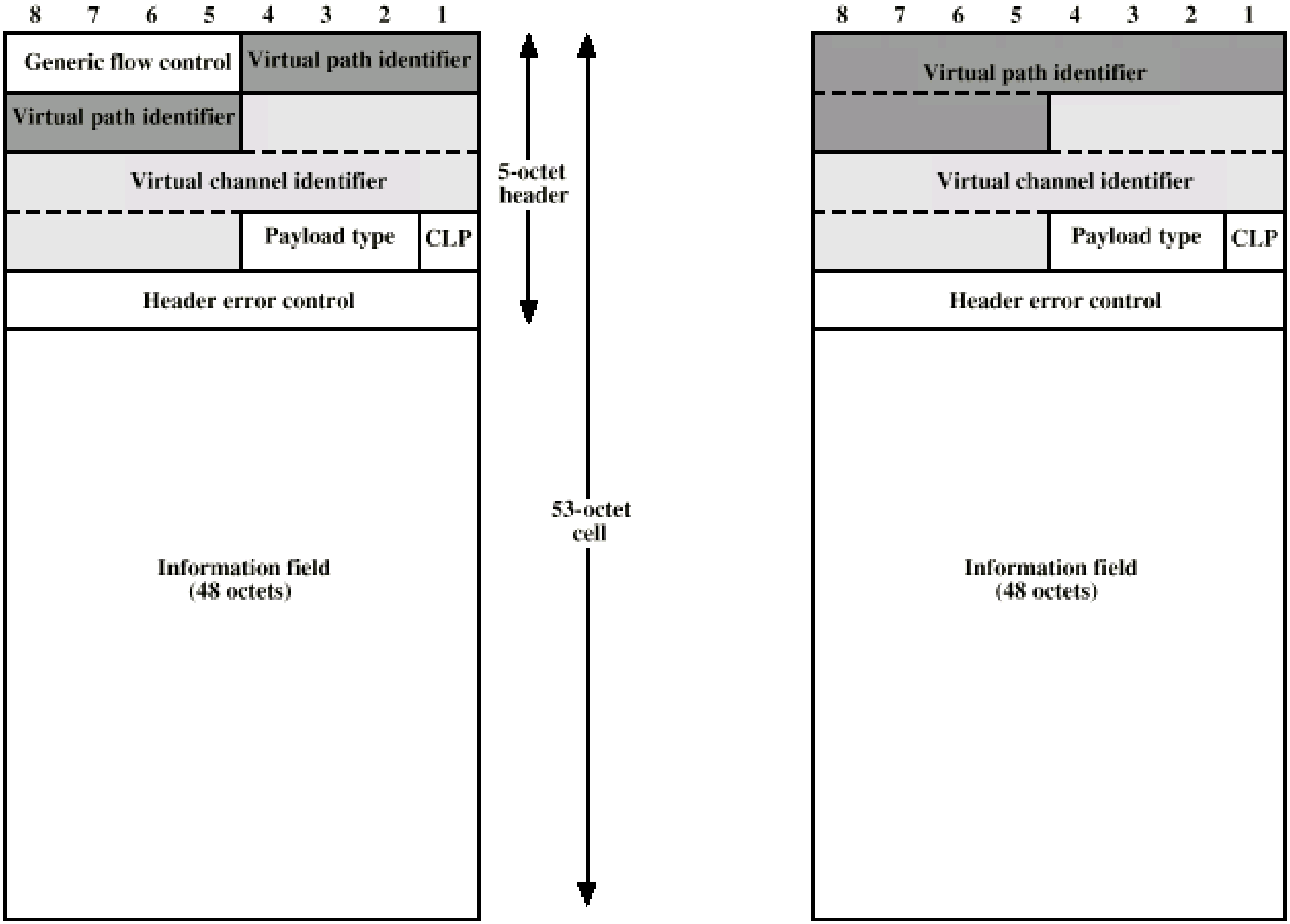
- Quality of service
- Switched and semi-permanent channel connections
- Call sequence integrity
- Traffic parameter negotiation and usage monitoring

- VPC only
  - Virtual channel identifier restriction within VPC

ATM Cells

- Fixed size
- 5 octet header
- 48 octet information field
- Small cells reduce queuing delay for high priority cells
- Small cells can be switched more efficiently
- Easier to implement switching of small cells in hardware

ATM Cell Format



8 7 6 5 4 3 2 1

Generic flow control

Virtual path identifier

Virtual path identifier

Virtual channel identifier

Payload type

CLP

Header error control

Information field
(48 octets)

5-octet
header

53-octet
cell

8 7 6 5 4 3 2 1

Virtual path identifier

Virtual channel identifier

Payload type

CLP

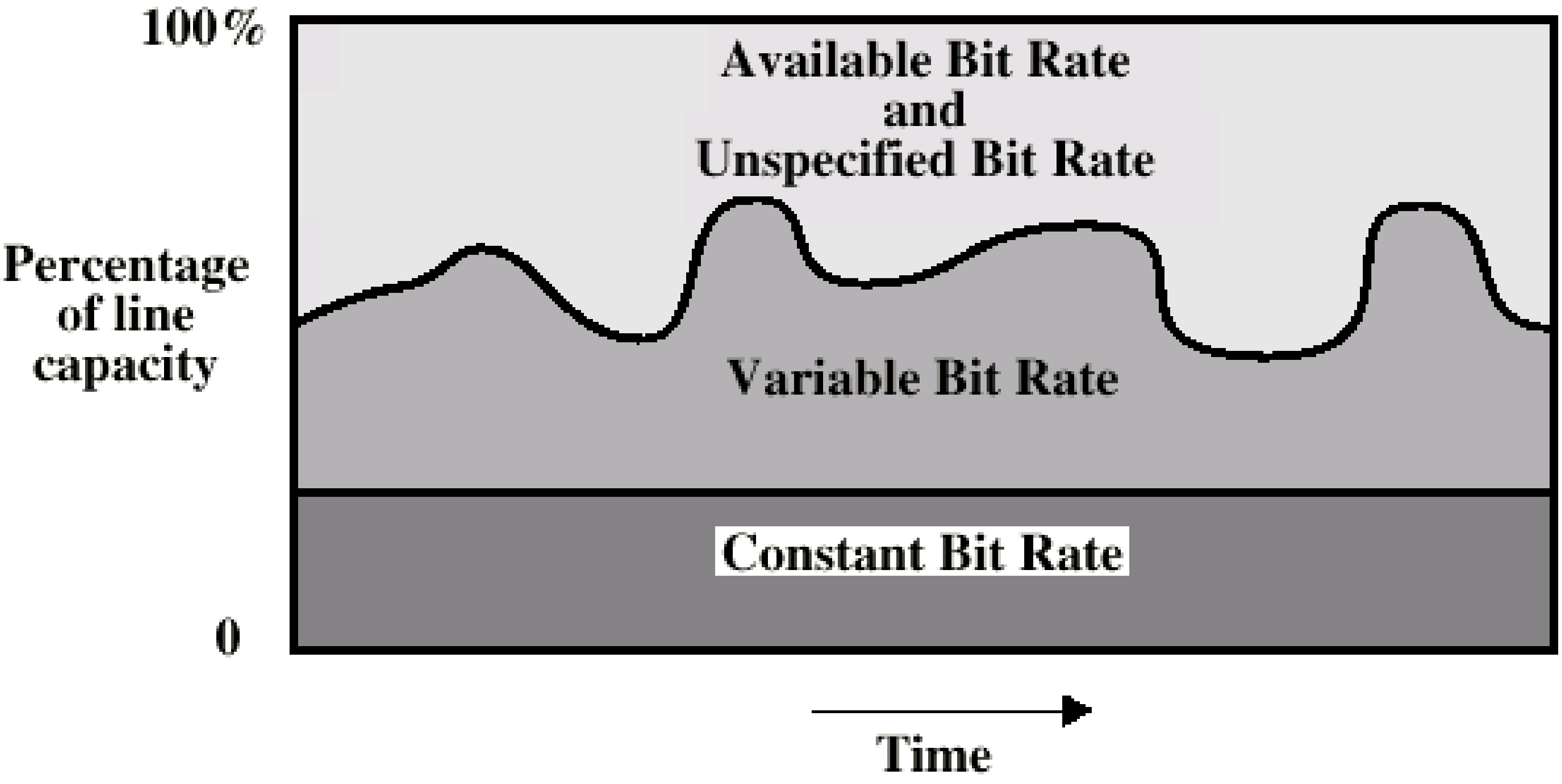
Header error control

Information field
(48 octets)

(a) User-Network Interface

(b) Network-Network Interface

ATM Bit Rate Services



- For Detail Study Please Refer the text Book!!
- Thank you.