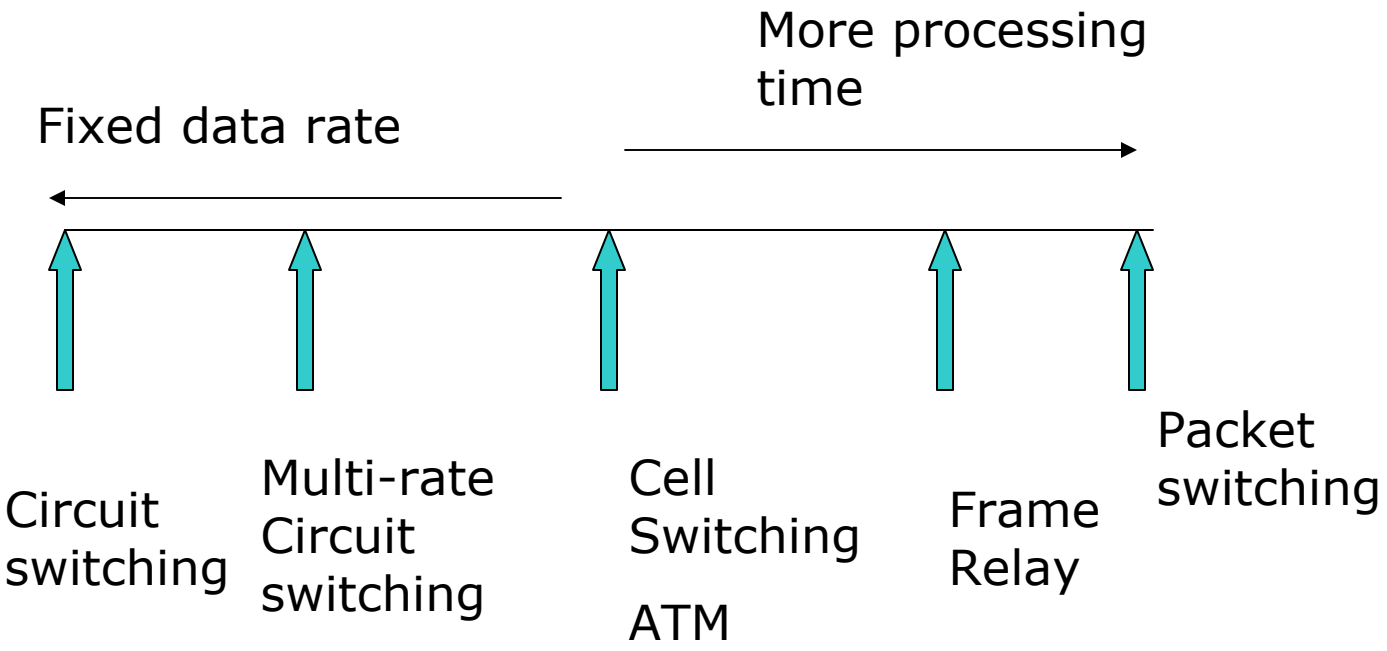
Arab Academy for Science, Technology & Maritime Transport
Computer Engineering Dept.

Computer Networks II
CC514

Switching Techniques



- Circuit Switching

Dedicated communications path established for the duration of the conversation
e.g. telephone network

- Packet Switching

Data sent out of sequence
Small chunks (packets) of data at a time
Packets passed from node to node between source and destination
Used for terminal to computer and computer to computer communications

- Frame Relay

Packet switching systems have large overheads to compensate for errors
Modern systems are more reliable
Errors can be caught in end system
Most overhead for error control is stripped out

- Asynchronous Transfer Mode
  ATM

Evolution of frame relay
Little overhead for error control
Fixed packet (called cell) length
Anything from 10Mbps to Gbps
Constant data rate using packet switching technique

Synchronous versus Asynchronous Transmission

- Synchronous:

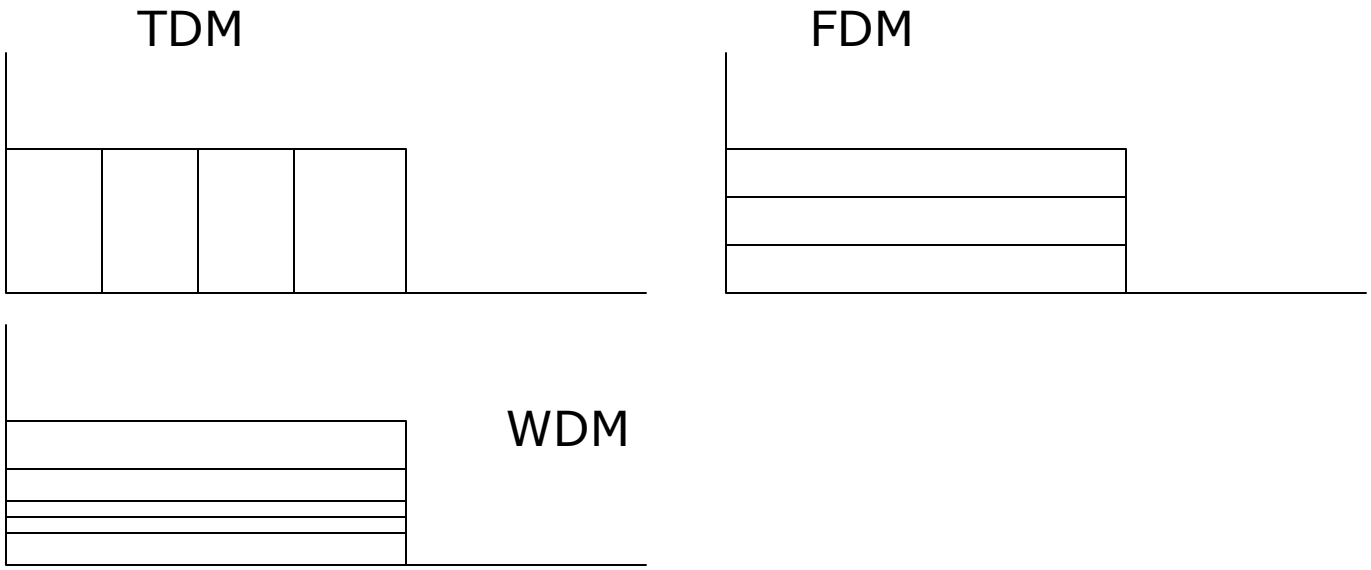
Start, End bits

Code rate = Bi/Bt

- Asynchronous:

Framing with start and end flags

FDM, TDM, WDT



LAN Applications

- Personal computer LANs
  - Low cost
  - Limited data rate
- Back end networks and storage area networks
  - Interconnecting large systems (mainframes and large storage devices)
    - High data rate
    - High speed interface
    - Distributed access
    - Limited distance
    - Limited number of devices

LAN Applications (cont.)

- High speed office networks
  - Desktop image processing
  - High capacity local storage
- Backbone LANs
  - Interconnect low speed local LANs
  - Reliability
  - Capacity
  - Cost

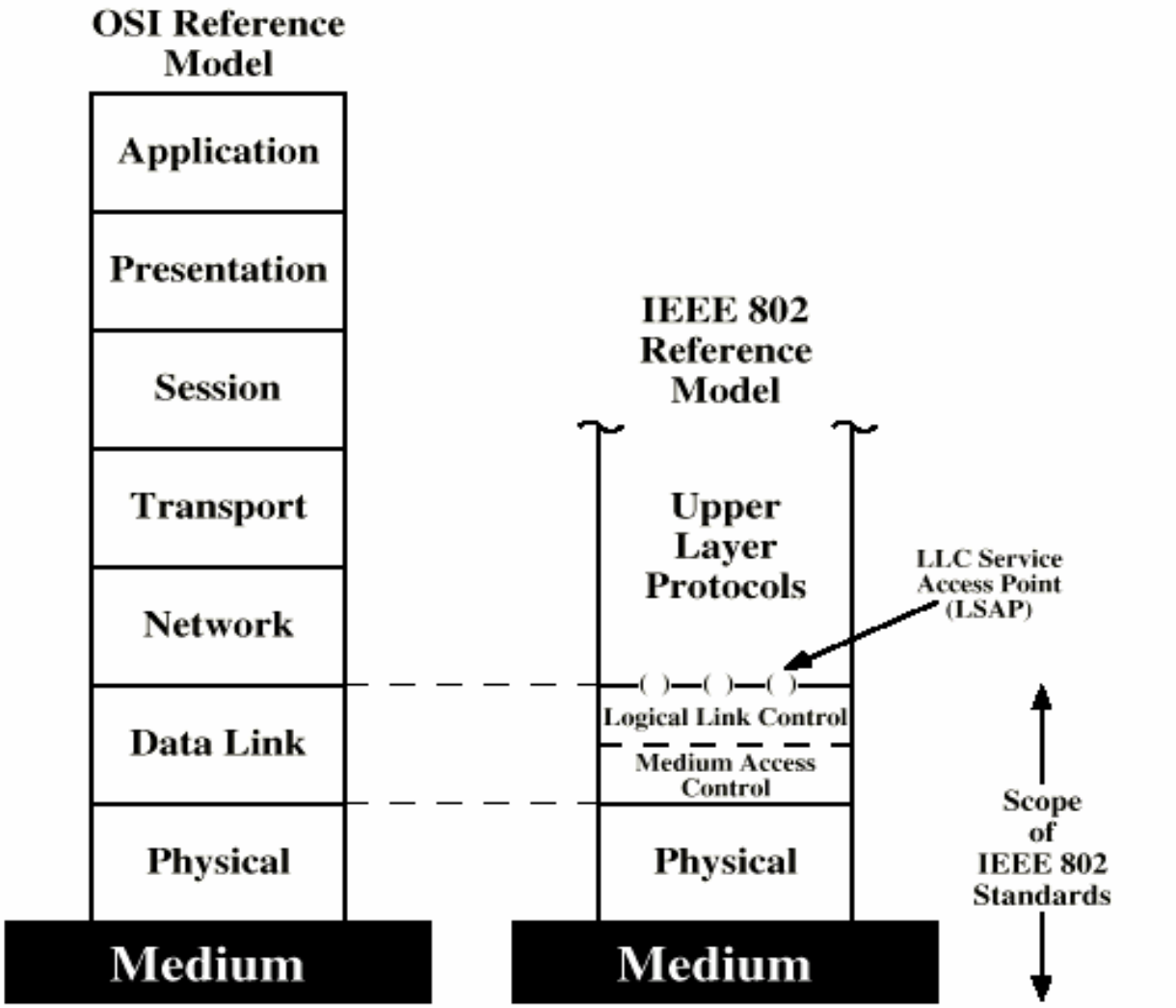
LAN Architecture

- Protocol architecture
- Topologies
- Media access control
- Logical Link Control

Network Architecture Features

- Addressing
- Packet size
- Access mechanism
- Timeouts
- Error recovery
- Status reporting
- Routing
- User access control
- Connection based or connectionless

IEEE 802 v OSI



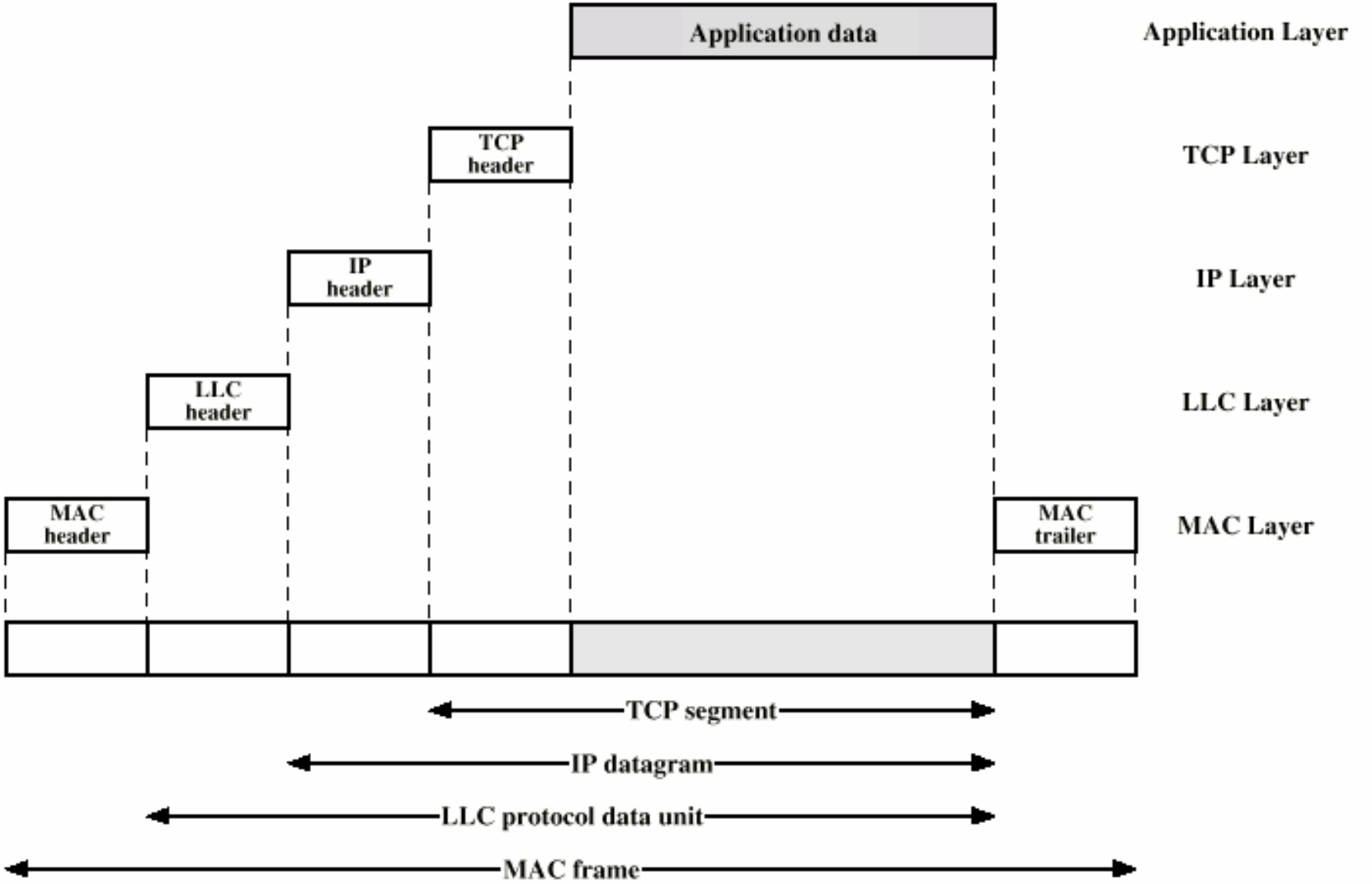
802 Layers - physical

- Encoding/decoding
- Preamble generation/removal
- Bit transmission/reception
- Transmission medium and topology

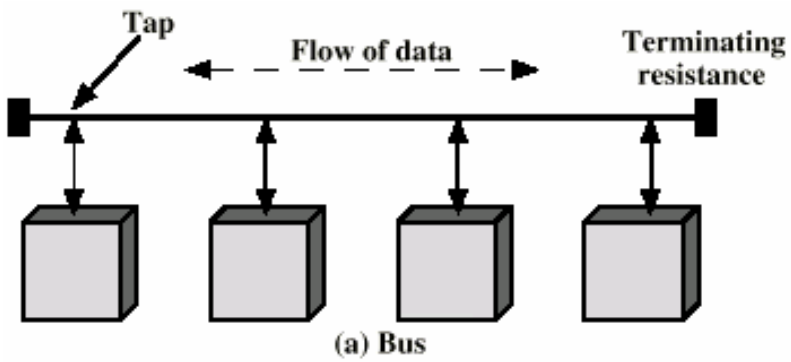
802 Layers - Logical Link Control

- Interface to higher levels
- Flow and error control

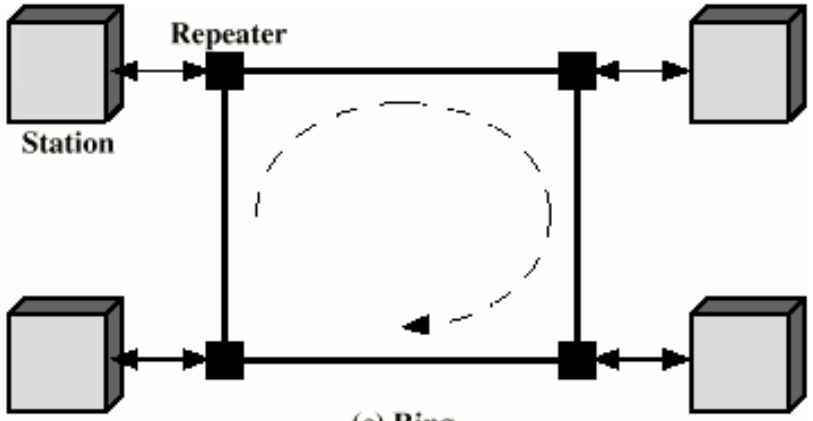
LAN Protocols in Context



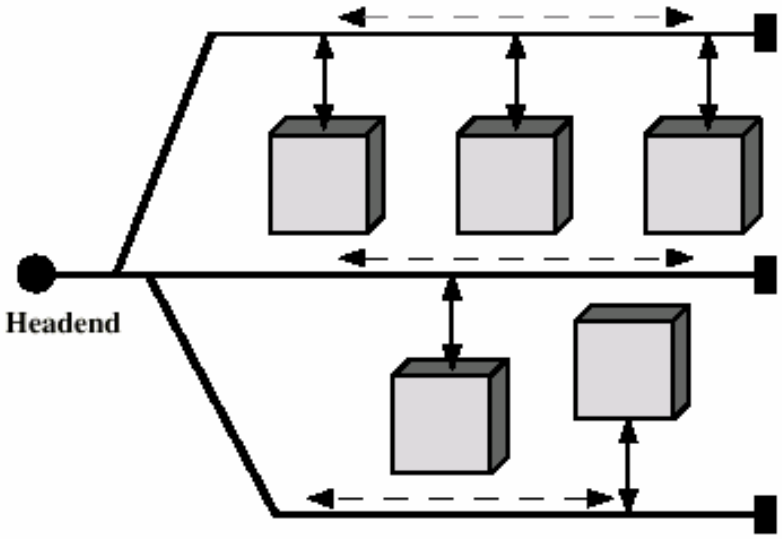
LAN Topologies



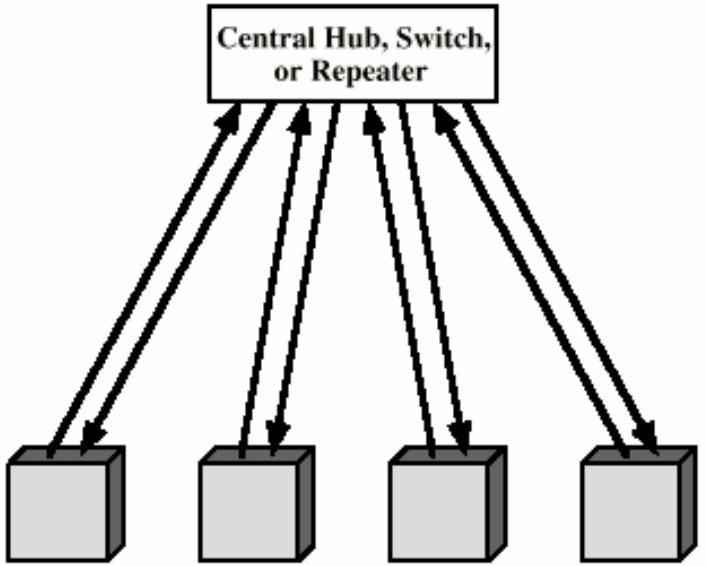
(a) Bus



(c) Ring



(b) Tree



(d) Star

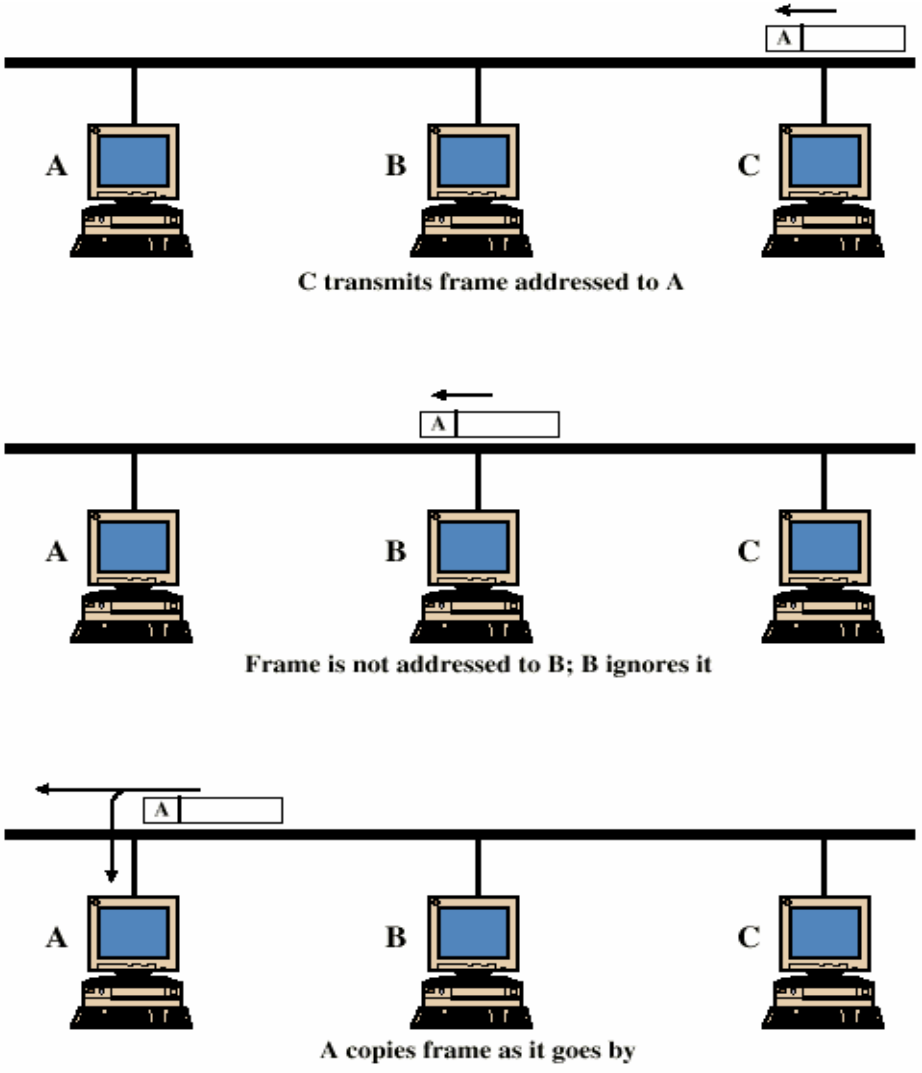
Ring Topology

- Repeaters joined by point to point links in closed loop
  - Receive data on one link and retransmit on another
  - Links unidirectional
  - Stations attach to repeaters

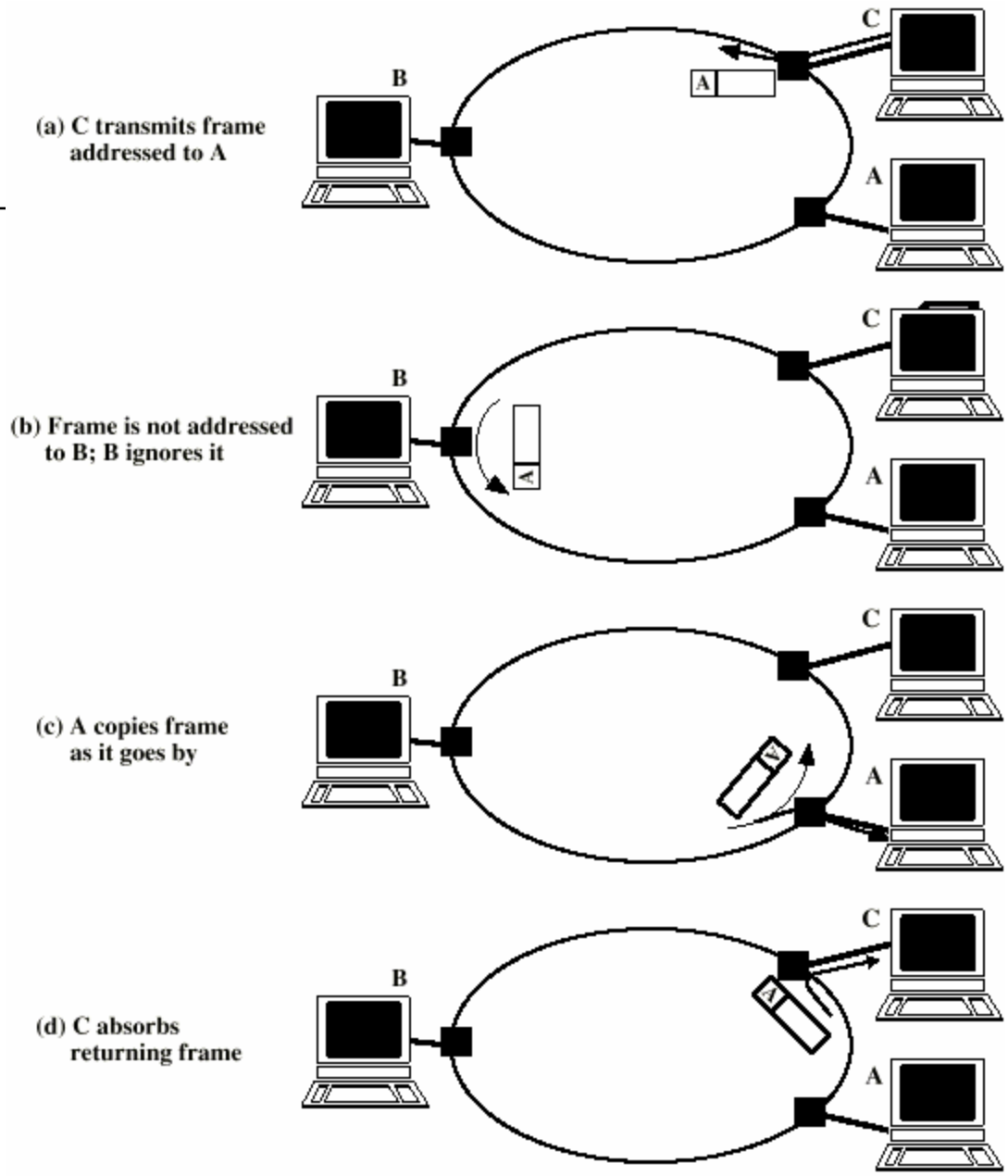
Ring Topology (cont.)

- Data in frames
  - Circulate past all stations
  - Destination recognizes address and copies frame
  - Frame circulates back to source where it is removed
- Media access control determines when station can insert frame

Frame Transmission - Bus LAN



Frame Transmission Ring LAN



Star Topology

- Each station connected directly to central node
  - Usually via two point to point links
- Central node can broadcast
  - Physical star, logical bus
  - Only one station can transmit at a time
- Central node can act as frame switch

Media Access Control

- Where
  - Central
    - Greater control
    - Simple access logic at station
    - Avoids problems of co-ordination
    - Single point of failure
    - Potential bottleneck
  - Distributed

Media Access Control (cont.)

- How
  - Synchronous
    - Specific capacity dedicated to connection
  - Asynchronous
    - In response to demand

Asynchronous Systems

- Round robin
  - Good if many stations have data to transmit over extended period
- Reservation
  - Good for stream traffic

Asynchronous Systems (cont.)

- Contention
  - Good for bursty traffic
  - All stations contend for time
  - Distributed
  - Simple to implement
  - Efficient under moderate load
  - Tend to collapse under heavy load

MAC Frame Format

- MAC layer receives data from LLC layer
- MAC control
- Destination MAC address
- Source MAC address

MAC Frame Format

- LLS
- CRC
- MAC layer detects errors and discards frames
- LLC optionally retransmits unsuccessful frames

Bus and Tree

- Multipoint medium
- Transmission propagates throughout medium
- Heard by all stations
  - Need to identify target station
    - Each station has unique address
- Full duplex connection between station and tap
  - Allows for transmission and reception

Bus and Tree

- Need to regulate transmission
  - To avoid collisions
  - To avoid hogging
    - Data in small blocks - frames
- Terminator absorbs frames at end of medium

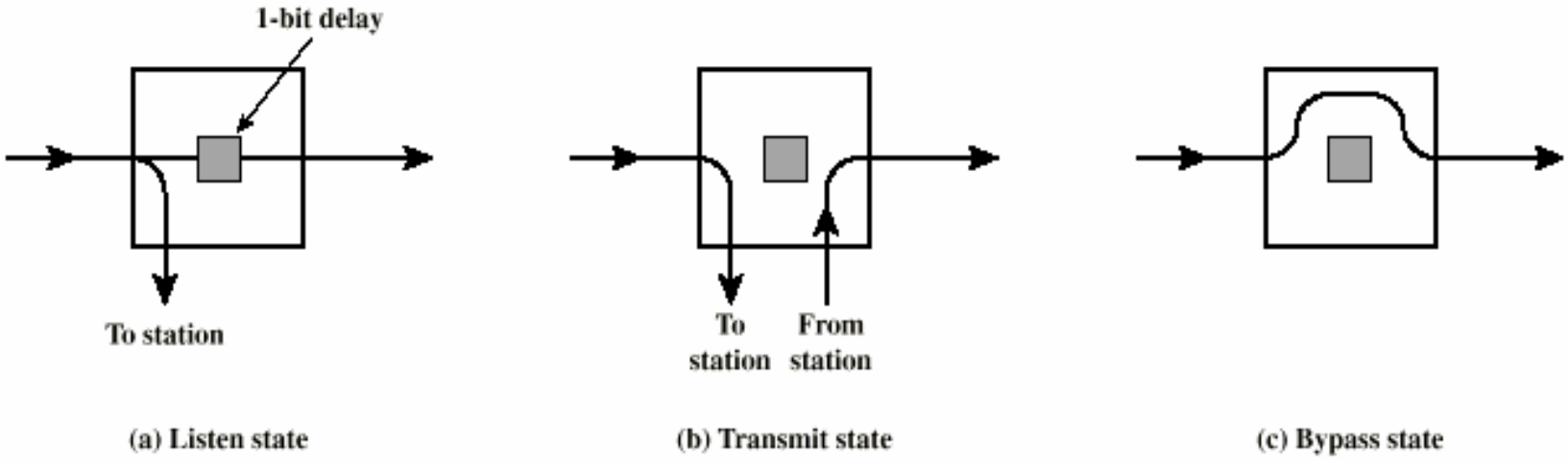
Star Topology

- Each station connected directly to central node
  - Usually via two point to point links
- Central node can broadcast
  - Physical star, logical bus
  - Only one station can transmit at a time
- Central node can act as frame switch

Repeaters

- Transmits in both directions
- Joins two segments of cable
- No buffering
- No logical isolation of segments
- If two stations on different segments send at the same time, packets will collide
- Only one path of segments and repeaters between any two stations

Ring Repeater States



(a) Listen state

(b) Transmit state

(c) Bypass state

Listen State Functions

- Scan passing bit stream for patterns
  - Address of attached station
  - Token permission to transmit
- Copy incoming bit and send to attached station
  - Whilst forwarding each bit
- Modify bit as it passes
  - e.g. to indicate a packet has been copied (ACK)

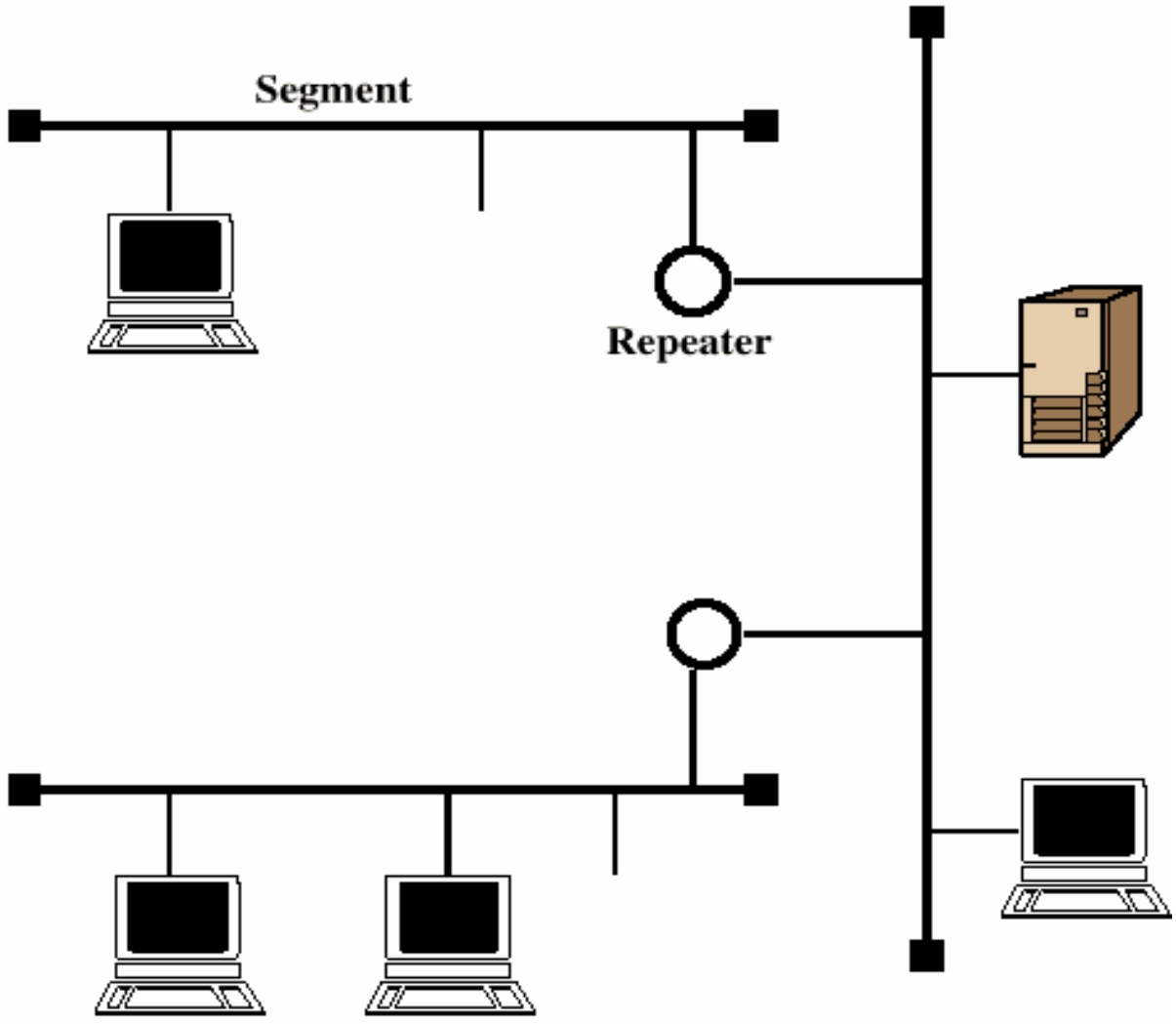
Transmit State Functions

- Station has data
- Repeater has permission
- May receive incoming bits
  - If ring bit length shorter than packet
    - Pass back to station for checking (ACK)
  - May be more than one packet on ring
    - Buffer for retransmission later

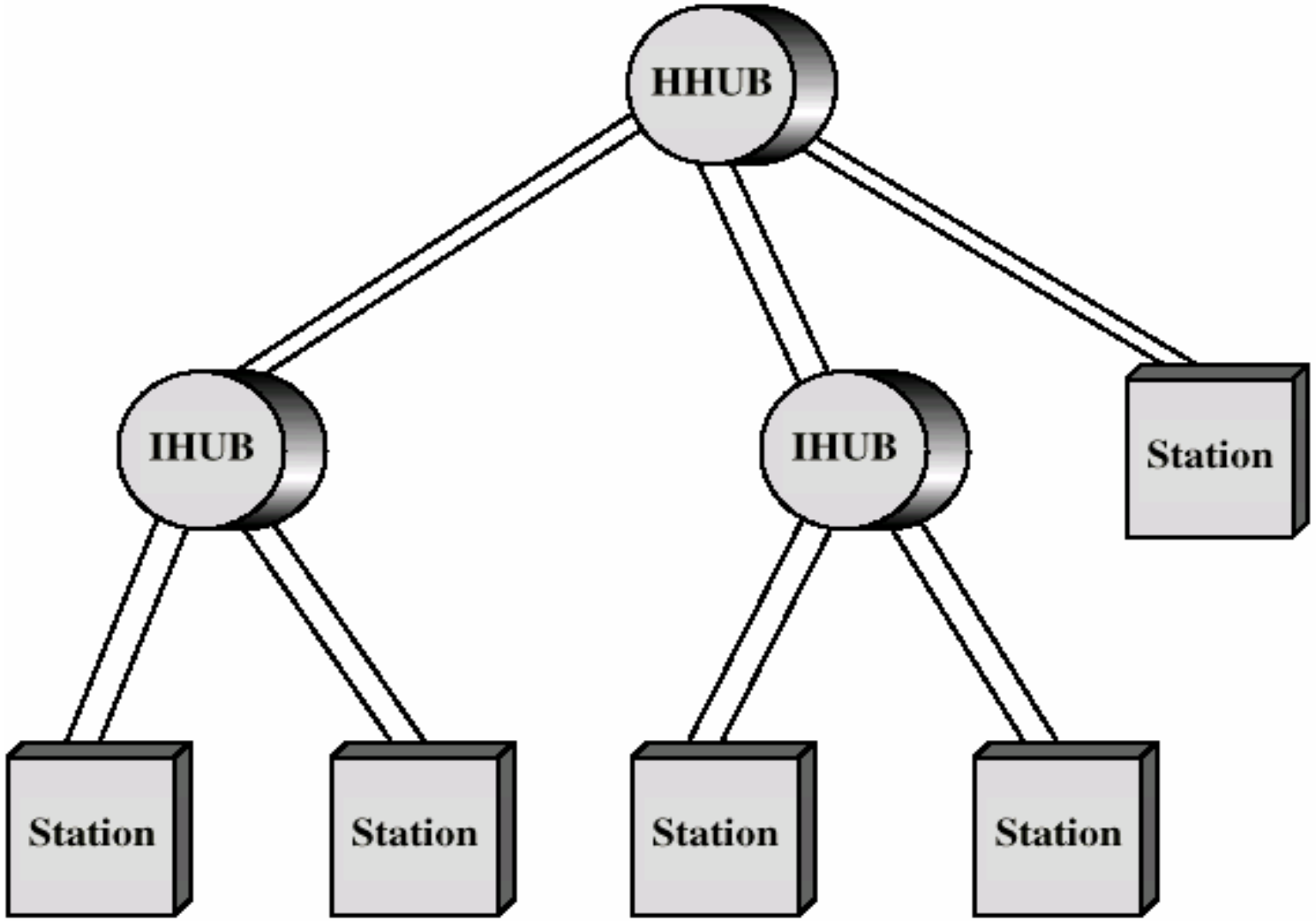
Bypass State

- Signals propagate past repeater with no delay (other than propagation delay)
- Partial solution to reliability problem (see later)
- Improved performance

Baseband Configuration



Two Level Star Topology



Bridges

- Ability to expand beyond single LAN
- Provide interconnection to other LANs/WANs
- Use Bridge or router

Bridges (cont.)

- Bridge is simpler
  - Connects similar LANs
  - Identical protocols for physical and link layers
  - Minimal processing
- Router more general purpose
  - Interconnect various LANs and WANs
  - see later

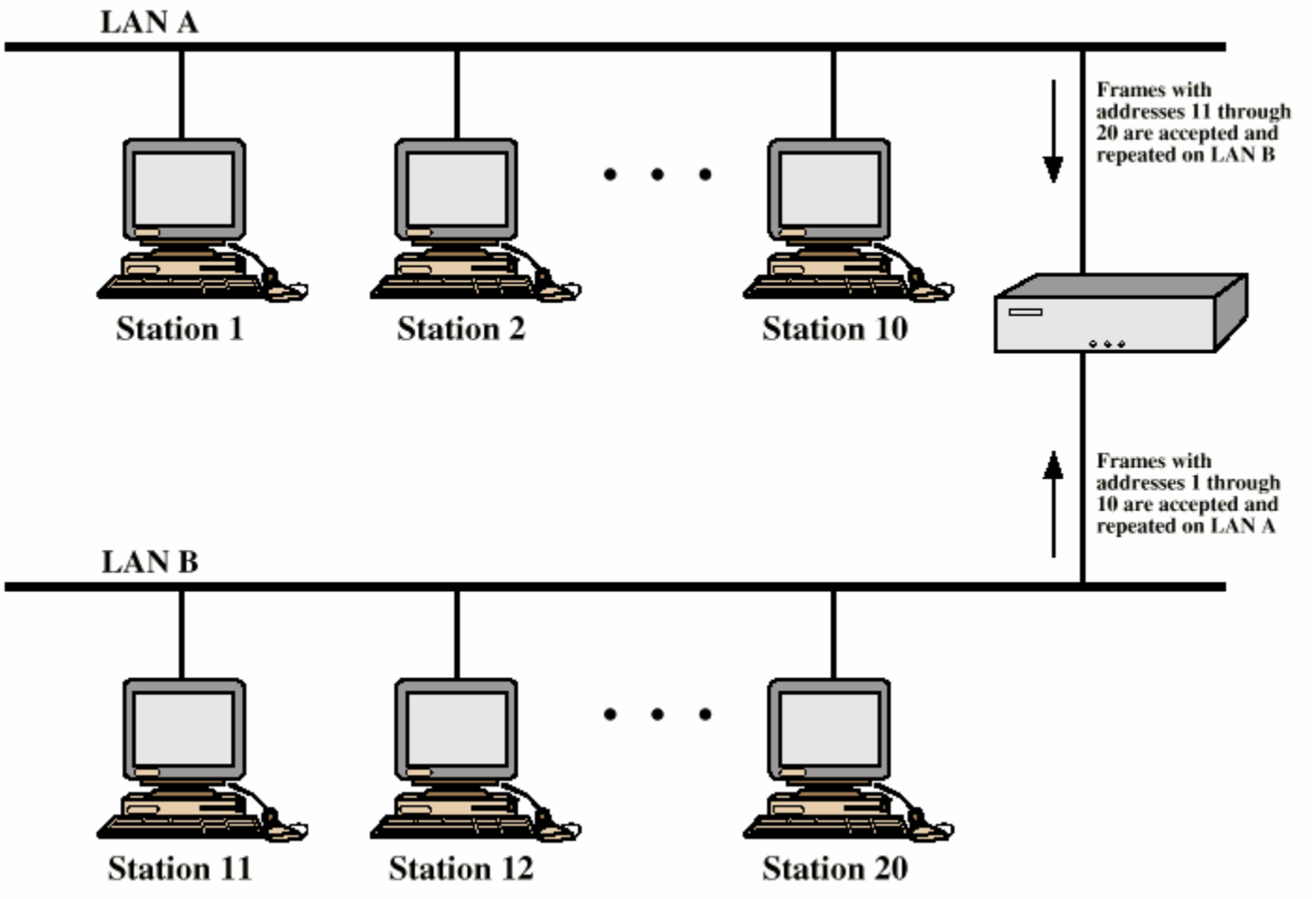
Why Bridge?

- Reliability
- Performance
- Security
- Geography

Functions of a Bridge

- Read all frames transmitted on one LAN and accept those address to any station on the other LAN
- Using MAC protocol for second LAN, retransmit each frame
- Do the same the other way round

Bridge Operation



Bridge Design Aspects

- No modification to content or format of frame
- No encapsulation
- Exact bitwise copy of frame
- Minimal buffering to meet peak demand

Bridge Design Aspects (cont.)

- Contains routing and address intelligence
  - Must be able to tell which frames to pass
  - May be more than one bridge to cross
- May connect more than two LANs
- Bridging is transparent to stations
  - Appears to all stations on multiple LANs as if they are on one single LAN

Bridge Protocol Architecture

- IEEE 802.1D
- MAC level
  - Station address is at this level
- Bridge does not need LLC layer
  - It is relaying MAC frames

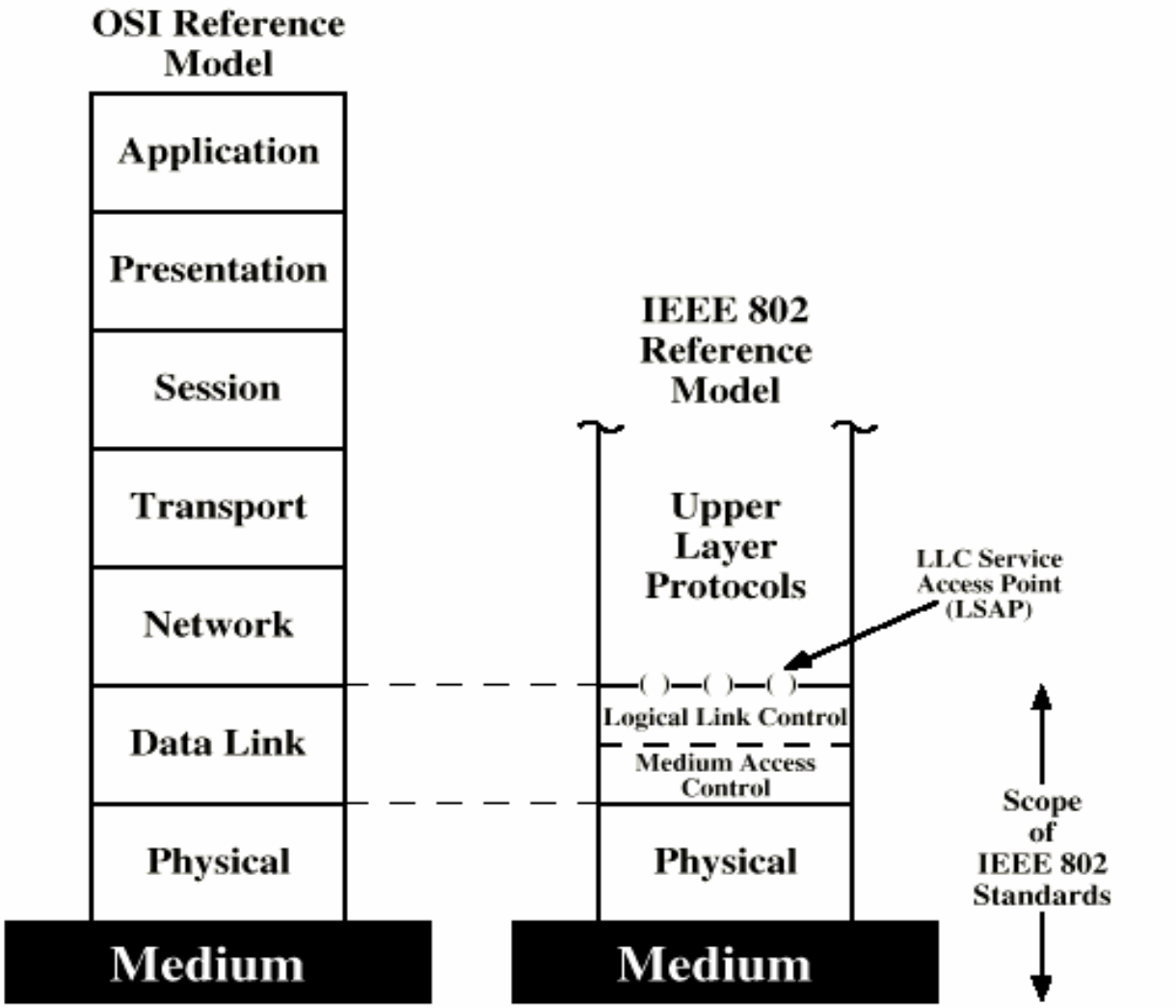
Bridge Protocol Architecture (cont.)

- Can pass frame over external communications system
  - For example WAN link
  - Capture frame
  - Encapsulate it
  - Forward it across link
  - Remove encapsulation and forward over LAN link

Protocol Architecture

- Lower layers of OSI model
- IEEE 802 reference model
- Physical
- Logical link control (LLC)
- Media access control (MAC)

IEEE 802 v OSI



Logical Link Control

- Transmission of link level PDUs between two stations
- Must support multi-access, shared medium
- Relieved of some link access details by MAC layer
- Addressing involves specifying source and destination LLC users
  - Referred to as service access points (SAP)
  - Typically higher level protocol

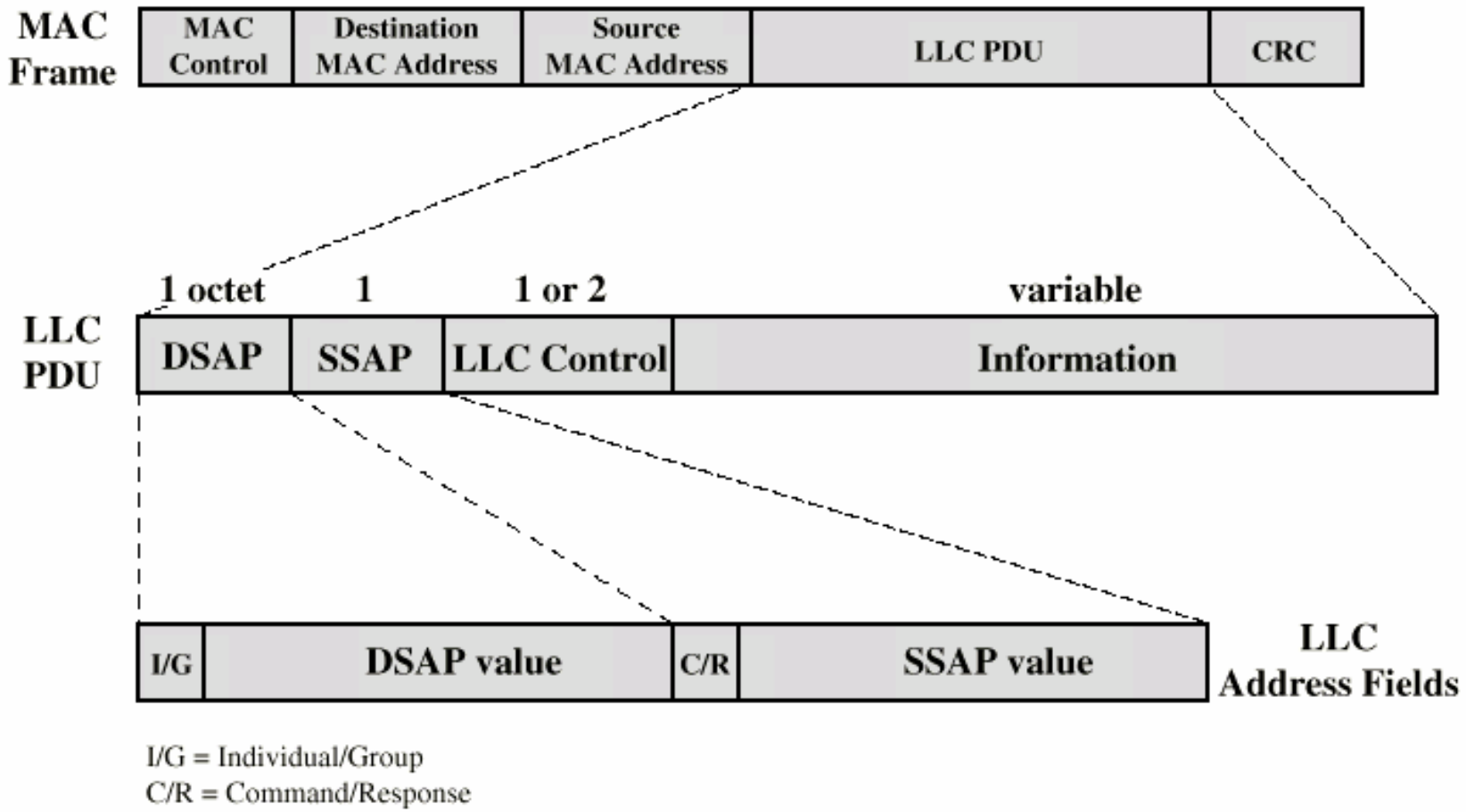
LLC Services

- Based on HDLC
- Unacknowledged connectionless service
- Connection mode service
- Acknowledged connectionless service

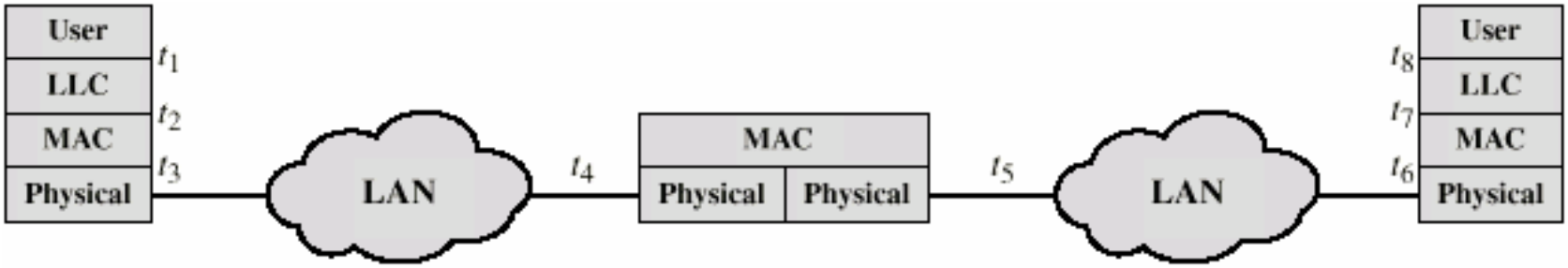
LLC Protocol

- Modeled after HDLC
- Asynchronous balanced mode to support connection mode LLC service (type 2 operation)
- Unnumbered information PDUs to support Acknowledged connectionless service (type 1)
- Multiplexing using LSAPs

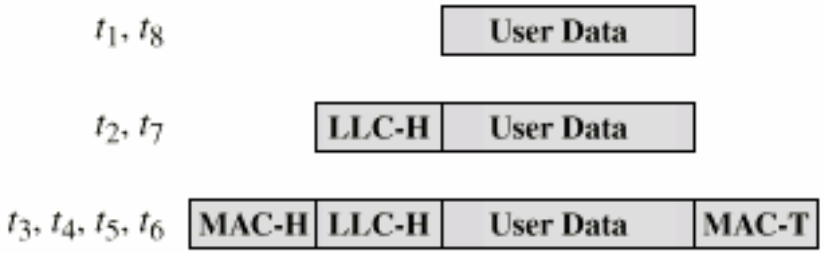
Typical Frame Format



Bridge Connection of Two LANs

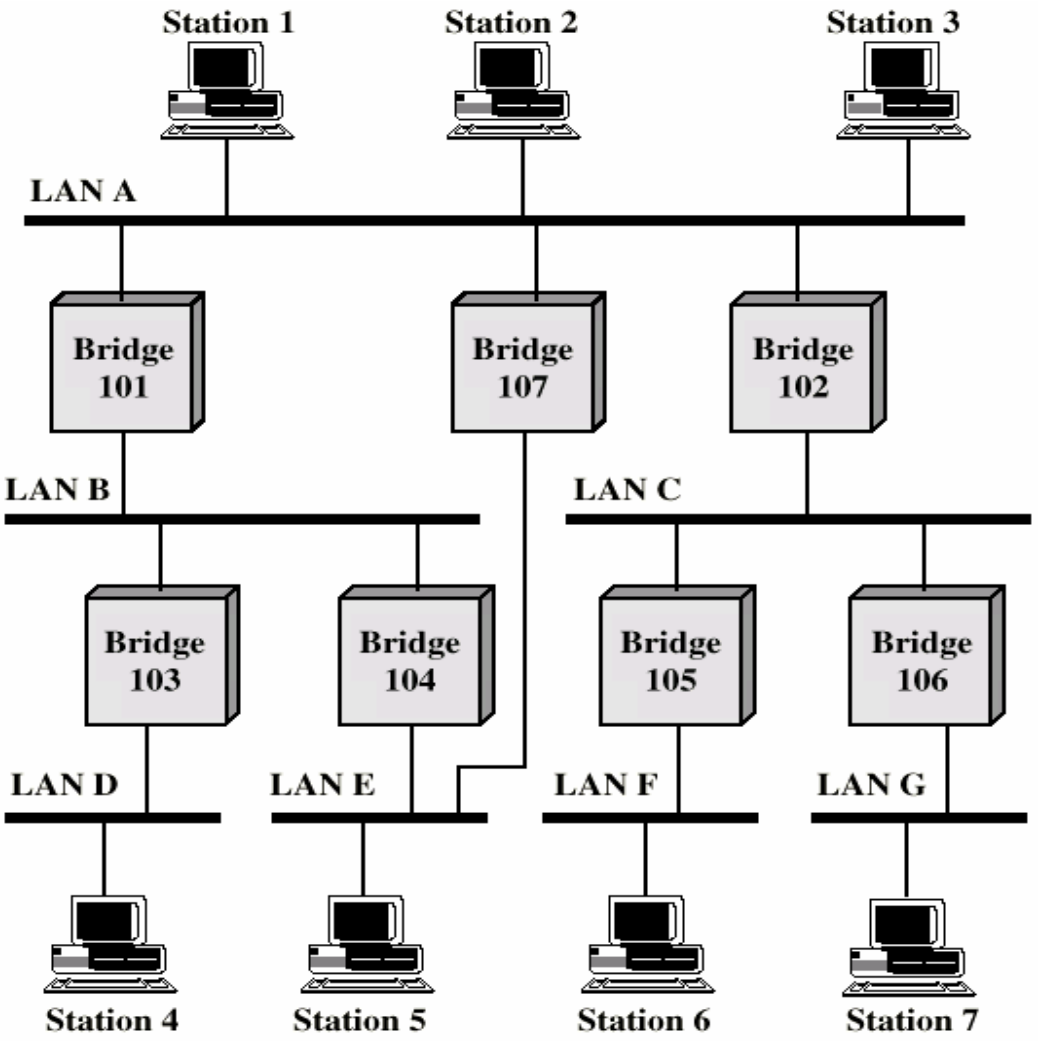


(a) Architecture

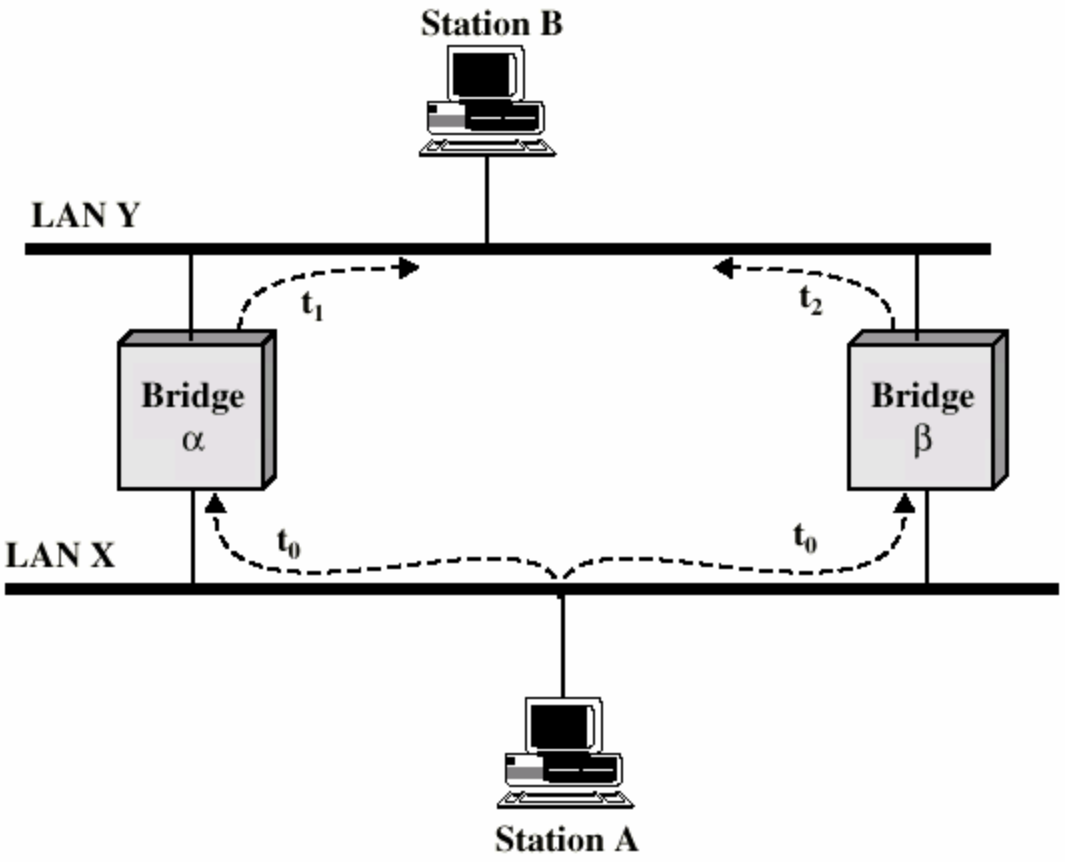


(b) Operation

Multiple LANs



Loop of Bridges



Internetworking Terms

- Communications Network
  - Facility that provides data transfer service
- An internet
  - Collection of communications networks interconnected by bridges and/or routers

Internetworking Terms (cont.)

- The Internet - note upper case I
  - The global collection of thousands of individual machines and networks
- Intranet
  - Corporate internet operating within the organization
  - Uses Internet (TCP/IP and http) technology to deliver documents and resources

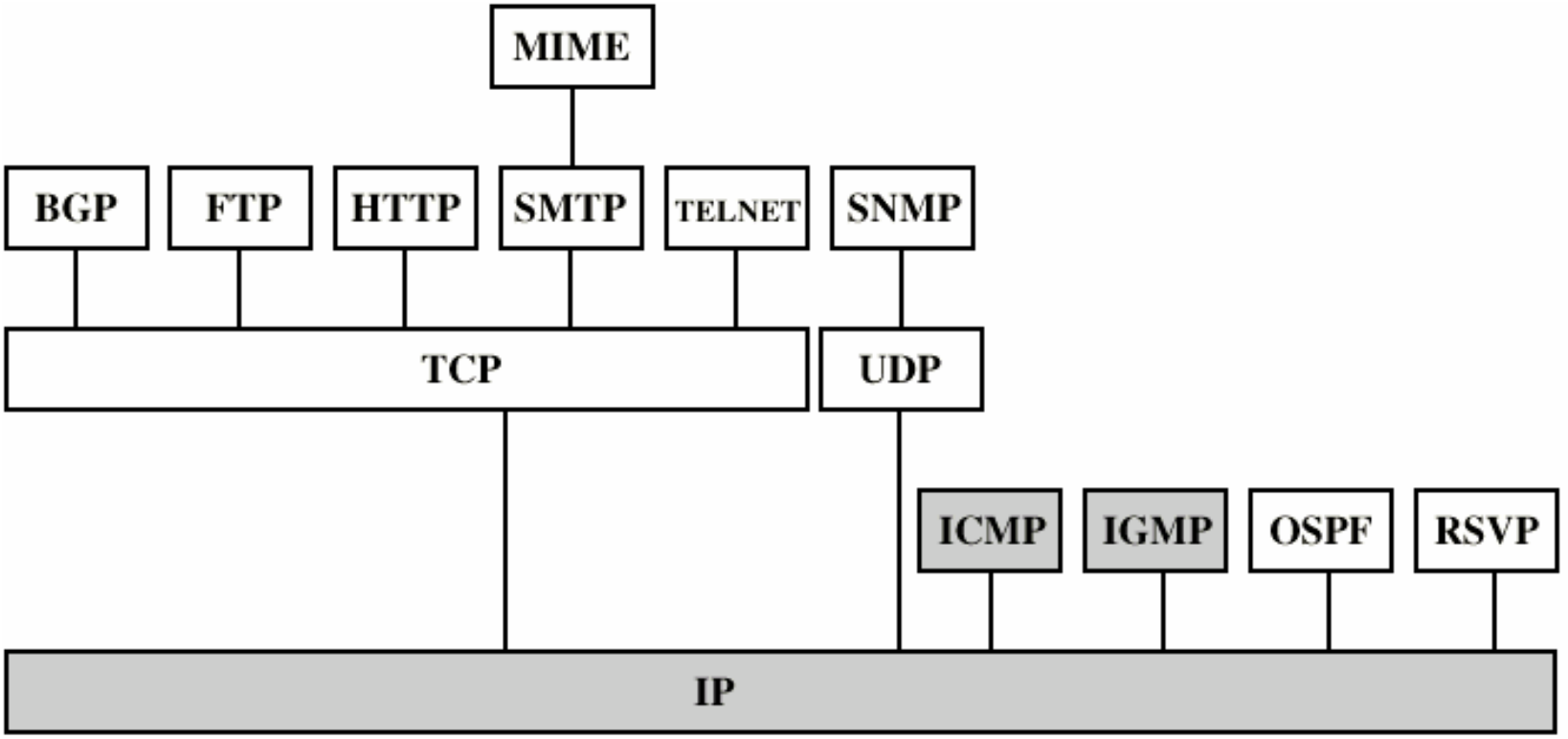
Internetworking Terms (cont.)

- End System (ES)
  - Device attached to one of the networks of an internet
  - Supports end-user applications or services
- Intermediate System (IS)
  - Device used to connect two networks
  - Permits communication between end systems attached to different networks

Internetworking Terms (cont.)

- Bridge
  - IS used to connect two LANs using similar LAN protocols
  - Address filter passing on packets to the required network only
  - OSI layer 2 (Data Link)
- Router
  - Connects two (possibly dissimilar) networks
  - Uses internet protocol present in each router and end system
  - OSI Layer 3 (Network)

Internetworking Protocols



Requirements of Internetworking

- Link between networks
  - Minimum physical and link layer
- Routing and delivery of data between processes on different networks
- Accounting services and status info
- Independent of network architectures

Network Architecture Features

- Addressing
- Packet size
- Access mechanism
- Timeouts
- Error recovery
- Status reporting
- Routing
- User access control
- Connection based or connectionless

Architectural Approaches

- Connection oriented
- Connectionless

Connection Oriented

- Assume that each network is connection oriented
- IS connect two or more networks
  - IS appear as DTE to each network
  - Logical connection set up between DTEs
    - Concatenation of logical connections across networks
  - Individual network virtual circuits joined by IS

Connection Oriented (cont.)

- May require enhancement of local network services
  - 802, FDDI are datagram services

Connection Oriented IS Functions

- Relaying
- Routing
- e.g. X.75 used to interconnect X.25 packet switched networks
- Connection oriented not often used
  - (IP dominant)

Connectionless Operation

- Corresponds to datagram mechanism in packet switched network
- Each NPDU treated separately
- Network layer protocol common to all DTEs and routers
  - Known generically as the internet protocol

Connectionless Operation (cont.)

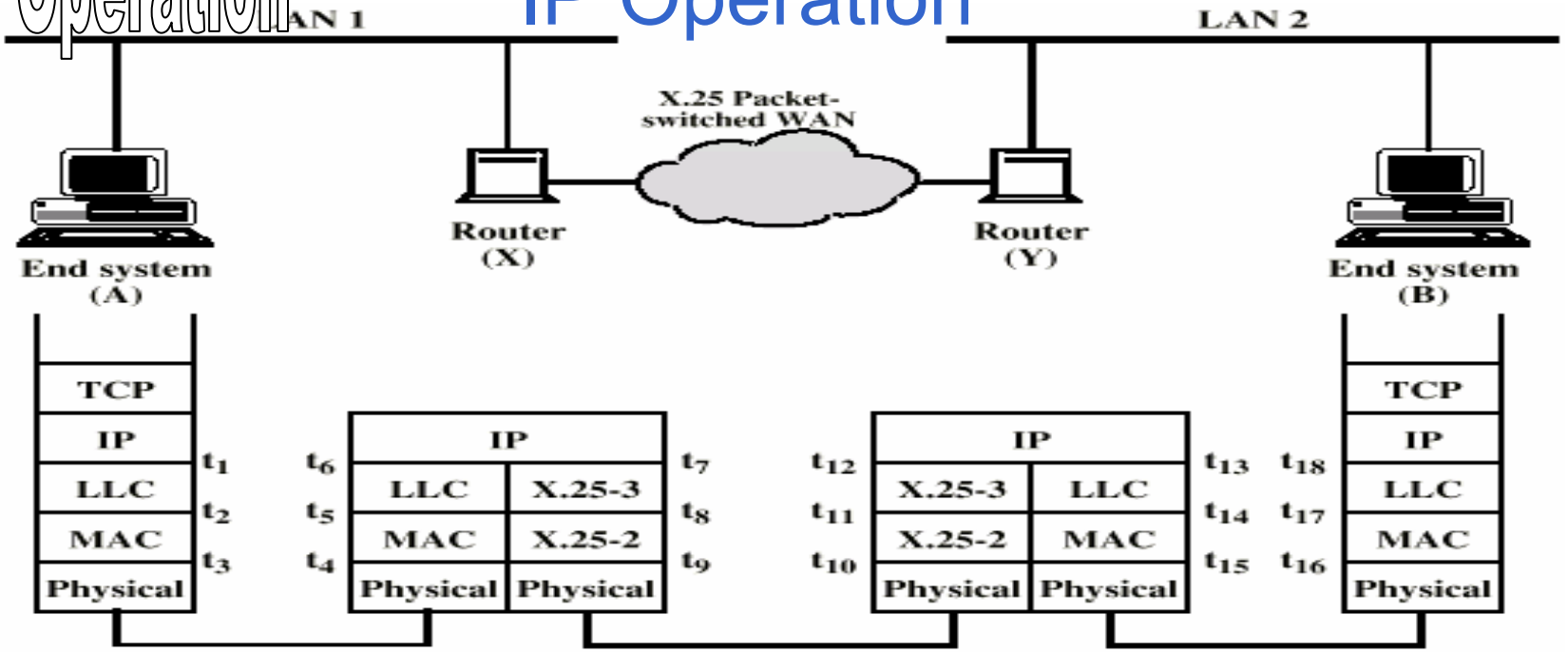
- Internet Protocol
  - One such internet protocol developed for ARPANET
  - RFC 791 (Get it and study it)
- Lower layer protocol needed to access particular network

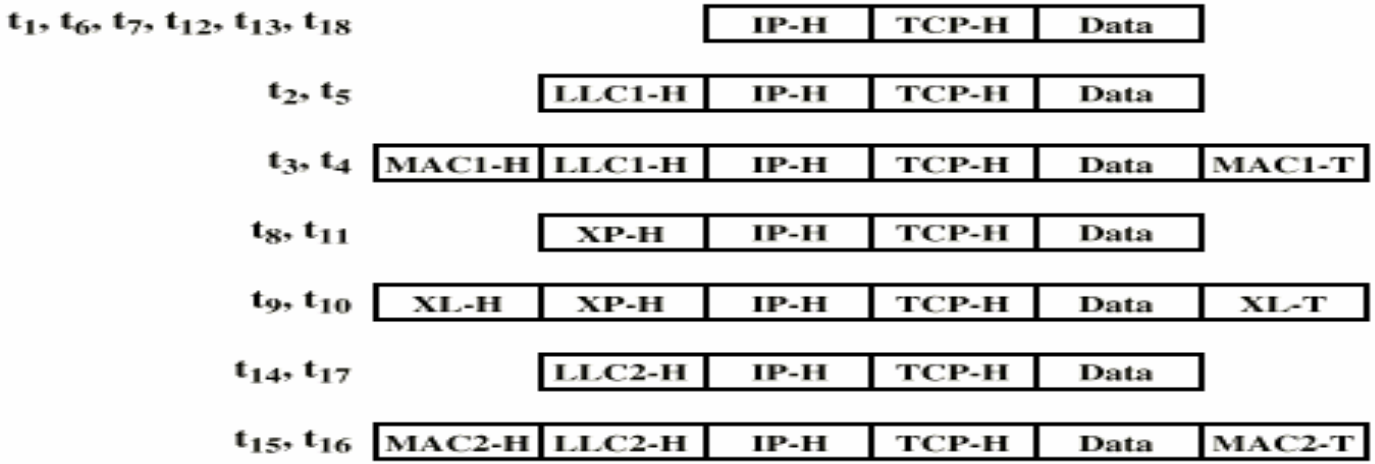
Connectionless Internetworking

- Advantages
  - Flexibility
  - Robust
  - No unnecessary overhead
- Unreliable
  - Not guaranteed delivery
  - Not guaranteed order of delivery
    - Packets can take different routes
  - Reliability is responsibility of next layer up (e.g. TCP)

Router Operation

IP Operation





TCP-H = TCP header
IP-H = IP header
LLCi-H = LLC header
MACi-H = MAC header
MACi-T = MAC trailer
XP-H = X.25 packet header
XL-H = X.25 link header
XL-T = X.25 link trailer

Design Issues

- Routing
- Datagram lifetime
- Fragmentation and re-assembly
- Error control
- Flow control

Routing

- End systems and routers maintain routing tables
  - Indicate next router to which datagram should be sent
  - Static
    - May contain alternative routes
  - Dynamic
    - Flexible response to congestion and errors

Routing (cont.)

- Source routing
  - Source specifies route as sequential list of routers to be followed
  - Security
  - Priority
- Route recording

Datagram Lifetime

- Datagrams could loop indefinitely
  - Consumes resources
  - Transport protocol may need upper bound on datagram life

Datagram Lifetime (cont.)

- Datagram marked with lifetime
  - Time To Live field in IP
  - Once lifetime expires, datagram discarded (not forwarded)
  - Hop count
    - Decrement time to live on passing through a each router
  - Time count
    - Need to know how long since last router
- (Aside: compare with Logan's Run)

Fragmentation and Re-assembly

- Different packet sizes
- When to re-assemble
  - At destination
    - Results in packets getting smaller as data traverses internet
  - Intermediate re-assembly
    - Need large buffers at routers
    - Buffers may fill with fragments
    - All fragments must go through same router
      - Inhibits dynamic routing

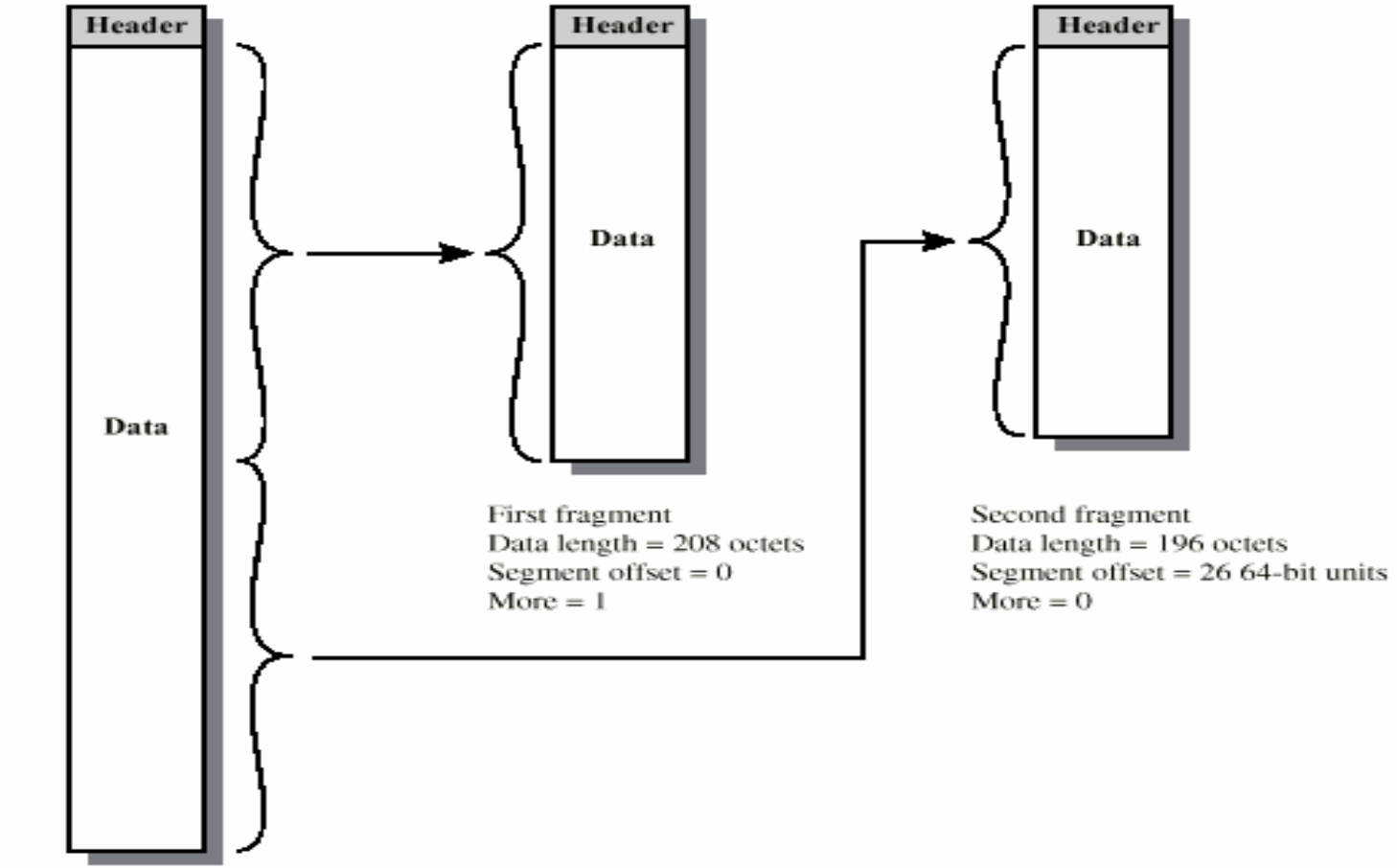
IP Fragmentation

- IP re-assembles at destination only
- Uses fields in header
  - Data Unit Identifier (ID)
    - Identifies end system originated datagram
      - Source and destination address
      - Protocol layer generating data (e.g. TCP)
      - Identification supplied by that layer
  - Data length
    - Length of user data in octets

IP Fragmentation (cont.)

- Offset
  - Position of fragment of user data in original datagram
  - In multiples of 64 bits (8 octets)
- *More* flag
  - Indicates that this is not the last fragment

Fragmentation Example



Dealing with Failure

- Re-assembly may fail if some fragments get lost
- Need to detect failure
- Re-assembly time out
  - Assigned to first fragment to arrive
  - If timeout expires before all fragments arrive, discard partial data
- Use packet lifetime (time to live in IP)
  - If time to live runs out, kill partial data

Error Control

- Not guaranteed delivery
- Router should attempt to inform source if packet discarded
  - e.g. for time to live expiring
- Source may modify transmission strategy
- May inform high layer protocol
- Datagram identification needed
- (Look up ICMP)

Flow Control

- Allows routers and/or stations to limit rate of incoming data
- Limited in connectionless systems
- Send flow control packets
  - Requesting reduced flow
- e.g. ICMP

Internet Protocol (IP)

- Part of TCP/IP
  - Used by the Internet
- Specifies interface with higher layer
  - e.g. TCP
- Specifies protocol format and mechanisms

IP Services

- Primitives
  - Functions to be performed
  - Form of primitive implementation dependent
    - e.g. subroutine call
  - Send
    - Request transmission of data unit
  - Deliver
    - Notify user of arrival of data unit
- Parameters
  - Used to pass data and control info

Parameters

- Source address
- Destination address
- Protocol
  - Recipient e.g. TCP
- Type of Service
  - Specify treatment of data unit during transmission through networks

Parameters (cont.)

- Identification
  - Source, destination address and user protocol
  - Uniquely identifies PDU
  - Needed for re-assembly and error reporting
  - Send only

Parameters (cont.)

- Don’t fragment indicator
  - Can IP fragment data
  - If not, may not be possible to deliver
  - Send only
- Time to live
  - Send only
- Data length
- Option data
- User data

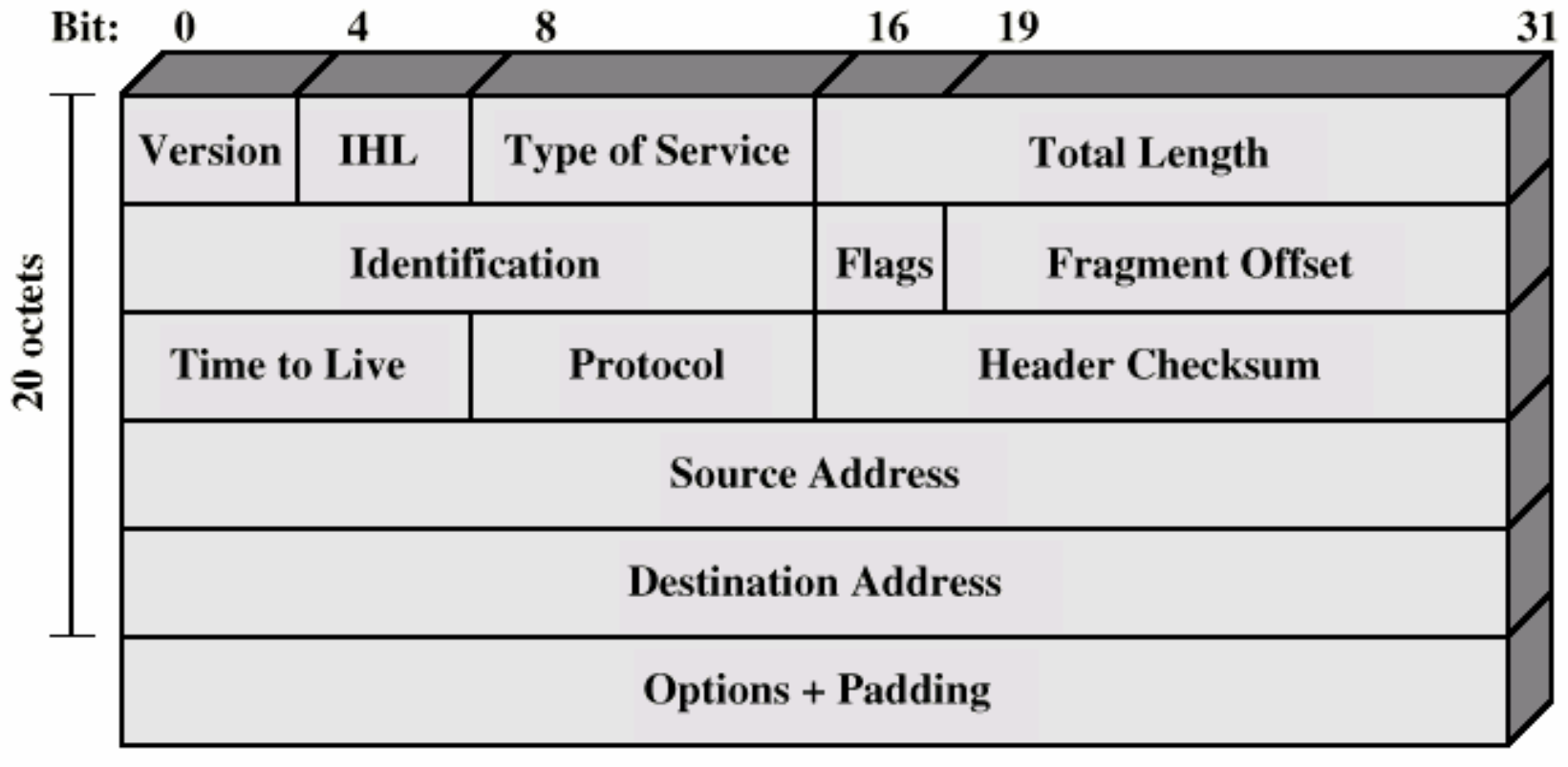
Type of Service

- Precedence
  - 8 levels
- Reliability
  - Normal or high
- Delay
  - Normal or low
- Throughput
  - Normal or high

Options

- Security
- Source routing
- Route recording
- Stream identification
- Time stamping

IP v4 Protocol



Header Fields

- Version
  - Currently 4
  - IP v6 - see later
- Internet header length
  - In 32 bit words
  - Including options
- Type of service
- Total length
  - Of datagram, in octets

Header Fields (cont.)

- Identification
  - Sequence number
  - Used with addresses and user protocol to identify datagram uniquely
- Flags
  - More bit
  - Don’t fragment

Header Fields (cont.)

- Fragmentation offset
- Time to live
- Protocol
  - Next higher layer to receive data field at destination

Header Fields (cont.)

- Header checksum
  - Recomputed at each router
  - 16 bit ones complement sum of all 16 bit words in header
  - Set to zero during calculation
- Source address

Header Fields (cont.)

- Destination address
- Options
- Padding
  - To fill to multiple of 32 bits long

Data Field

- Carries user data from next layer up
- Integer multiple of 8 bits long (octet)
- Max length of datagram (header plus data) 65,535 octets

IP Addresses - Class A

- 32 bit global internet address
- Network part and host part
- Class A
  - Start with binary 0
  - All 0 reserved
  - 01111111 (127) reserved for loopback
  - Range 1.x.x.x to 126.x.x.x
  - All allocated

IP Addresses - Class B

- Start 10
- Range 128.x.x.x to 191.x.x.x
- Second Octet also included in network address
- 2^{14} = 16,384 class B addresses
- All allocated

IP Addresses - Class C

- Start 110
- Range 192.x.x.x to 223.x.x.x
- Second and third octet also part of network address
- 2^{21} = 2,097,152 addresses
- Nearly all allocated
  - See IPv6

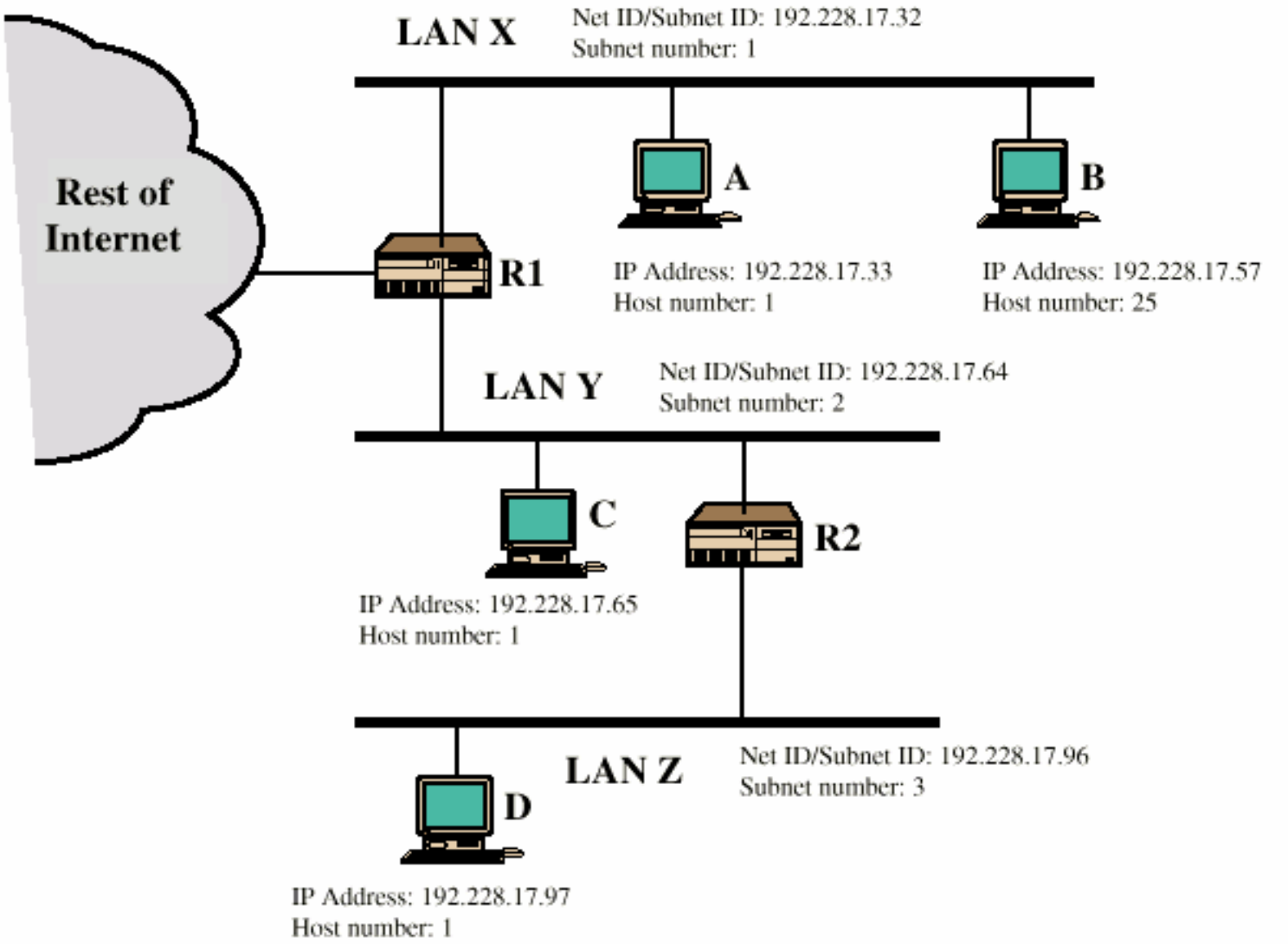
Subnets and Subnet Masks

- Allow arbitrary complexity of inter-networked LANs within organization
- Insulate overall internet from growth of network numbers and routing complexity
- Site looks to rest of internet like single network

Subnets and Subnet Masks (cont.)

- Each LAN assigned subnet number
- Host portion of address partitioned into subnet number and host number
- Local routers route within subnetted network
- Subnet mask indicates which bits are subnet number and which are host number

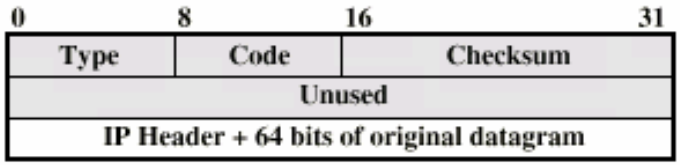
Routing Using Subnets



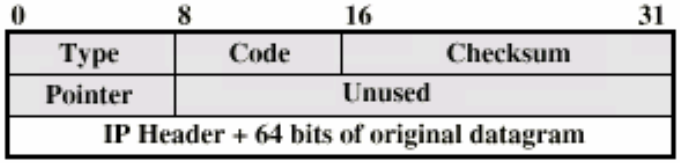
ICMP

- Internet Control Message Protocol
- RFC 792 (get it and study it)
- Transfer of (control) messages from routers and hosts to hosts
- Feedback about problems
  - e.g. time to live expired
- Encapsulated in IP datagram
  - Not reliable

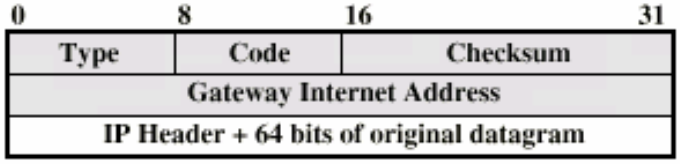
ICMP Message Formats



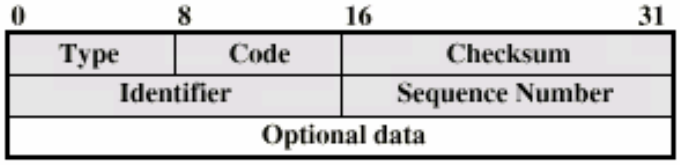
(a) Destination Unreachable; Time Exceeded; Source Quench



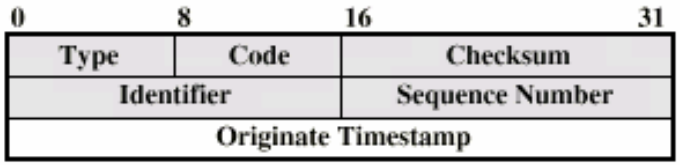
(b) Parameter Problem



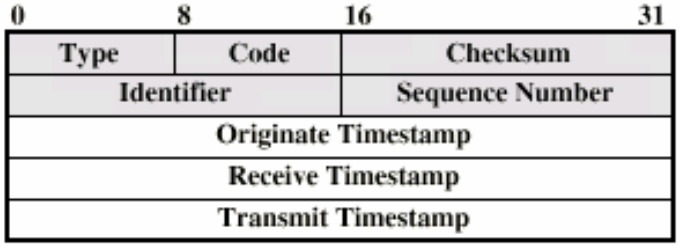
(c) Redirect



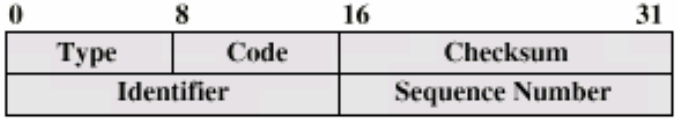
(d) Echo, Echo Reply



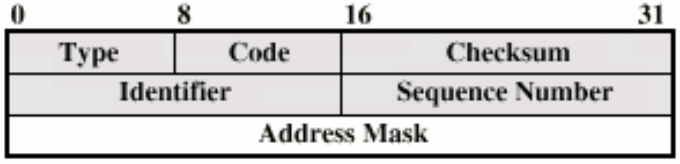
(e) Timestamp



(f) Timestamp Reply



(g) Address Mask Request



(h) Address Mask Reply

IP v6 - Version Number

- IP v 1-3 defined and replaced
- IP v4 - current version
- IP v5 - streams protocol
- IP v6 - replacement for IP v4
  - During development it was called IPng
  - Next Generation

Why Change IP?

- Address space exhaustion
  - Two level addressing (network and host) wastes space
  - Network addresses used even if not connected to Internet
  - Growth of networks and the Internet
  - Extended use of TCP/IP
  - Single address per host
- Requirements for new types of service

IPv6 RFCs

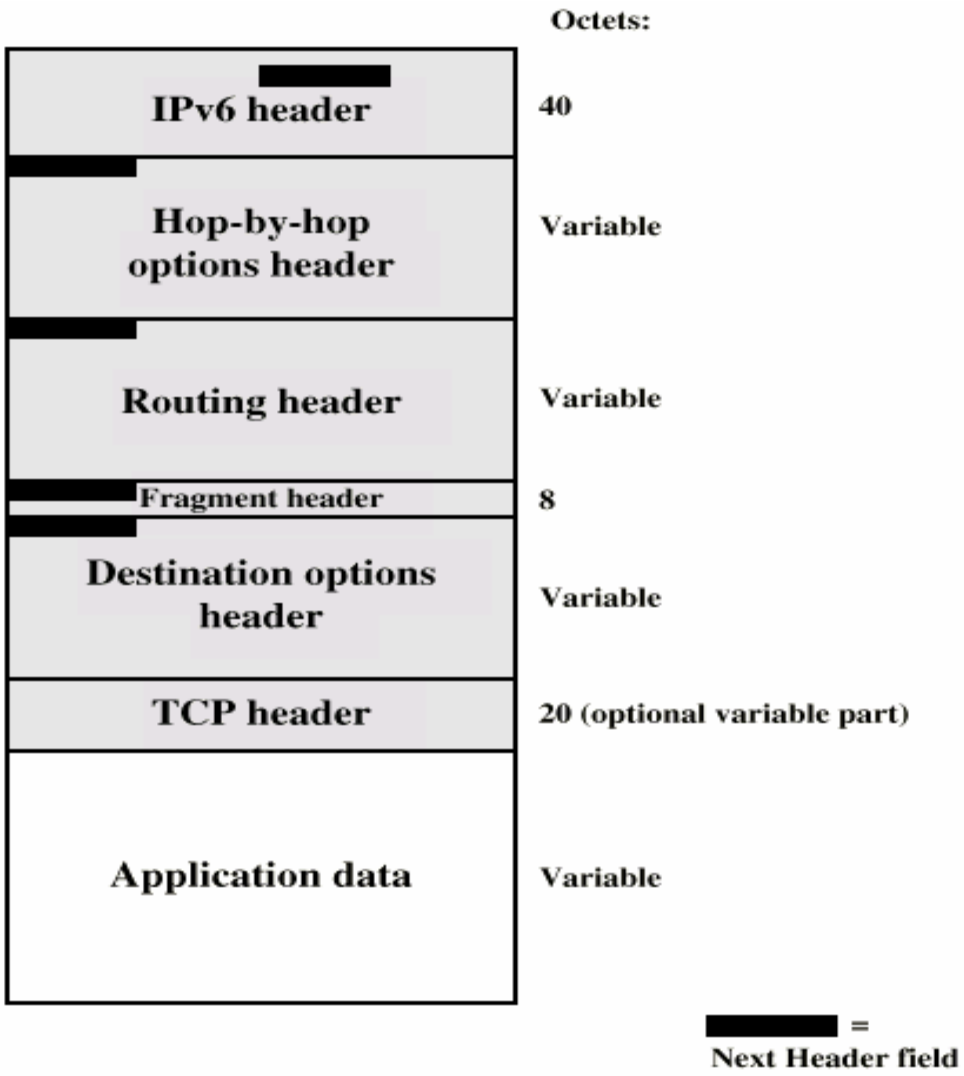
- 1752 - Recommendations for the IP Next Generation Protocol
- 2460 - Overall specification
- 2373 - addressing structure
- others (find them)

- Expanded address space
  - 128 bit
- Improved option mechanism
  - Separate optional headers between IPv6 header and transport layer header
  - Most are not examined by intermediate routes
    - Improved speed and simplified router processing
    - Easier to extend options
- Address autoconfiguration
  - Dynamic assignment of addresses

IPv6 Enhancements (2)

- Increased addressing flexibility
  - Anycast - delivered to one of a set of nodes
  - Improved scalability of multicast addresses
- Support for resource allocation
  - Replaces type of service
  - Labeling of packets to particular traffic flow
  - Allows special handling
  - e.g. real time video

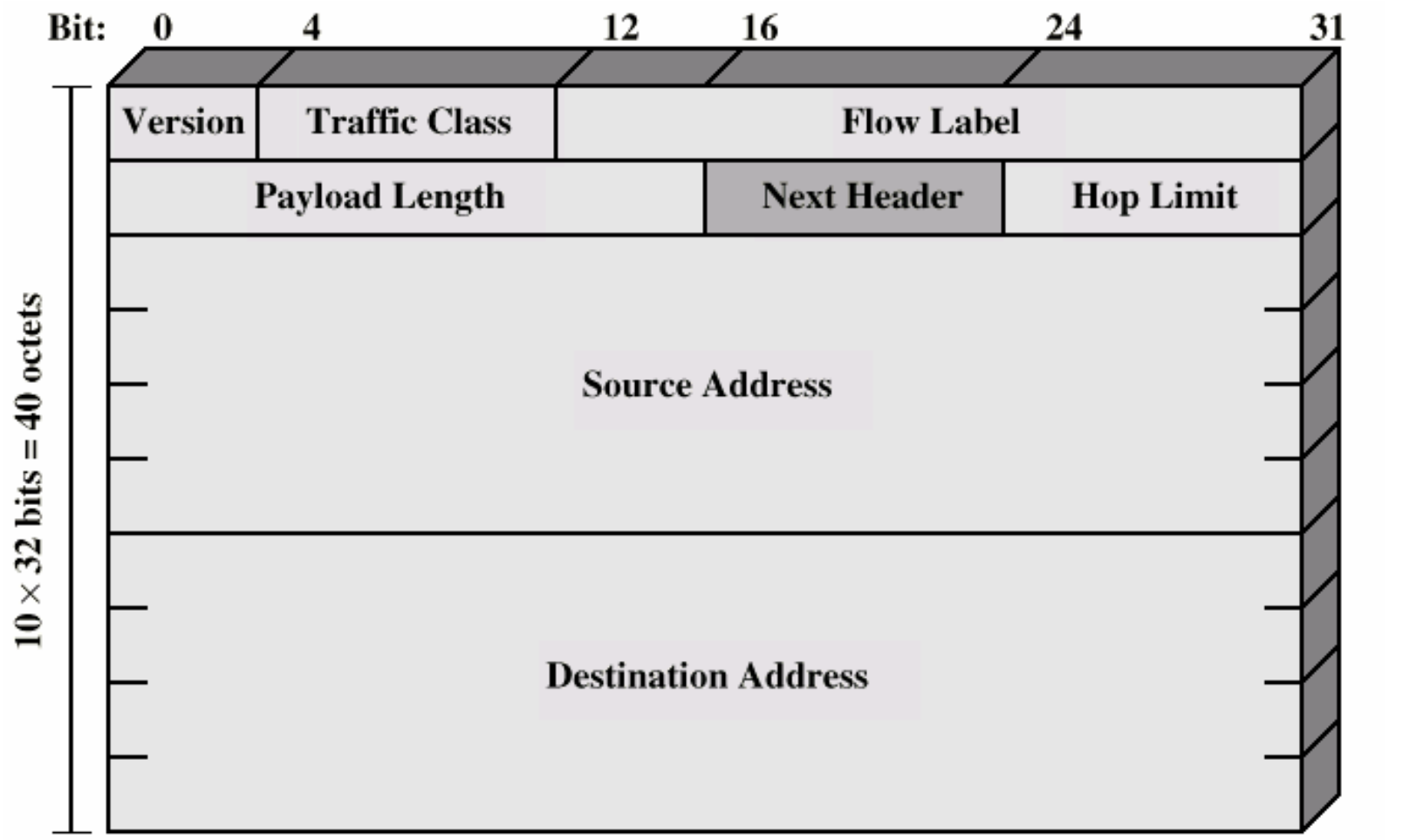
Structure


Octets:
IPv6 header
40
Hop-by-hop options header
Variable
Routing header
Variable
Fragment header
8
Destination options header
Variable
TCP header
20 (optional variable part)
Application data
Variable
=
Next Header field

Extension Headers

- Hop-by-Hop Options
  - Require processing at each router
- Routing
  - Similar to v4 source routing
- Fragment
- Authentication
- Encapsulating security payload
- Destination options
  - For destination node

IP v6 Header


Bit:
0
4
12
16
24
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
10 × 32 bits = 40 octets

IP v6 Header Fields

- Version 6
- Traffic Class
  - Classes or priorities of packet
  - Still under development
  - See RFC 2460

IP v6 Header Fields (cont.)

- Flow Label
  - Used by hosts requesting special handling
- Payload length
  - Includes all extension headers plus user data
- Next Header
  - Identifies type of header
    - Extension or next layer up
- Source Address
- Destination address

IPv6 Addresses

- 128 bits long
- Assigned to interface
- Single interface may have multiple unicast addresses
- Three types of address

Types of address

- Unicast
  - Single interface
- Anycast
  - Set of interfaces (typically different nodes)
  - Delivered to any one interface
  - the “nearest”
- Multicast
  - Set of interfaces
  - Delivered to all interfaces identified

Hop-by-Hop Options

- Next header
- Header extension length
- Options
  - Jumbo payload
    - Over 2^{16} = 65,535 octets
  - Router alert
    - Tells the router that the contents of this packet is of interest to the router
    - Provides support for RSPV (chapter 16)

Fragmentation Header

- Fragmentation only allowed at source
- No fragmentation at intermediate routers
- Node must perform path discovery to find smallest MTU of intermediate networks
- Source fragments to match MTU
- Otherwise limit to 1280 octets

Fragmentation Header Fields

- Next Header
- Reserved
- Fragmentation offset
- Reserved
- More flag
- Identification

Routing Header

- List of one or more intermediate nodes to be visited
- Next Header
- Header extension length
- Routing type
- Segments left
  - i.e. number of nodes still to be visited

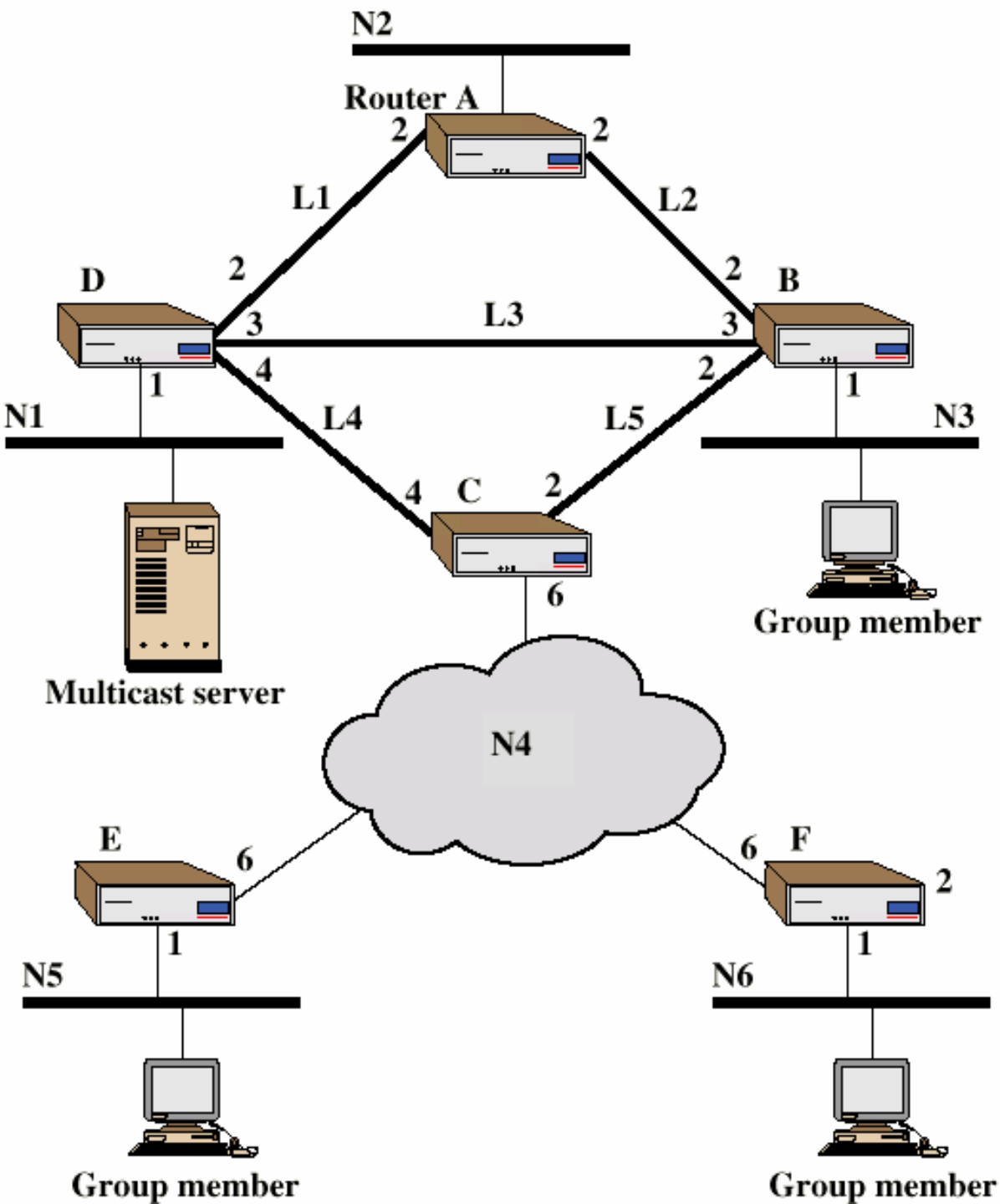
Destination Options

- Same format as Hop-by-Hop options header

Multicasting

- Addresses that refer to group of hosts on one or more networks
- Uses
  - Multimedia “broadcast”
  - Teleconferencing
  - Database
  - Distributed computing
  - Real time workgroups

Example Configuration



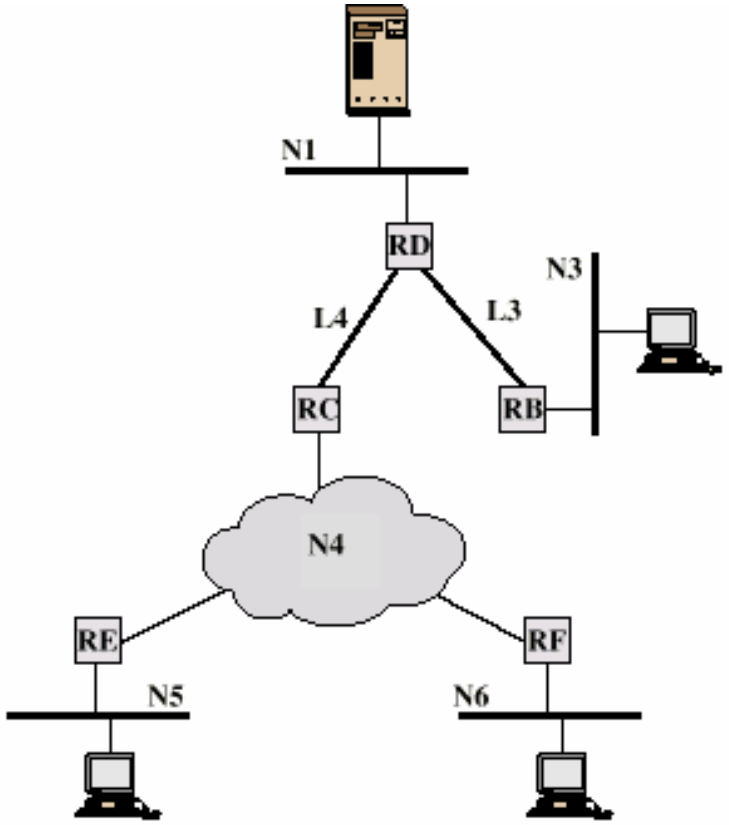
Broadcast and Multiple Unicast

- Broadcast a copy of packet to each network
  - Requires 13 copies of packet
- Multiple Unicast
  - Send packet only to networks that have hosts in group
  - 11 packets

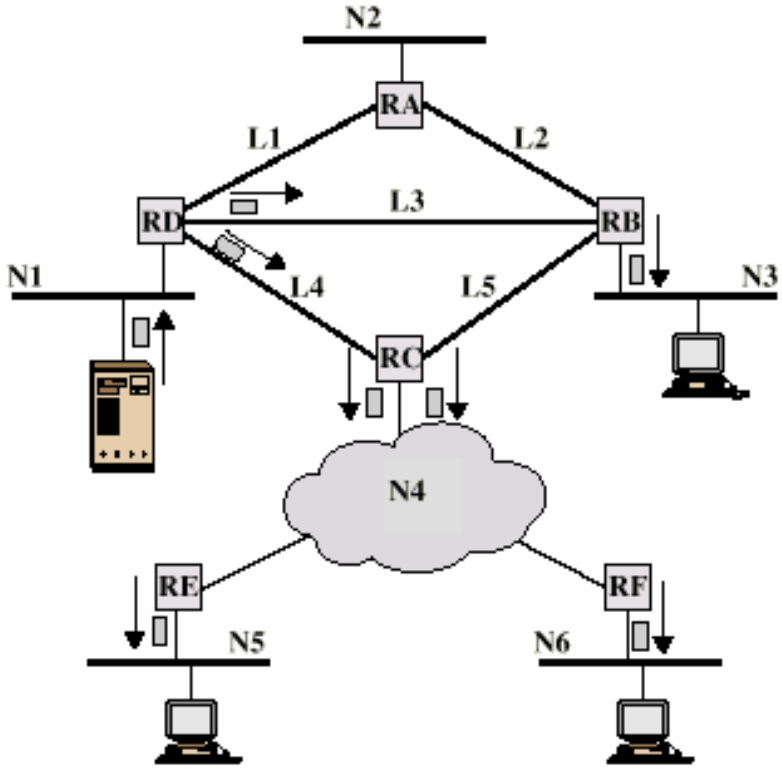
True Multicast

- Determine least cost path to each network that has host in group
  - Gives spanning tree configuration containing networks with group members
- Transmit single packet along spanning tree
- Routers replicate packets at branch points of spanning tree
- 8 packets required

Multicast Example



(a) Spanning tree from source to multicast group



(b) Packets generated for multicast transmission

Requirements for Multicasting

- Router may have to forward more than one copy of packet
- Convention needed to identify multicast addresses
  - IPv4 - Class D - start 1110
  - IPv6 - 8 bit prefix, all 1, 4 bit flags field, 4 bit scope field, 112 bit group identifier

Requirements for Multicasting (cont.)

- Nodes must translate between IP multicast addresses and list of networks containing group members
- Router must translate between IP multicast address and network multicast address
- Mechanism required for hosts to join and leave multicast group

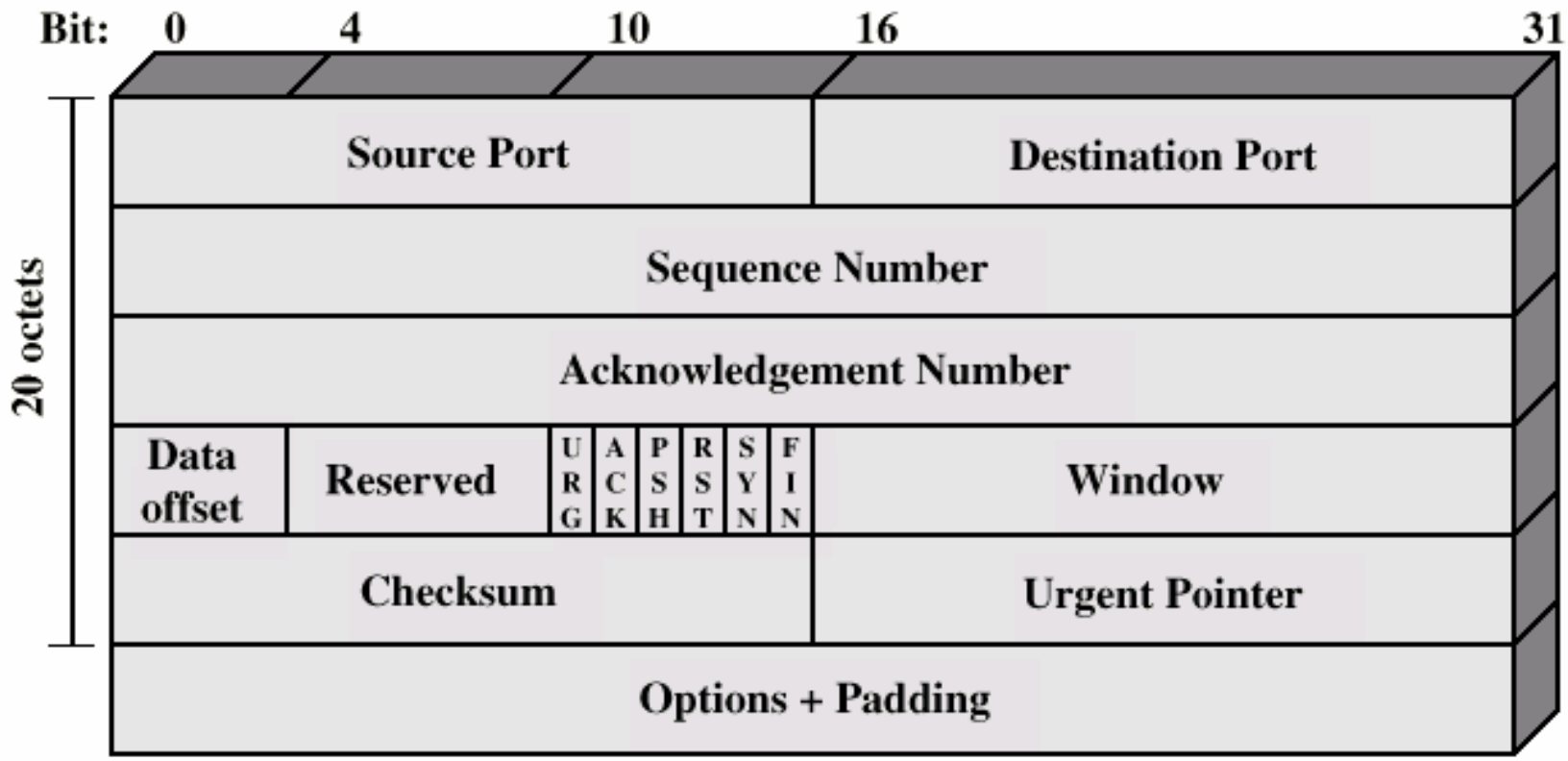
Requirements for Multicasting (cont.)

- Routers must exchange info
  - Which networks include members of given group
  - Sufficient info to work out shortest path to each network
  - Routing algorithm to work out shortest path
  - Routers must determine routing paths based on source and destination addresses

IGMP

- Internet Group Management Protocol
- RFC 1112
- Host and router exchange of multicast group info
- Use broadcast LAN to transfer info among multiple hosts and routers

TCP Header


Bit:
0
4
10
16
31
20 octets
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window
Checksum
Urgent Pointer
Options + Padding

Items Passed to IP

- TCP passes some parameters down to IP
  - Precedence
  - Normal delay/low delay
  - Normal throughput/high throughput
  - Normal reliability/high reliability
  - Security

TCP Mechanisms

- Connection establishment
  - Three way handshake
  - Between pairs of ports
  - One port can connect to multiple destinations

TCP Mechanisms (cont.)

- Data transfer
  - Logical stream of octets
  - Octets numbered modulo 2^{23}
  - Flow control by credit allocation of number of octets
  - Data buffered at transmitter and receiver

TCP Mechanisms (cont.)

- Connection termination
  - Graceful close
  - TCP users issues CLOSE primitive
  - Transport entity sets FIN flag on last segment sent
  - Abrupt termination by ABORT primitive
    - Entity abandons all attempts to send or receive data
    - RST segment transmitted

Implementation Policy Options

- Send
- Deliver
- Accept
- Retransmit
- Acknowledge

Send

- If no push or close TCP entity transmits at its own convenience
- Data buffered at transmit buffer
- May construct segment per data batch
- May wait for certain amount of data

Deliver

- In absence of push, deliver data at own convenience
- May deliver as each in order segment received
- May buffer data from more than one segment

Accept

- Segments may arrive out of order
- In order
  - Only accept segments in order
  - Discard out of order segments
- In windows
  - Accept all segments within receive window

Retransmit

- TCP maintains queue of segments transmitted but not acknowledged
- TCP will retransmit if not ACKed in given time
  - First only
  - Batch
  - Individual

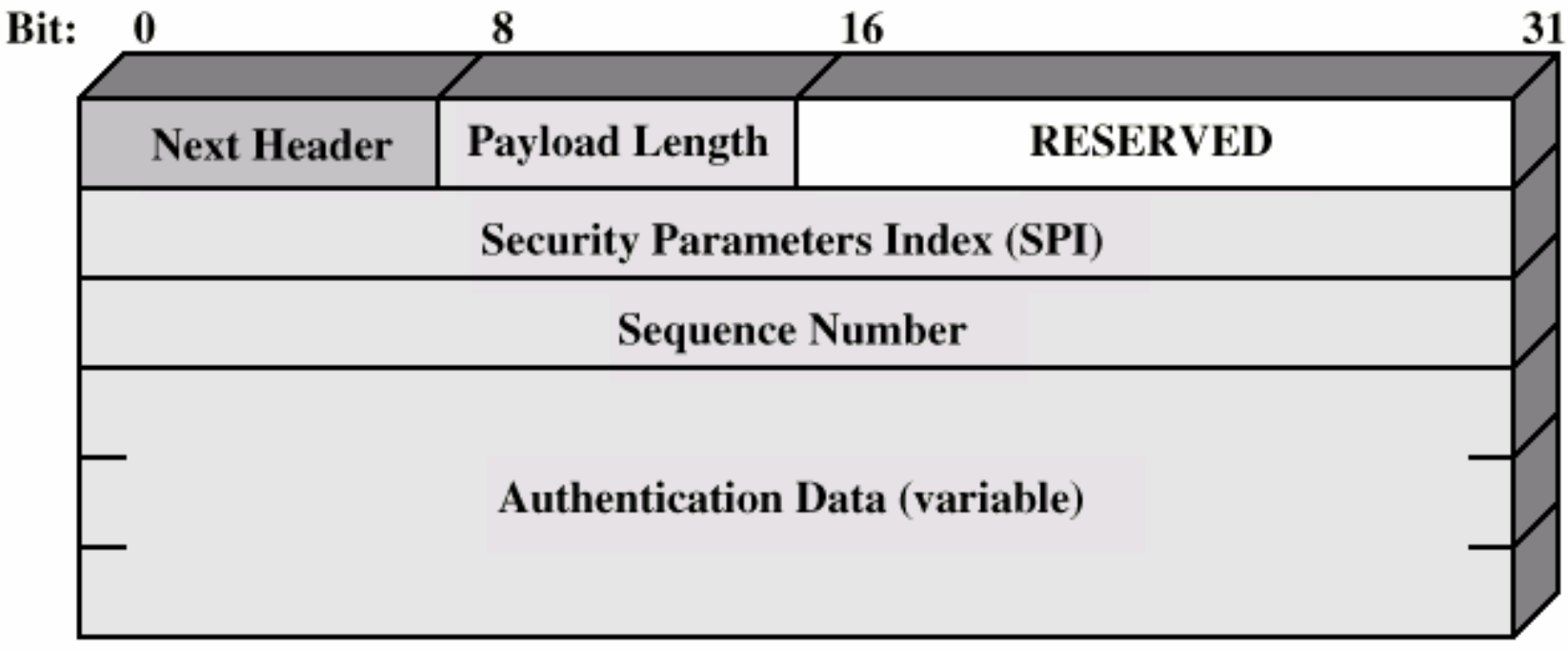
Acknowledgement

- Immediate
- Cumulative

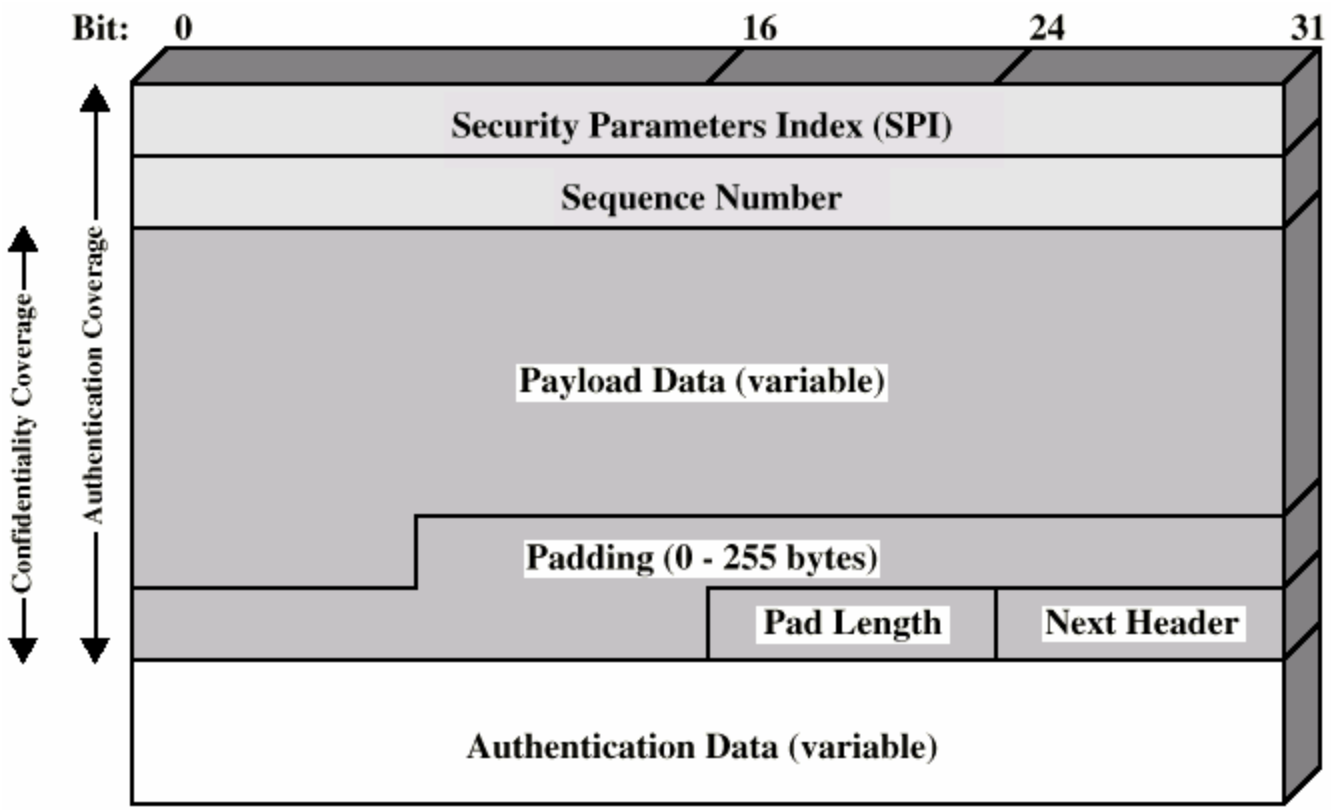
Congestion Control

- RFC 1122, Requirements for Internet hosts
- Retransmission timer management
  - Estimate round trip delay by observing pattern of delay
  - Set time to value somewhat greater than estimate
  - Simple average
  - Exponential average
  - RTT Variance Estimation (Jacobson's algorithm)

Authentication Header



ESP Packet


Bit:
0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Confidentiality Coverage
Authentication Coverage

Ethernet (CSAM/CD)

- Carriers Sense Multiple Access with Collision Detection
- Xerox - Ethernet
- IEEE 802.3

IEEE802.3 Medium Access Control

- Random Access
  - Stations access medium randomly
- Contention
  - Stations content for time on medium

ALOHA

- Packet Radio
- When station has frame, it sends
- Station listens (for max round trip time)plus small increment
- If ACK, fine. If not, retransmit
- If no ACK after repeated transmissions, give up
- Frame check sequence (as in HDLC)
- If frame OK and address matches receiver, send ACK
- 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 in 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%

CSMA

- Propagation time is much less than transmission time
- All stations know that a transmission has started almost immediately
- First listen for clear medium (carrier sense)
- If medium idle, transmit
- If two stations start at the same instant, collision
- Wait reasonable time (round trip plus ACK contention)
- No ACK then retransmit
- Max utilization depends on propagation time (medium length) and frame length
  - Longer frame and shorter propagation gives better utilization

If Busy?

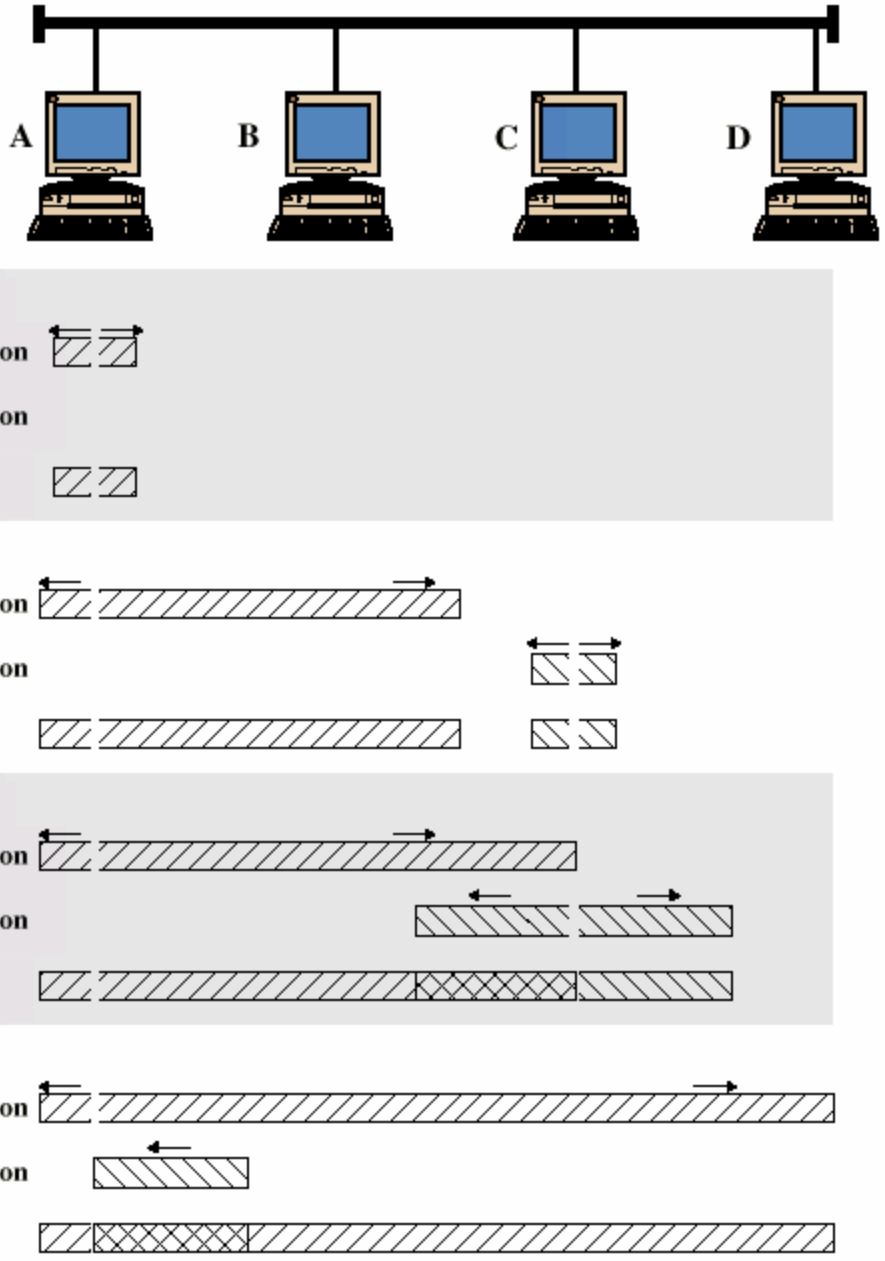
- If medium is idle, transmit
- If busy, listen for idle then transmit immediately
- If two stations are waiting, collision

CSMA/CD

- With CSMA, collision occupies medium for duration of transmission
- Stations listen whilst transmitting

- If medium idle, transmit
- If busy, listen for idle, then transmit
- If collision detected, jam then cease transmission
- After jam, wait random time then start again

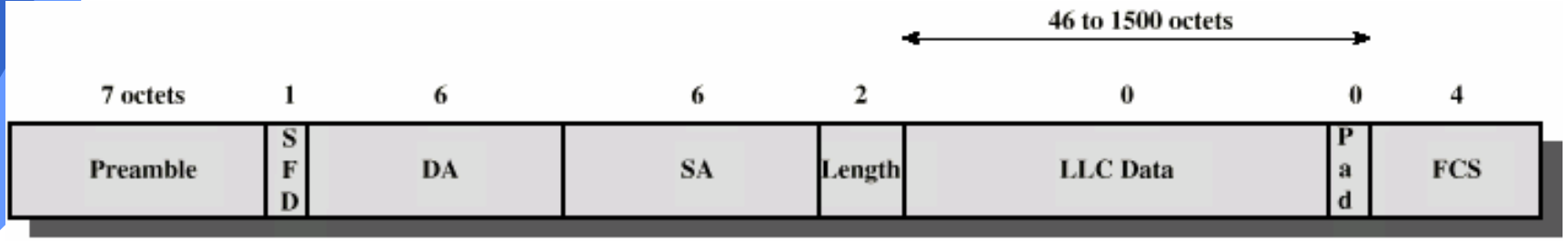
CSMA/CD Operation



Collision Detection

- On baseband bus, collision produces much higher signal voltage than signal
- Collision detected if cable signal greater than single station signal
- Signal attenuated over distance
- Limit distance to 500m (10Base5) or 200m (10Base2)
- For twisted pair (star-topology) activity on more than one port is

IEEE 802.3 Frame Format



SFD = Start of frame delimiter
DA = Destination address
SA = Source address
FCS = Frame check sequence

10Mbps Specification (Ethernet)

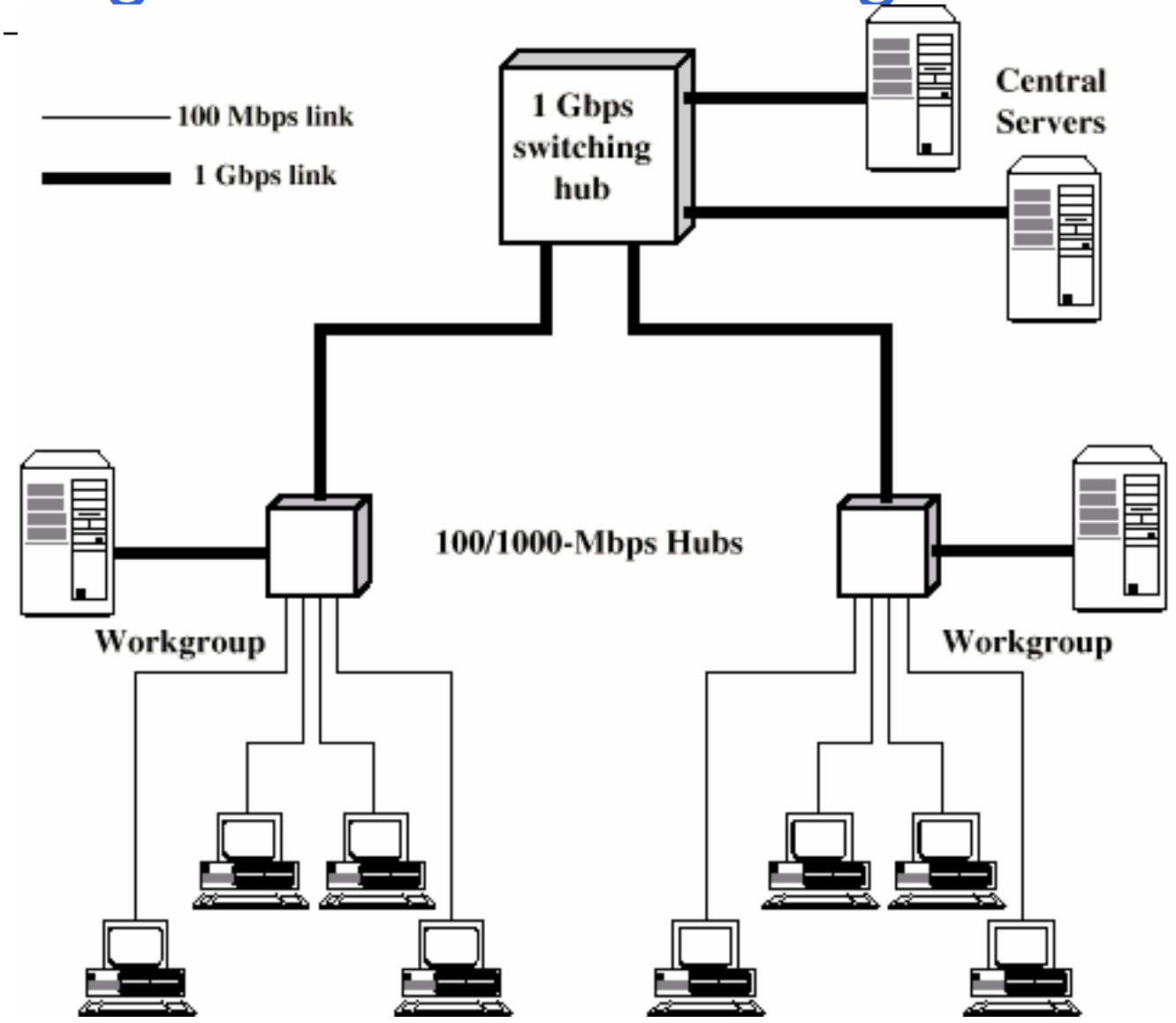
- <data rate><Signaling method><Max segment length>

	10Base5	10Base2	10Base-T	10Base-FP
Medium	Coaxial	Coaxial	UTP	850nm fiber
Signaling	Baseband Manchester	Baseband Manchester	Baseband Manchester	Baseband On/Off
Topology	Bus	Bus	Star	Star

100Mbps (Fast Ethernet)

100Base-TX	100Base-T4	100Base-FX
2 pair, STP		2 pair, Cat 5UTP
	2 optical fiber	4 pair, cat 3,4,5
MLT-3	MLT-3	4B5B,NRZI
	8B6T,NRZ	

Gigabit Ethernet Configuration



Gigabit Ethernet - Differences

- Carrier extension
- At least 4096 bit-times long (512 for 10/100)
- Frame bursting

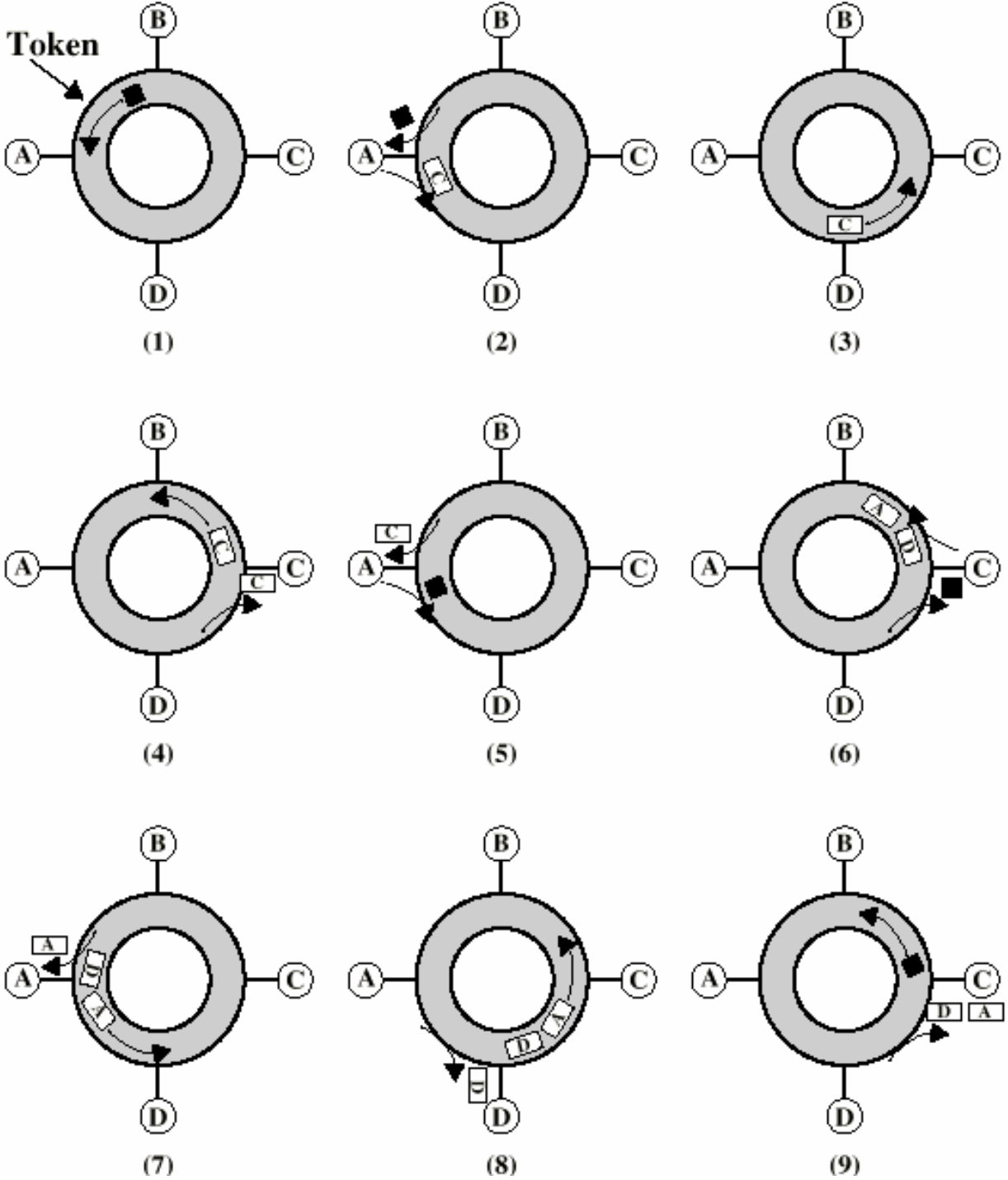
Gigabit Ethernet - Physical

- 1000Base-SX
  - Short wavelength, multimode fiber
- 1000Base-LX
  - Long wavelength, Multi or single mode fiber
- 1000Base-CX
  - Copper jumpers <25m, shielded twisted pair
- 1000Base-T
  - 4 pairs, cat 5 UTP

Token Ring (802.5)

- MAC protocol
  - Small frame (token) circulates when idle
  - Station waits for token
  - Changes one bit in token to make it SOF for data frame
  - Append rest of data frame
  - Frame makes round trip and is absorbed by transmitting station
  - Station then inserts new token when transmission has finished and leading edge of returning frame arrives

Token Ring Operation



Token Ring MAC Frame

SD = starting delimiter
AC = access control
FC = frame control
DA = destination address
SA = source address
FCS = frame check sequence
ED = ending delimiter
FS = frame status

(a) General Frame Format

(b) Token Frame Format

J, K = non-data bits
I = intermediate frame bit
E = error-detected bit

(c) Ending Delimiter Field

PPP = priority bits
T = token bit
M = monitor bit
RRR = reservation bits

(c) Access Control Field

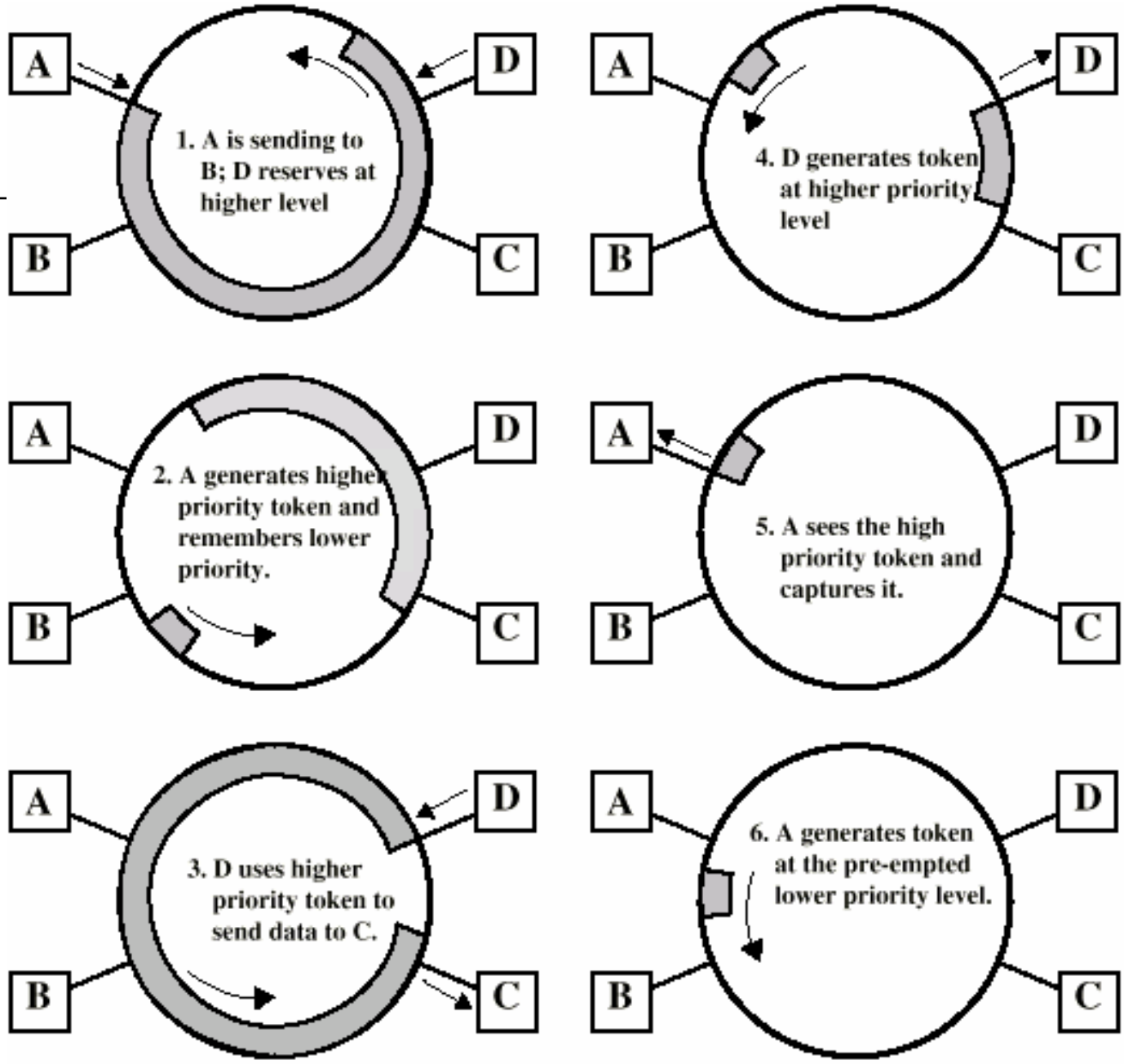
A = Address recognized bit
C = Frame copied bit
r = reserved

(e) Frame Status Field

FF = frame-type bits
ZZZZZZ = control bits

(d) Frame Control Field

Priority Scheme



Dedicated Token Ring

- Central hub
- Acts as switch
- Full duplex point to point link
- Concentrator acts as frame level repeater
- No token passing

802.5 Physical Layer

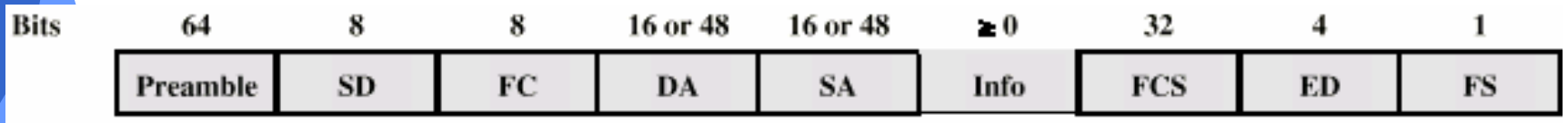
Data Rate	4	16	100
Medium	UTP,STP,Fiber		
Signaling	Differential Manchester		
Max Frame	4550	18200	18200
Access Control	TP or DTR	TP or DTR	TP or DTR

- Note: 1Gbit in development

FDDI

- 100Mbps
- LAN and MAN applications
- Token Ring

FDDI MAC Frame Format



(a) General Frame Format

(b) Token Frame Format

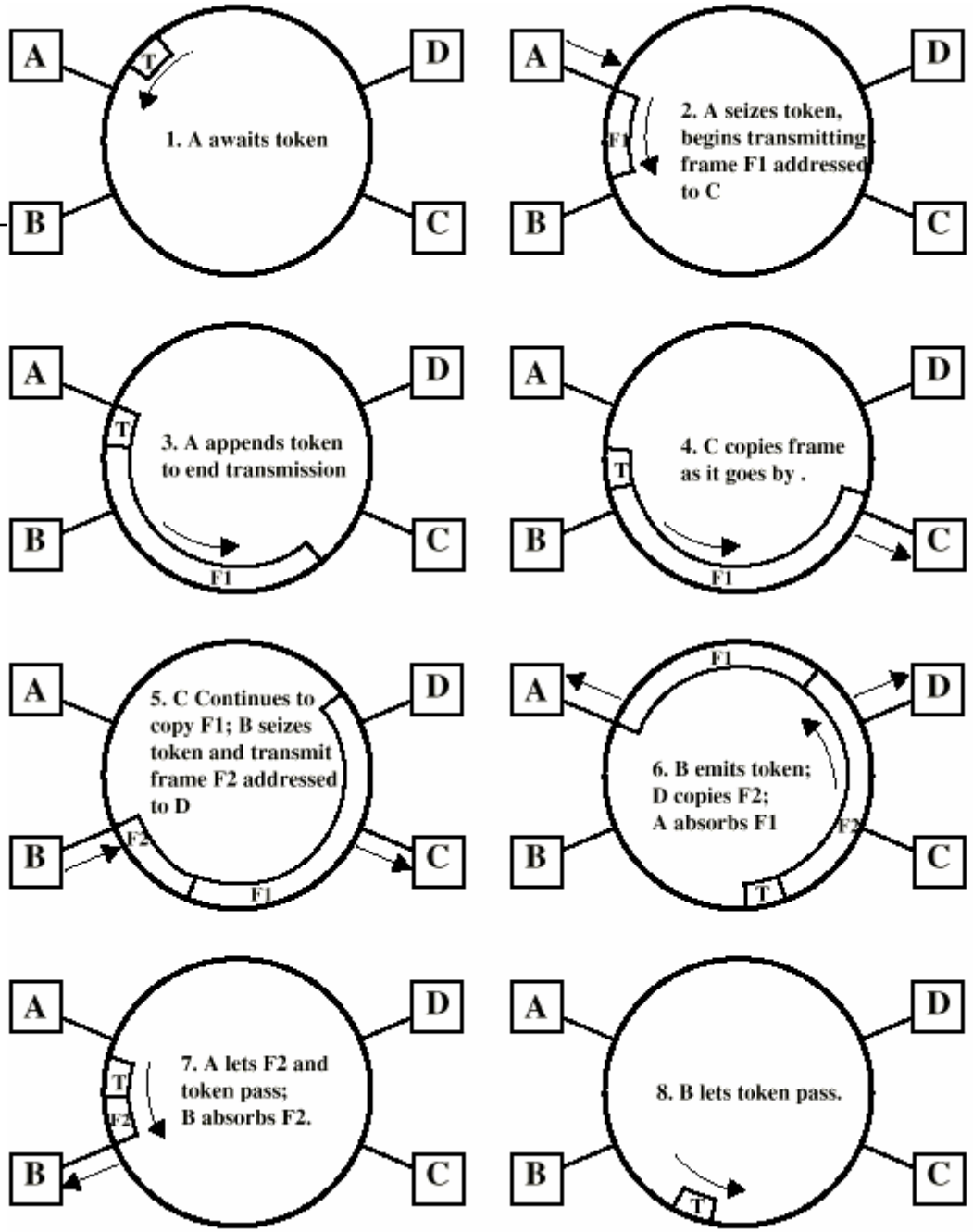
SD = starting delimiter
FC = frame control
DA = destination address
SA = source address
FCS = frame check sequence
ED = ending delimiter
FS = frame status

FDDI MAC Protocol

- As for 802.5 except:

- Station seizes token by aborting token transmission
- Once token captured, one or more data frames transmitted
- New token released as soon as transmission finished (early token release in 802.5)

FDDI Operation



FDDI Physical Layer

Medium	Optical Fiber Twisted Pair	
Data rate	100	100
Signaling	4B/5B/NRZI	MLT-3
Max repeaters	100	100
Between repeaters	100m	2km

LAN Generations

- First
  - CSMA/CD and token ring
  - Terminal to host and client server
  - Moderate data rates
- Second
  - FDDI
  - Backbone
  - High performance workstations
- Third
  - ATM
  - Aggregate throughput and real time support for multimedia applications