NANJING UNIVERSITY · SOFTWARE INSTITUTE

南京大学 软件学院

OSI Layer 2: Data Link Layer

CISCO SYSTEMS

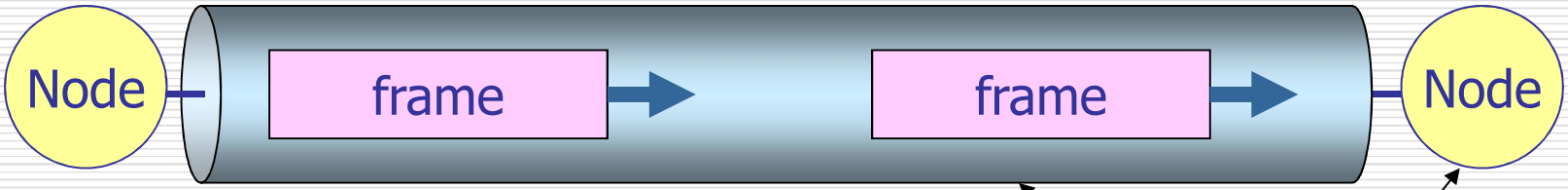
EMPOWERING THE INTERNET GENERATION℠

Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

Data Link Layer

- Problem:How to transfer data correctly on a instable link?



- The DATA LINK LAYER provides:
  - Access to the networking media
  - Physical transmission across the media
- Layer 2 protocols (procedures) define:
  - The format of data exchanged on a link
  - The action of the two nodes on the link
- In Data Link Layer, 'procedure' = 'protocol'

Node：Host and router in the network

Link：The channel connects the adjacent nodes

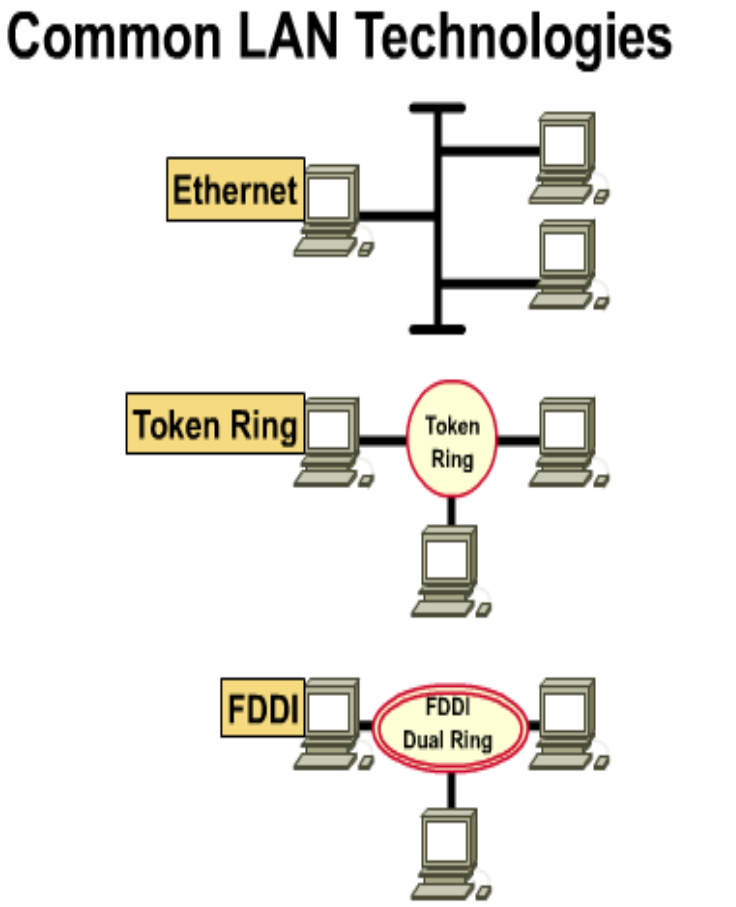
LANS and the Data Link Layer

- Main tasks:
  - Error notification
  - Network topology
  - Flow control
- Differences between Layer 1 and Layer 2:
  - Layer 1 cannot communicate with the upper-level layers; Layer 2 does that with *Logical Link Control* (*LLC*).
  - Layer 1 cannot decide which host will transmit or receive binary data from a group;
    Layer 2 does that with *Media Access Control* (*MAC*)
  - Layer 1 cannot name or identify computers;
    Layer 2 uses an *addressing* (or naming) process.
  - Layer 1 can only describe streams of bits;
    Layer 2 uses *framing* to organize or group the bits.

Services provided by Layer 2

- Three services provided to the network layer (by LLC)
  - Connectionless service with no acknowledgement, used on:
    - Reliable links (upper layers to ensure the data correctness)
    - Real-time tasks
    - Most of LANs
  - Connectionless service with acknowledgements: unreliable link, such as the wireless network
  - Connection service with acknowledgements

Media Access Control in Common LANs



- *Ethernet* - logical bus topology (information flow is on a linear bus) and physical star or extended star (wired as a star)
- *Token Ring* - logical ring topology (information flow is in a ring) and a physical star topology (wired as a star)
- *FDDI* - logical ring topology (information flow is in a ring) and physical dual-ring topology (wired as a dual-ring)

Access Methods for Media-Access Control

- Two broad categories:
  - *Deterministic*—taking turns
    - Token Ring and FDDI
  - *Non-deterministic (probabilistic)*—first come, first served
    - Ethernet/802.3

Deterministic MAC Protocols

- A special data token circulates the ring.
- When a host receives the token, it can transmit data instead of the token. This is called *seizing the token*.
- When the transmitted frame comes back around to the transmitter, the station transmits a new token; the frame is removed or *stripped* from the ring.

Non-Deterministic MAC Protocols

- This MAC protocol is called ***Carrier Sense Multiple Access with Collision Detection (CSMA/CD)***

- To use this shared-medium technology, Ethernet allows the networking devices to arbitrate for the right to transmit.

LAN Transmission Methods

LAN data transmissions fall into 3 classifications:

- **unicast**--a single packet is sent from the source to a single destination on a network
- **multicast**--consists of a single data packet that is sent to a specific subset of nodes on the network.
- **broadcast**--consists of a single data packet that is transmitted to all nodes on the network.

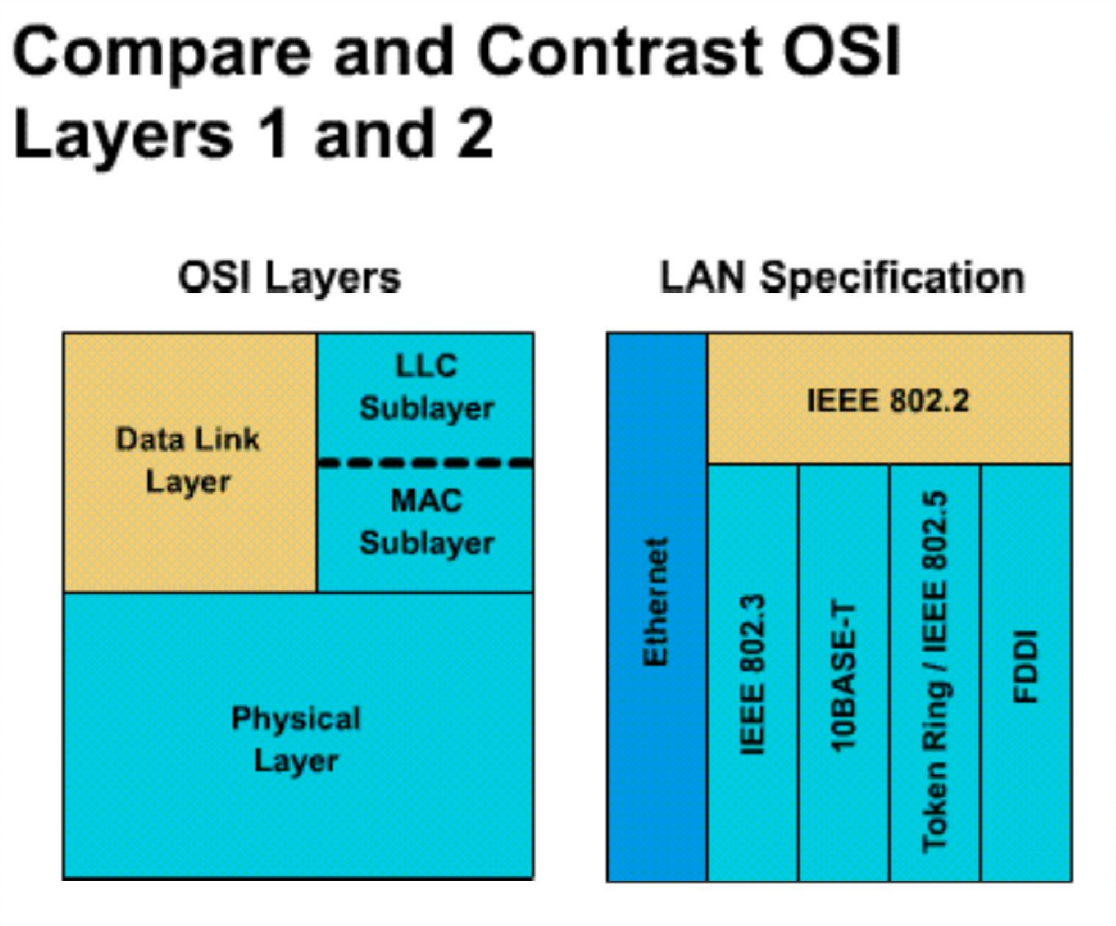
Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

LAN Standards

- Define the physical media and the connectors used to connect devices to media
- Define the way devices communicate at the DATA LINK LAYER
- The DATA LINK LAYER defines how data is transported over a physical media.
- The DATA LINK LAYER also defines how to *encapsulate* protocol-specific traffic in such a way that traffic going to different upper-layer protocols can use the same *channel* as it goes up the stack.

LAN Standards



- Data link layer is broken into two parts by **IEEE** :
  - **Media Access Control *(MAC)*** (transitions down to media)
  - **Logical Link Control *(LLC)*** (transitions up to the network layer)

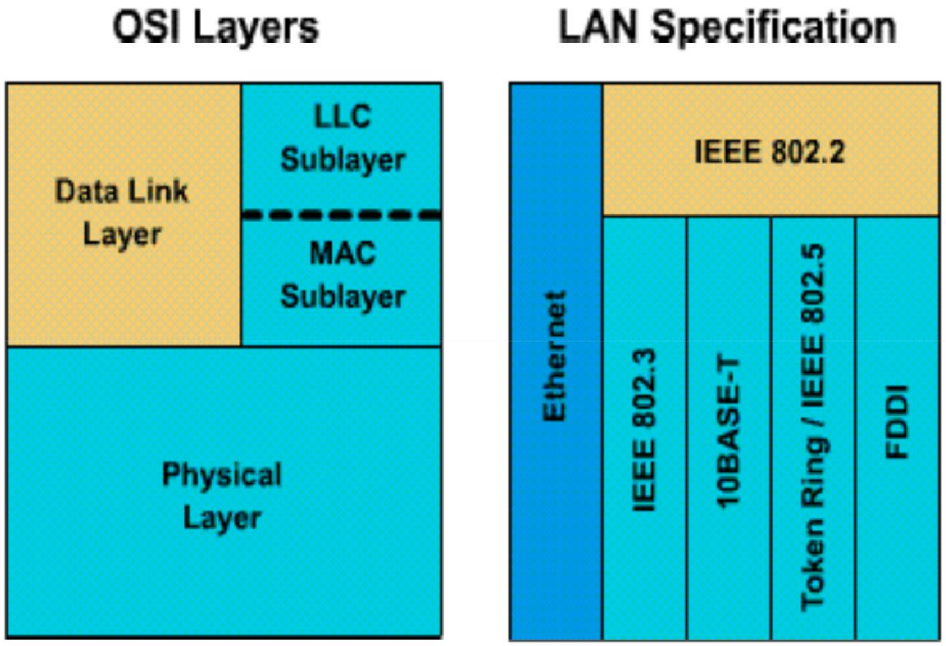
LAN Standards

- The IEEE standard appears, at first glance, to violate the OSI model in two ways.
  - First, it defines its own layer (LLC), including its interfaces, etc.
  - Second, it appears that the MAC layer standards, 802.3 and 802.5, cross over the Layer 2/Layer 1 interface.
- However, 802.3 and 802.5 define the naming, framing, and Media Access Control rules around which specific technologies were built.

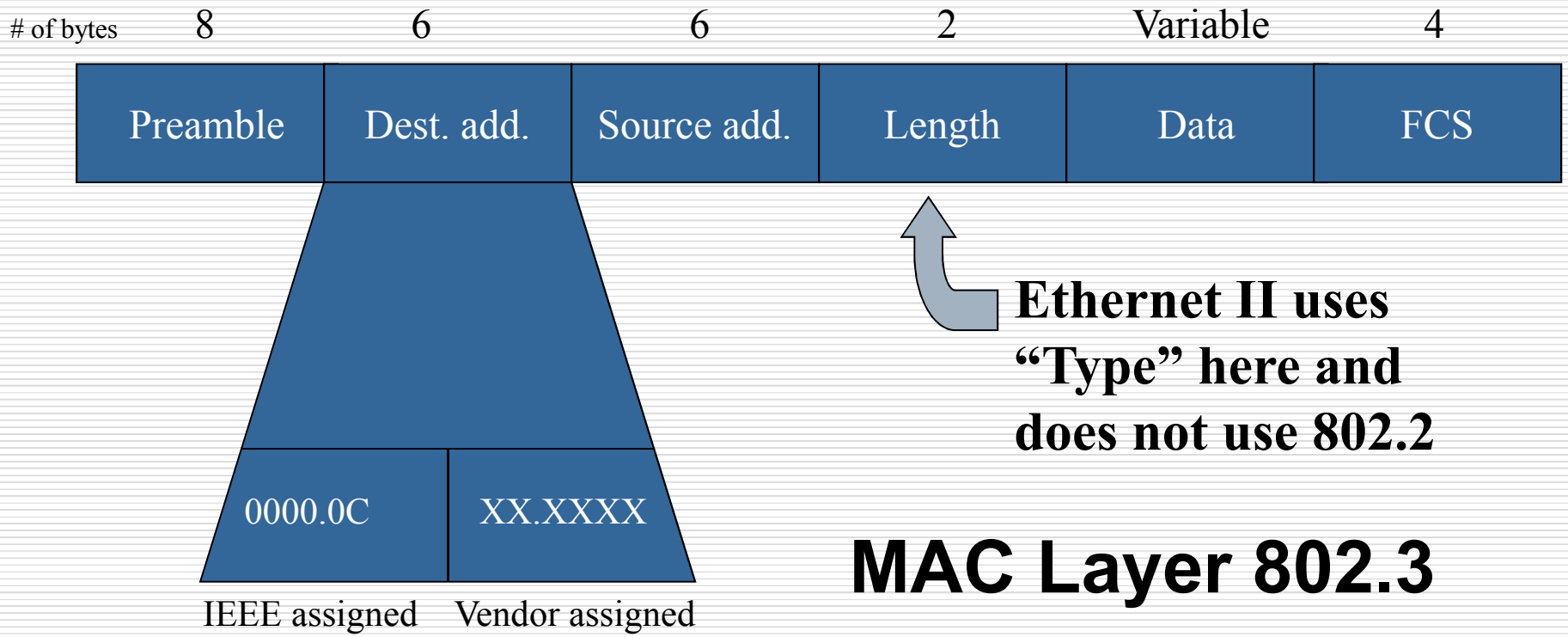
LAN Standards

- **MAC** sublayer (802.3)
  - Defines how to transmit frames on the physical wire
  - Handles physical addressing
  - Define network topology
  - Define line discipline.
- **LLC** sublayer (802.2)
  - logically identifies different protocol types and then encapsulates them.
  - Use SAP identifier to perform the logical identification
  - The type of LLC frame depends on what identifier the upper layer protocol expects.

Compare and Contrast OSI Layers 1 and 2

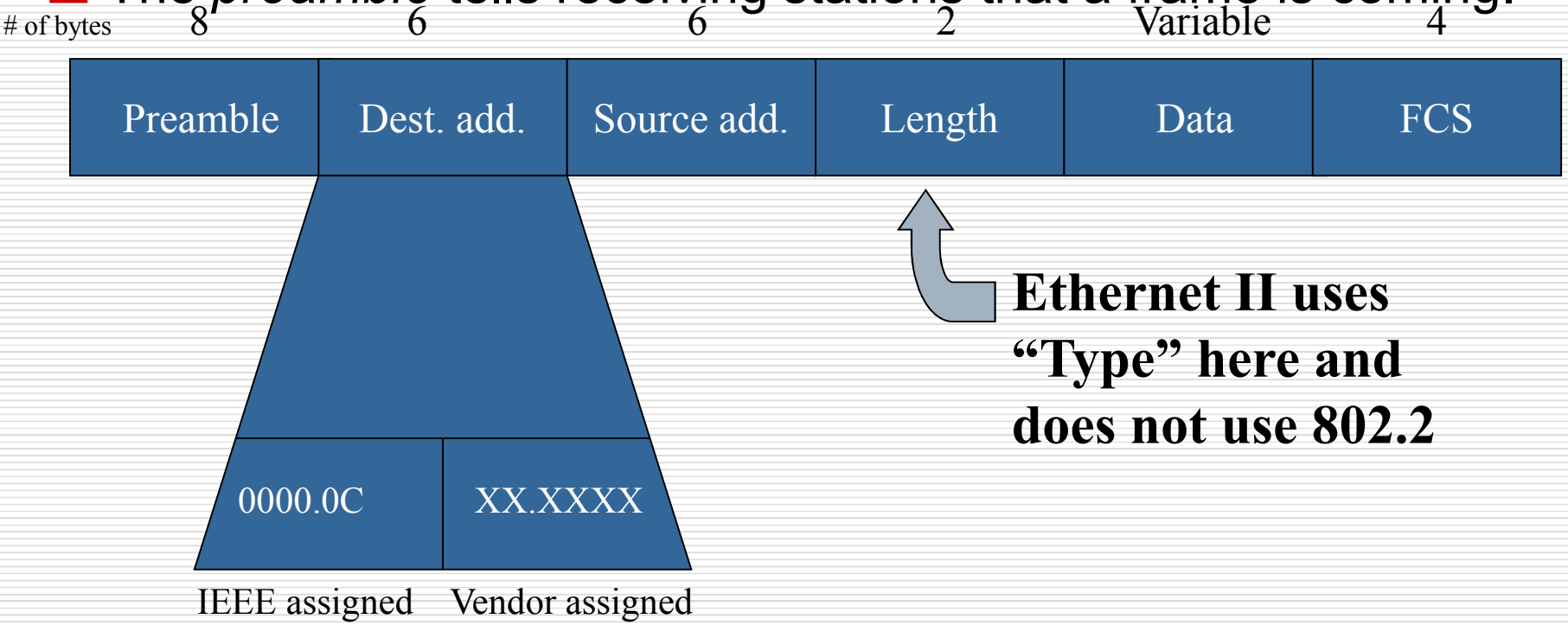


Media Access Control Sublayer



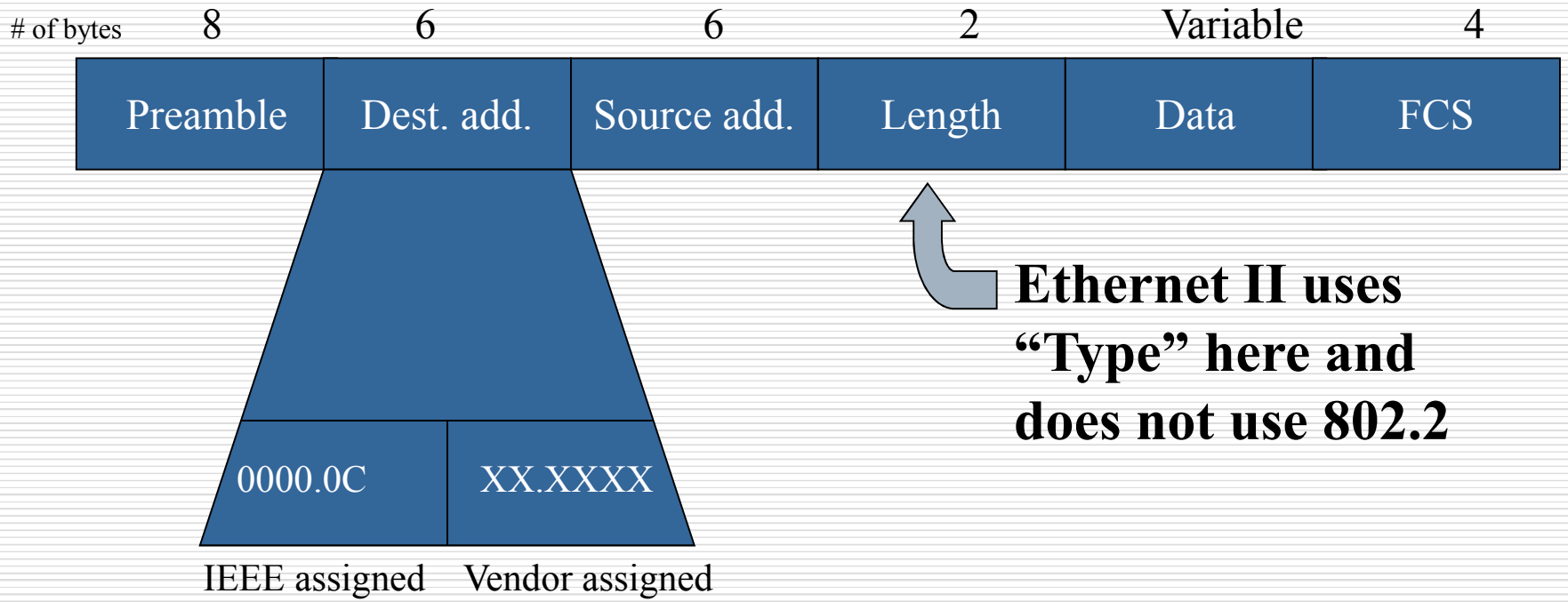
MAC Sub-layer: Fields in a Frame

- Begin with an alternating pattern of 1s and 0s called a *preamble*. (10101011)
- The *preamble* tells receiving stations that a frame is coming.



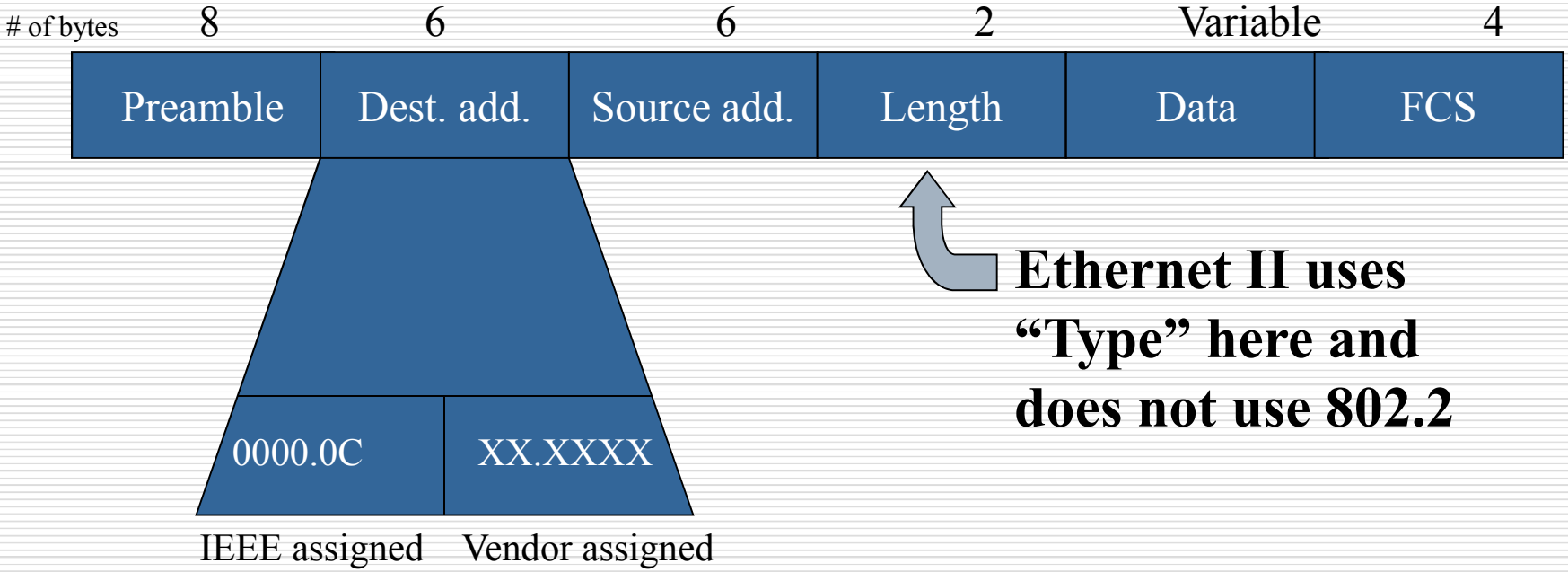
MAC Sub-layer: Fields in a Frame

- *Destination* and *source* physical address fields
  - *source address:* always a unicast address
  - destination address: unicast, multicast, or broadcast.



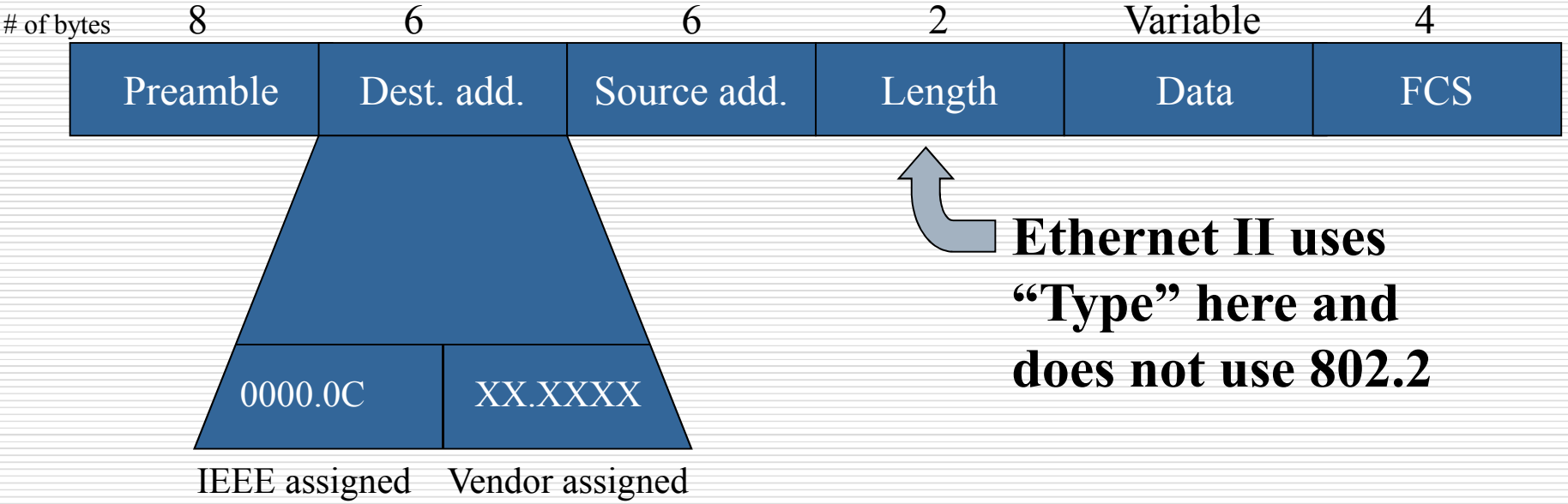
MAC Sub-layer: Fields in a Frame

- *length* field indicates the number of bytes of data that follow this field and precede the frame check sequence field.
- The *data* field contains the information you want to send.



MAC Sub-layer: Fields in a Frame

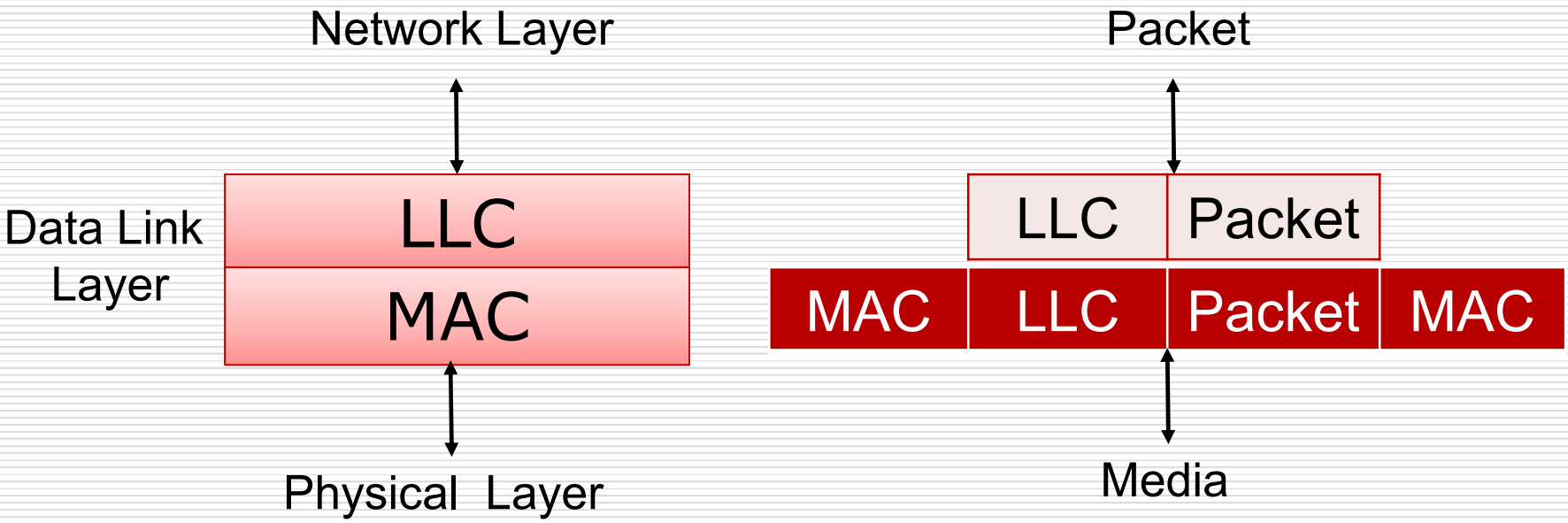
- FCS field (four bytes) contains a cyclic redundancy check value
  - The sending device creates the CRC
  - The receiving device recalculates the CRC to check for damage that might have occurred to the frame in transit.



Logical Link Control Sublayer

- The Logical Link Control (LLC) sublayer manages communication between devices over a single link
- LLC is defined in the IEEE 802.2 specification and supports both *connectionless* and *connect-oriented* services.
- LLC sublayer allows part of the DATA LINK LAYER to function independently from existing technologies.
  - A single LLC sub-layer can be compatible with different MAC sub-layers.

LLC Sub-layer: Encapsulation



(a) Position of LLC

(b) Encapsulation

LLC Sub-layer: Encapsulation

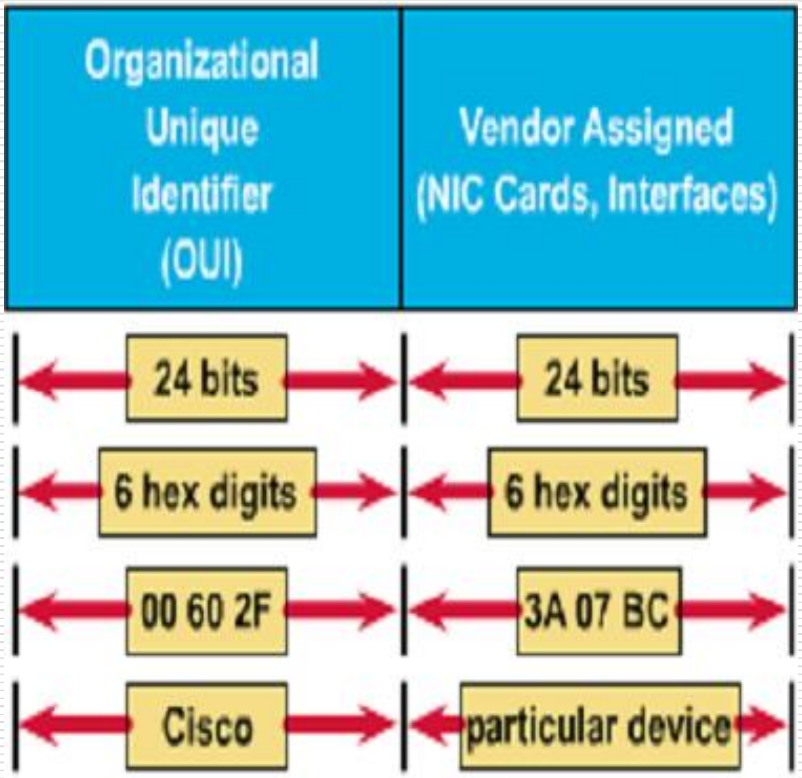
- The LLC takes the network protocol data (packet), and adds more control information to help deliver the packet to its destination.
- It adds two addressing components of the 802.2 specification to identify the upper layer protocol at each end :
  - The Destination Service Access Point (DSAP)
  - The Source Service Access Point (SSAP)
- This repackaged data then travels to the MAC for further encapsulation of the data.

Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

Hexadecimal Numbers as MAC Addresses

- MAC addresses are 48 bits and are always expressed as 12 hexadecimal digits.
- The first 6 hexadecimal digits (from left to right), which the IEEE administers, identify the **manufacturer** or **vendor** and comprise the *Organizational Unique Identifier* (OUI).
- The remaining 6 hex digits comprise the interface serial number, administered by specific vendor.



0000.0c12.3456 or 00-00-0c-12-34-56

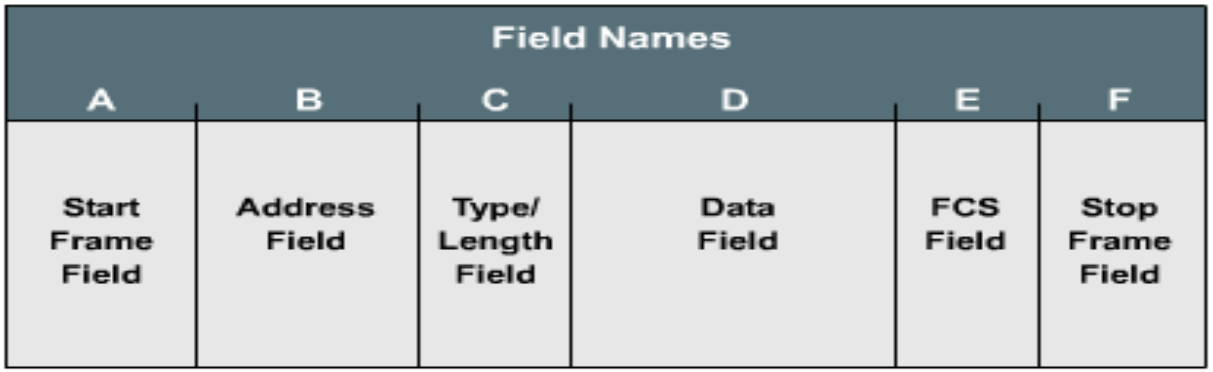
Ethernet 802.3 Broadcast

- Broadcast
  - The destination MAC: all 1s (FFFF.FFFF.FFFF)
- Broadcasting can seriously affect the performance of stations by interrupting them unnecessarily
- So broadcasts should be used only when:
  - The MAC address of the destination is unknown
  - The destination is all hosts

Framing

- Framing is the Layer 2 *encapsulation* process.
- A frame is a Layer 2 protocol data unit (*PDU*).
- A frame has sections called *fields*, and each field is composed of bytes.

- frame start field
- address field
- length/type/control field
- data field
- frame check sequence field
- frame stop field



Ethernet Media Access Control ——CSMA/CD: History

- Ethernet /IEEE 802.3 MAC mechanism: CSMA/CD.
- CSMA/CD stems from ALOHA
- In 1970s, Norman Abramson designed ALOHA
- Pure ALOHA:
  - Hosts always can send the data *if they want*:
    - If the signals collided, back off appropriate amount of time and resend
- Slotted ALOHA:
  - Hosts always can send the data *if they want, but they must wait for a new slot* :
    - If the signals collided, back off appropriate amount of time and resend

Ethernet Media Access Control ——CSMA/CD: History

- Question: Why don't we listen to the channel first to make sure that the channel is free?
  - That is CSMA(Carrier Sense Multiple Access)
- 1-persist CSMA :
  - Hosts always can send the data (have the probability of 1) if they *find the channel is free; if the channel is busy,they will listen to the channel and wait* :
    - If the signals collided, back off appropriate amount of time and resend

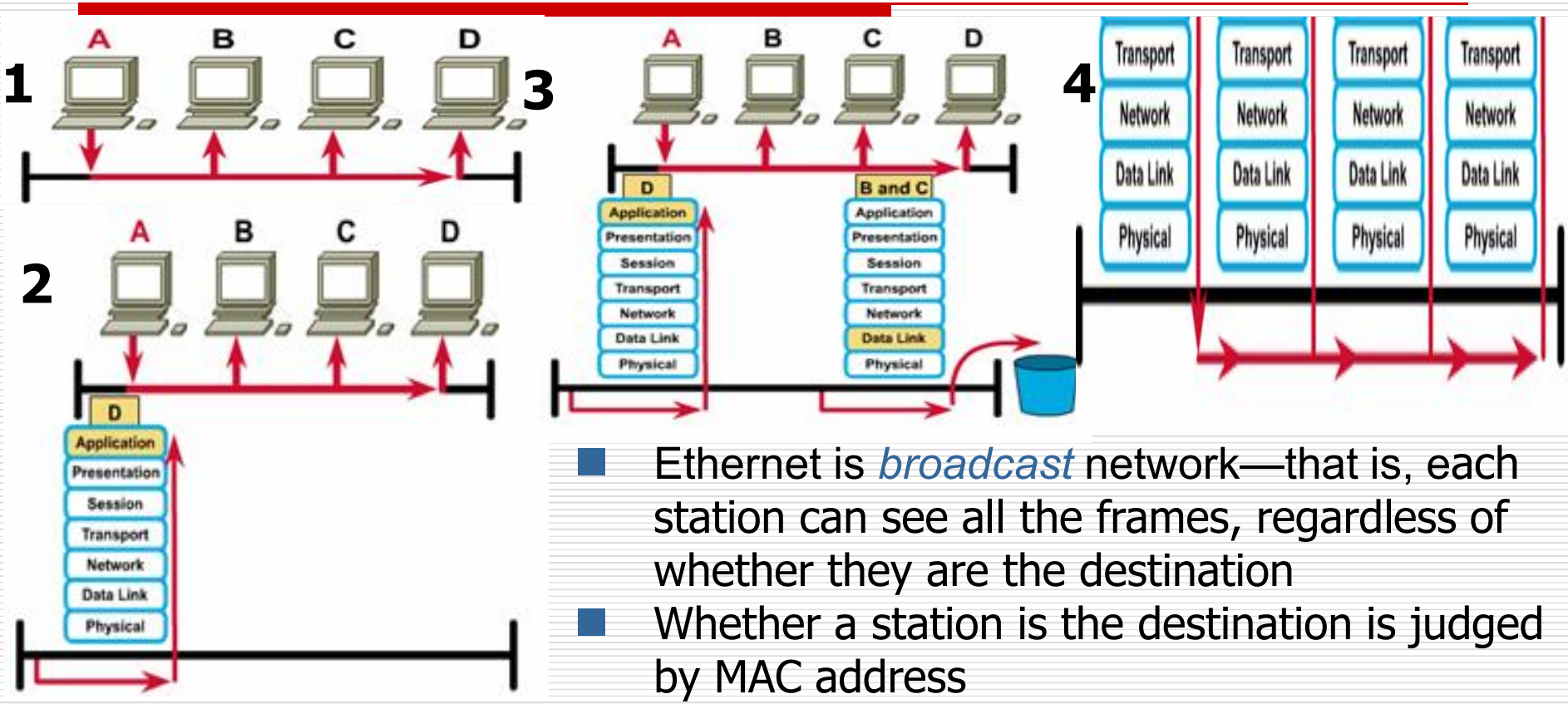
Ethernet Media Access Control ——CSMA/CD: History

- non-persist CSMA :
  - Hosts always can send the data (have the probability of 1) if they *find the channel is free. if the channel is busy, they will wait for a while to listen to the channel again* :
    - If the signals collided, back off appropriate amount of time and resend
- p-persist CSMA(working on slotted channel) :
  - If the hosts *find the channel is free, they will send the data in this slot at a probability of p, or propone the sending operation to the next slot at a probability of 1-p; if the channel is busy, they will wait until the next slot*:
    - If the signals collided, back off appropriate amount of time and resend

Ethernet Media Access Control ——CSMA/CD

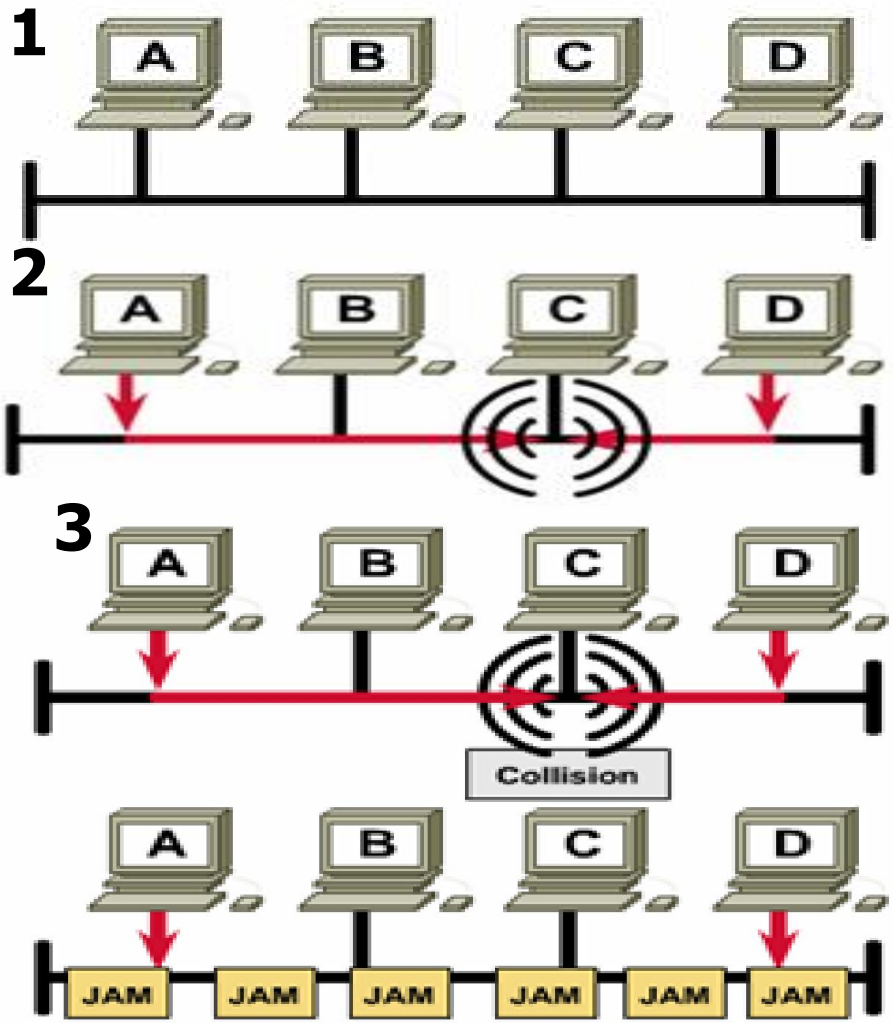
- Another improvement of ALOHA: Listen to the channel while transmitting data. If a collision detected, all transmissions will be cancelled *at once*
- CSMA/CD(Carrier Sense Multiple Access)
  - Use CSMA mechanism to judge if the host should send the data
  - In the transmitting process, listen to the channel at the same time
    - When a collision detected, broadcast the jam signal
    - Back off algorithms determine when the colliding stations can retransmit.

Ethernet Operation

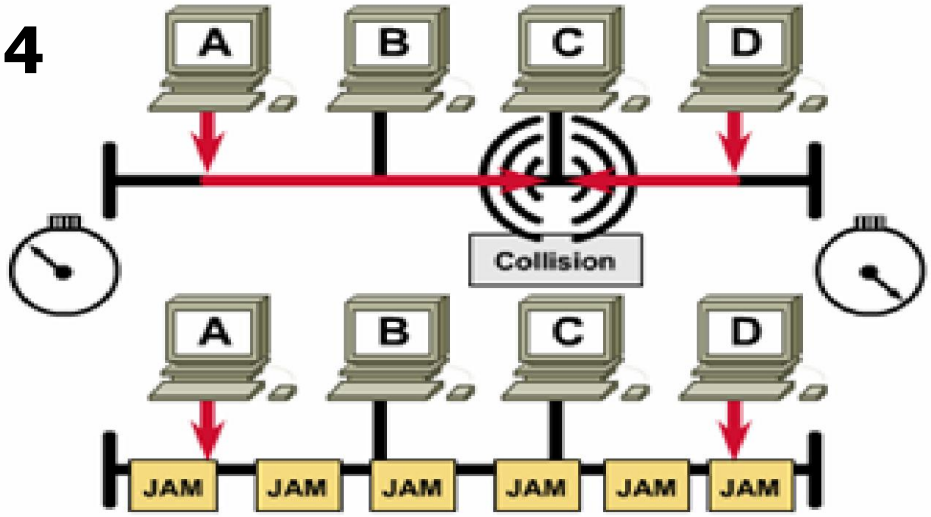


- Ethernet is *broadcast* network—that is, each station can see all the frames, regardless of whether they are the destination
- Whether a station is the destination is judged by MAC address
- Destination station sends data up OSI layers. Other nodes discard frame

Ethernet Operation

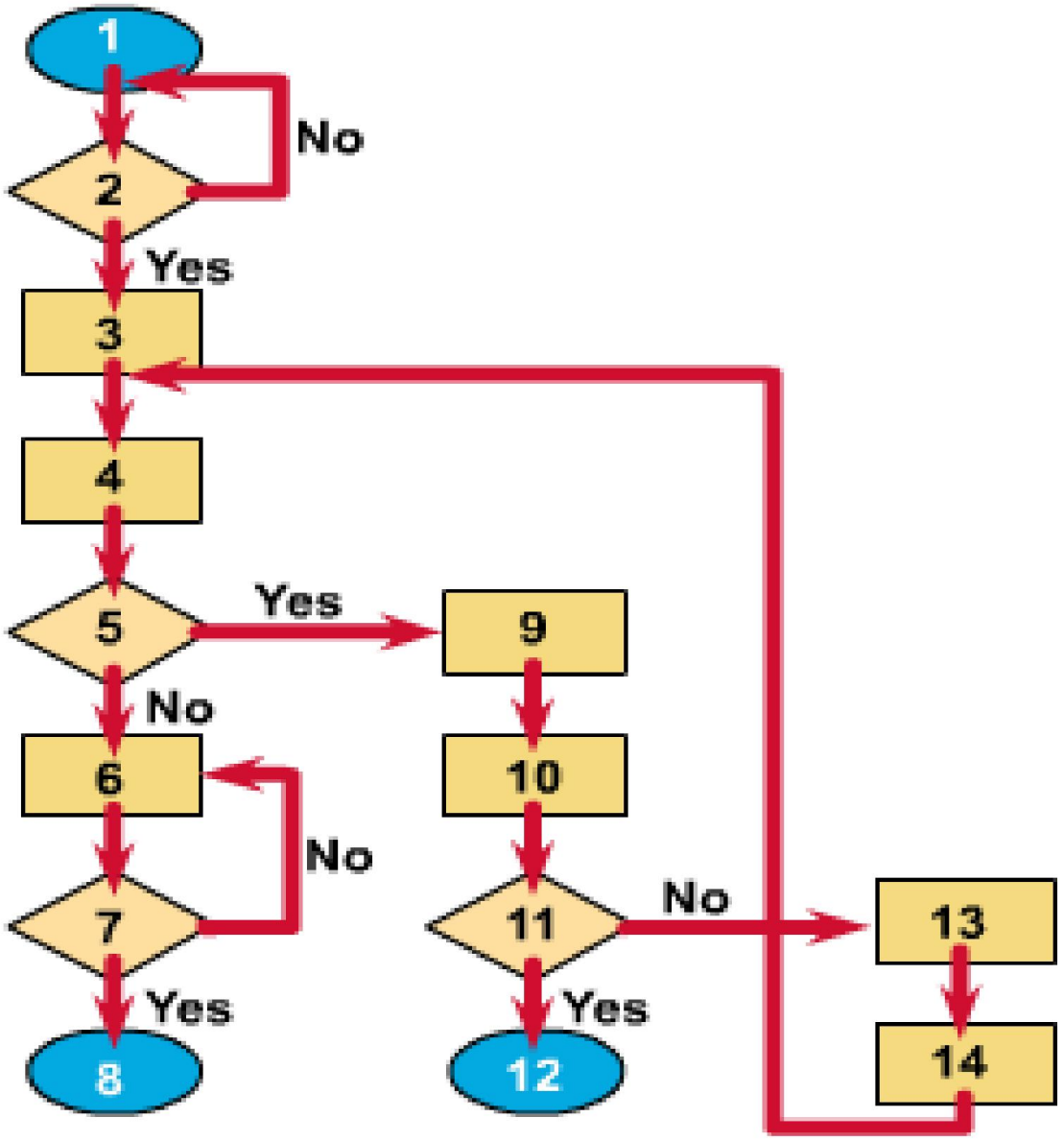


1. Listen then transmit
2. Broadcast jam signal
3. Collision occurs
4. Devices back off appropriate amount of time and then retransmit



Ethernet CSMA / CD

1. Host wants to transmit
2. Is carrier sensed?
3. Assemble frame
4. Start transmitting
5. Is a collision detected?
6. Keep transmitting
7. Is the transmission done?
8. Transmission completed
9. Broadcast jam signal
10. attempts = attempts + 1
11. attempts > too many?
12. Too many collisions; abort transmission
13. Algorithm calculates backoff
14. Wait for t seconds



Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

Flow Control in LLC Sub-layer

An Unrestricted Simplex Protocol

- 工作在理想情况，基于几个假设：
  - 单工传输
  - 发送方无休止工作（要发送的信息无限多）
  - 接收方无休止工作（缓冲区无限大）
  - 通信线路（信道）不损坏或丢失信息帧
- 工作过程
  - 发送程序：取数据，构成帧，发送帧；
  - 接收程序：等待，接收帧，送数据给高层

Flow Control in LLC Sub-layer

A Simplex Stop-and-Wait Protocol

- 增加约束条件：接收方不能无休止接收。
- 解决办法：接收方每收到一个帧，给发送方回送一个响应。
- 工作过程
  - 发送程序：取数据，成帧，发送帧，等待响应帧；
  - 接收程序：等待，接收帧，送数据给高层，回送响应帧

Flow Control in LLC Sub-layer

A Simplex Protocol for a Noisy Channel

- 增加约束条件：信道有差错，信息帧可能损坏或丢失
- 解决办法：出错重传
- 带来的问题：
  - 什么时候重传 —— 定时
  - 响应帧损坏怎么办（重复帧）—— 发送帧头中放入序号
  - 为了使帧头精简，序号取多少位 —— 1位
- 发方在发下一个帧之前等待一个肯定确认的协议叫做*PAR(Positive Acknowledgement with Retransmission)*或*ARQ(Automatic Repeat reQuest)*
- 注意:由于确认帧中没有序号，超时时间不能太短，否则协议失败。因此假设协议的发送和接收严格交替进行

Flow Control in LLC Sub-layer

- 滑动窗口协议（***Sliding Window Protocol***）：
  - 发送的信息帧都有一个序号**(0 ~ 2^n – 1)**
  - 发送端保持一个已发送但尚未确认的帧的序号表，称为发送窗口
    - 上界：*要发送的下一个帧的序号*
    - 下界：*未得到确认的帧的最小编号*
    - 发送窗口大小 **=** 上界 **-** 下界，大小可变
    - 发送端每发送一个帧，序号取上界值，上界加**1**
    - 每接收到一个正确响应帧，下界加**1**；
  - 接收端有一个接收窗口，大小固定，但不一定与发送窗口相同
    - 上界：*允许接收的序号最大的帧*
    - 下界：*希望接收的帧*
    - 接收窗口容纳允许接收的信息帧，*落在窗口外的帧均被丢弃*
    - 序号等于下界的帧被正确接收，并产生一个响应帧，上界、下界都加**1**。接收窗口大小不变。

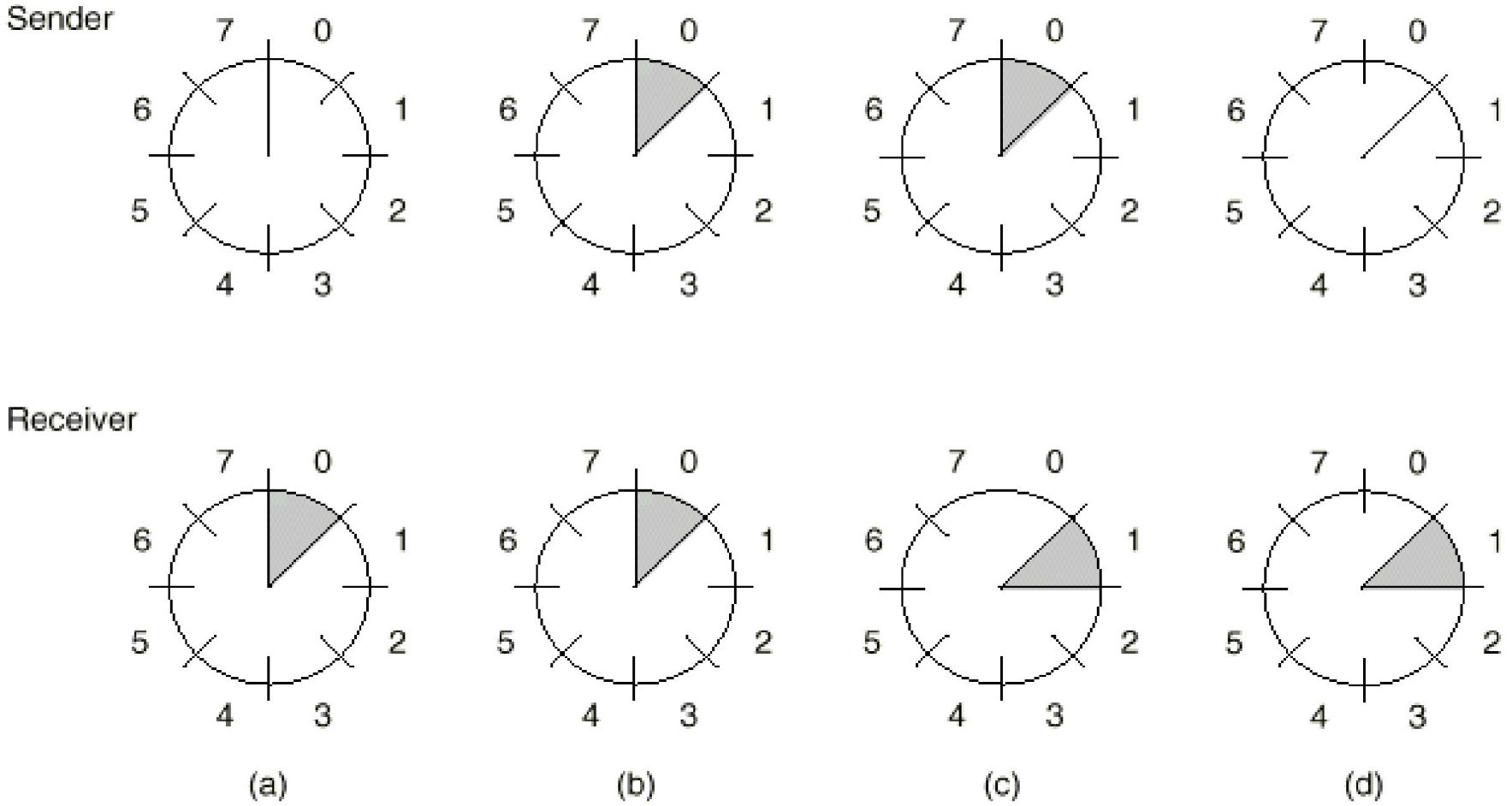


Fig. 3-12. A sliding window of size 1, with a 3-bit sequence number. (a) Initially. (b) After the first frame has been sent. (c) After the first frame has been received. (d) After the first acknowledgement has been received.

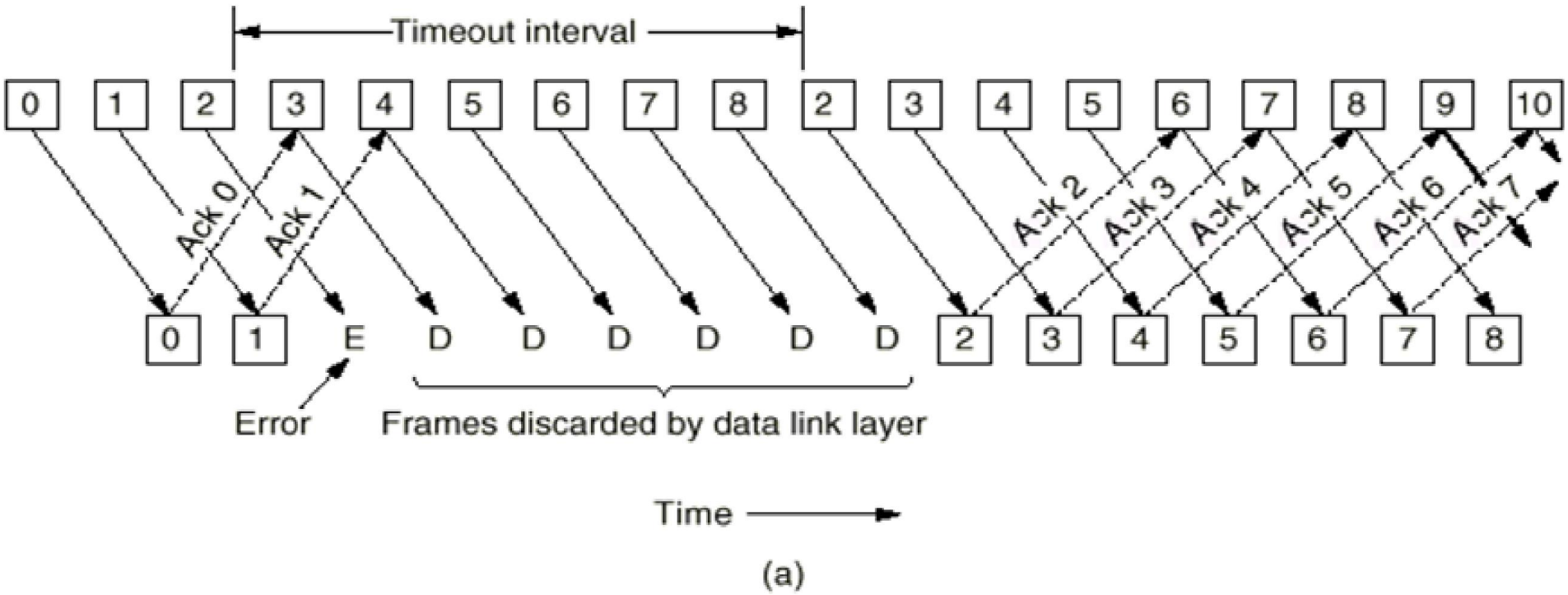
Flow Control in LLC Sub-layer

- 卫星信道传输速率50kbps，往返传输延迟500ms，则:
  - 若传输一个1000bit的帧，时间为：

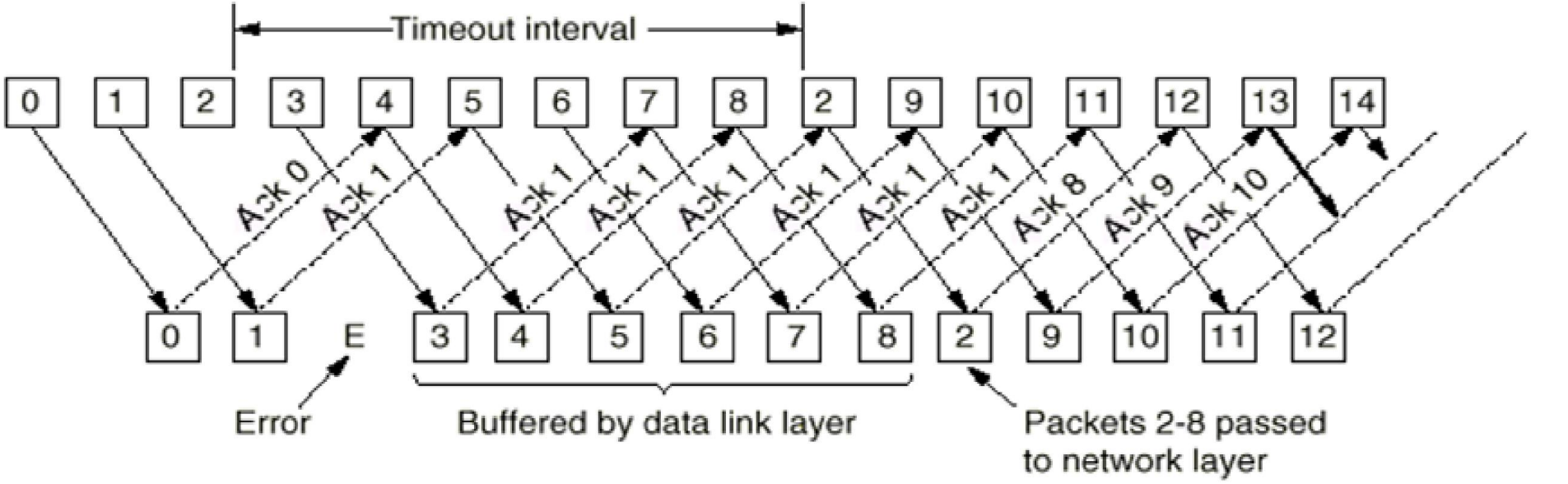
    发送时间 + 信息信道延迟 + 确认信道延迟（确认帧很短，忽略发送时间）= 1000bit / 50kbps + 250ms + 250ms = 520ms
  - 信道利用率 = 20 / 520 ≈ 4%
- 信道带宽*b*比特/秒，帧长度*L*比特，往返传输延迟*R*秒，则信道利用率为 $(L/b) / (L/b + R) = L / (L + Rb)$
- 结论
  - 传输延迟大，信道带宽高，帧短时，信道利用率低

Flow Control in LLC Sub-layer

- 解决办法：流水线技术 **(pipelining)**
  - 连续发送多帧后再等待确认
- 带来的问题
  - 信道误码率高时，对损坏帧的重传非常多
- 两种基本方法
  - 退后**n**帧**(go back n)**
    - 接收方从出错帧起丢弃所有后继帧
    - 接收窗口为**1**
    - 对于出错率较高的信道，浪费带宽
  - 选择重传**(selective repeat)**
    - 接收窗口大于**1**，先暂存出错帧的后继帧；
    - 只重传坏帧
    - 对最高序号的帧进行确认
    - 接收窗口较大时，需较大缓冲区


Timeout interval
0 1 2 3 4 5 6 7 8 2 3 4 5 6 7 8 9 10
Ack 0
Ack 1
Ack 2
Ack 3
Ack 4
Ack 5
Ack 6
Ack 7
0 1 E D D D D D D 2 3 4 5 6 7 8
Error
Frames discarded by data link layer
Time

(a)


Timeout interval
0 1 2 3 4 5 6 7 8 2 9 10 11 12 13 14
Ack 0
Ack 1
Ack 1
Ack 1
Ack 1
Ack 1
Ack 1
Ack 8
Ack 9
Ack 10
0 1 E 3 4 5 6 7 8 2 9 10 11 12
Error
Buffered by data link layer
Packets 2-8 passed
to network layer

(b)

Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

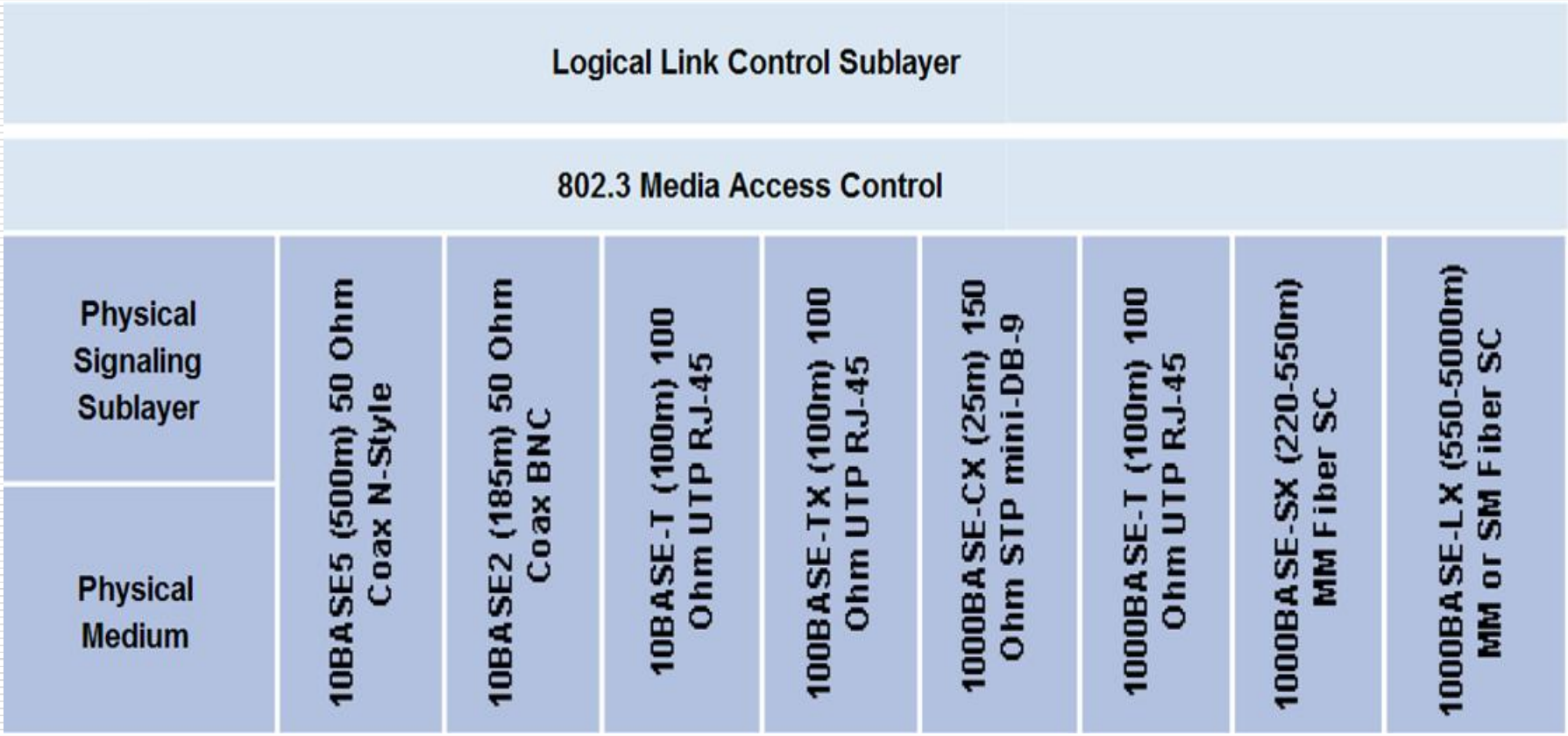
802 STANDARDS

IEEE	Title and Comments
802	Standards for Local and Metropolitan Area Networks
802.1	LAN and MAN Bridging and Management
802.2	Logical Link Control
802.3	CSMA/CD Access Method
802.3u	Fast Ethernet
802.3z	Gigabit Ethernet
802.4	Token Passing Bus Access Method
802.5	Token Ring Access Method
802.6	Distributed Queue Dual Bus Access Method (for WANs)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic Local and Metropolitan Area Networks
802.9	Integrated Services
802.10	LAN/MAN Security
802.11	Wireless LANs
802.12	High-speed LANs
802.14	Cable TV Access Method

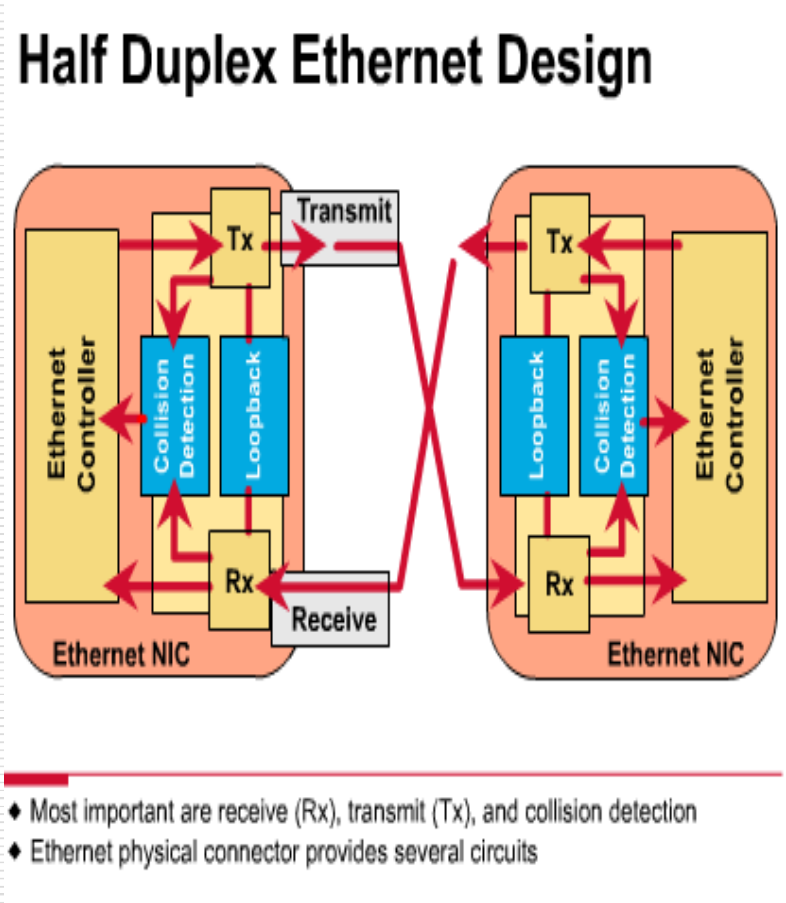
Ethernet and IEEE 802.3

- Ethernet is the most widely used LAN technology.
- Xerox Corporation's Palo Alto Research Center (PARC) developed Ethernet in the early 1970s.
- Ethernet is well suited to applications where a local communication medium must carry sporadic, occasionally heavy traffic at high peak data rates.

The Ethernet Family Tree

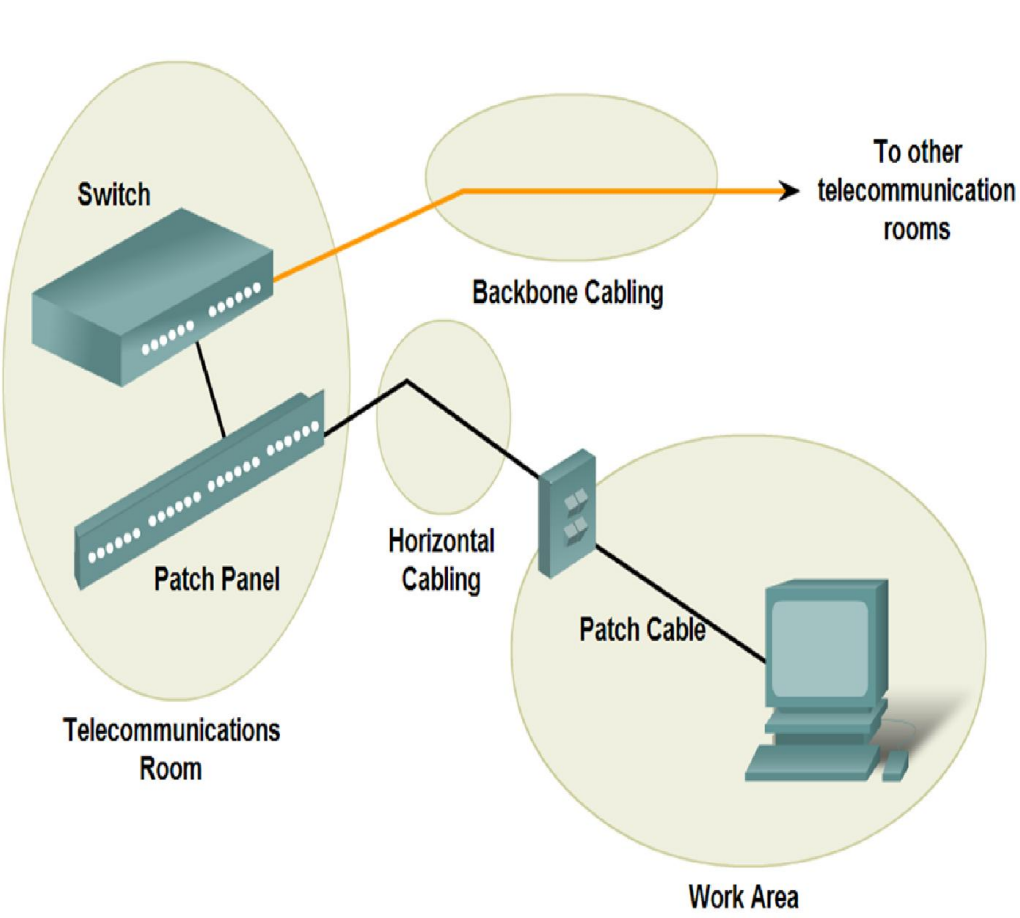


Ethernet Signaling



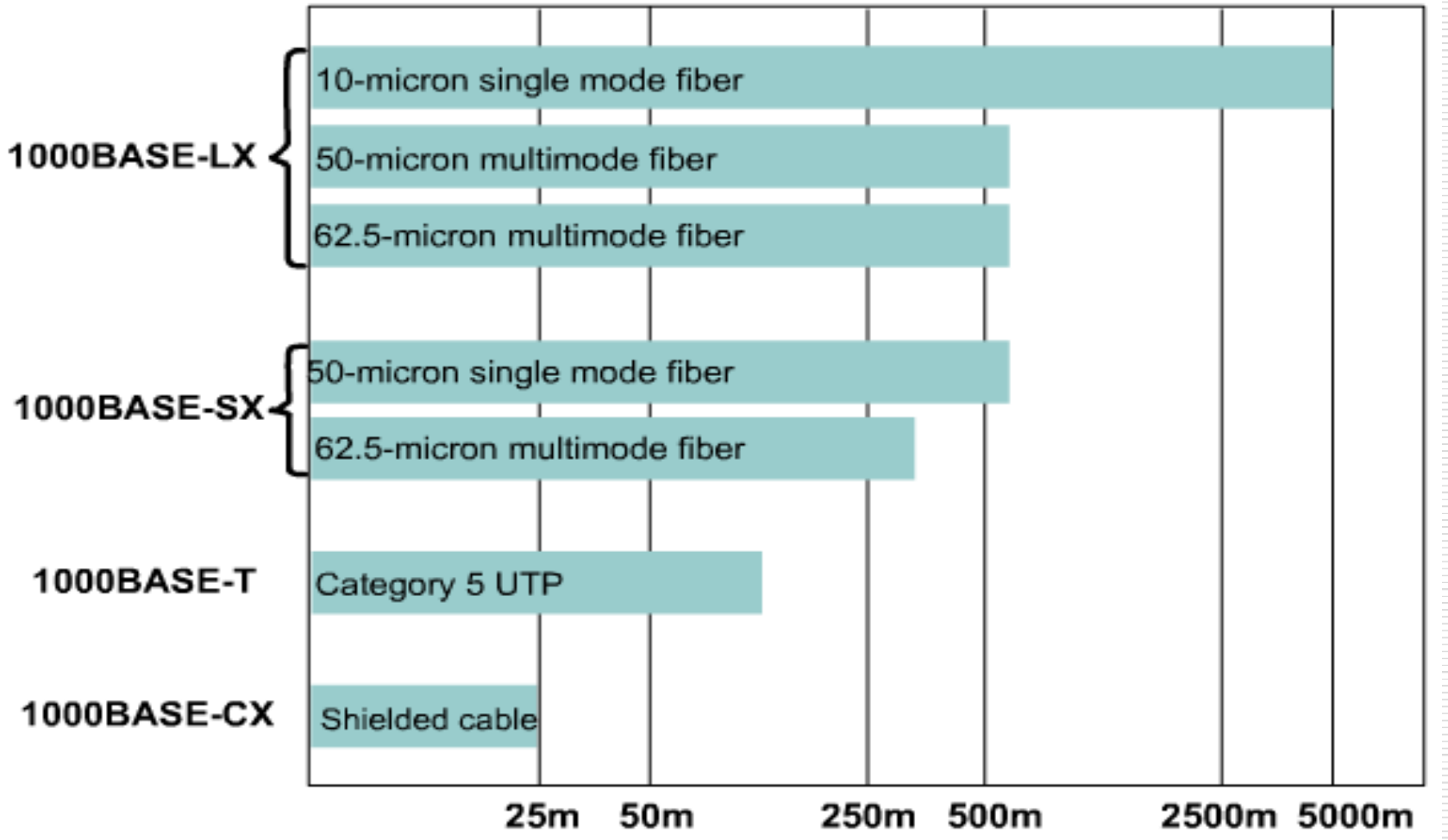
- ✓ 10BaseT signals use Manchester encoding
- ✓ 10Base-T transceivers are designed to send and receive signals over a segment that consists of 4 wires
  - ✓ 1 pair of wires for transmitting data
  - ✓ 1 pair of wires for receiving data
- ✓ Half-duplex

Ethernet 10BaseT Media and Topologies



- ✓ Horizontal cabling topology must be a star
- ✓ Maximum length of horizontal cabling for UTP cable is 90m
- ✓ Maximum length for patch cords at the telecom outlet/connector is 3 m
- ✓ Maximum length for patch cords/jumpers at the horizontal cross-connect is 6m

1000BASE Ethernet



1000BASE-T

- 1000BASE-T (IEEE 802.3ab) was developed to provide additional bandwidth to help alleviate these bottlenecks.
  - Fast Ethernet/100BASE-TX: Cat 5 copper cable
  - 1000BASE-T: would pass the Cat 5e test.
  - Most installed Cat 5 cable can pass 5e certification if properly terminated.
  - 1000BASE-T standard is interoperable with 10BASE-T and 100BASE-TX.

1000BASE-T

- Cat 5e cable can reliably carry up to 125 Mbps of traffic, then how to get 1000 Mbps of bandwidth?
  - use all four pairs of wires instead of the traditional two pairs of wires used by 10BASE-T and 100BASE-TX. This provides 250 Mbps per pair.
  - Full-duplex
  - Since the information travels simultaneously across the four paths, the circuitry has to divide frames at the transmitter and reassemble them at the receiver.
  - using 4D-PAM5 line encoding

1000BASE-SX and 1000BASE-LX

- Using NRZ encoding
- The signal can be pulsed into the fiber using:
  - Short-wavelength
    - 850 nm laser or LED source
    - multimode optical fiber (1000BASE-SX)
    - lower-cost but shorter distances
  - Long-wavelength
    - 1310 nm laser source
    - either single-mode or multimode optical fiber (1000BASE-LX)
    - Laser sources used with single-mode fiber can achieve distances of up to 5000 meters.
- The Media Access Control method treats the link as point-to-point.
- full duplex: transmitting (Tx) and receiving (Rx)
- Gigabit Ethernet permits only a single repeater between two stations

Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

Wireless LAN

- Wireless LAN
  - Communications based on cells
  - The signals sent by a station can only be received by the stations nearby
  - Short-distance transmission
- Wireless LAN Standard
  - IEEE 802.11
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g
  - IEEE 802.11n

Wireless LAN Standard

- IEEE 802.11
  - A key technology: Direct Sequence Spread Spectrum (DSSS)
  - DSSS applies to wireless devices operating within a 1 to 2 Mbps range.
  - DSSS may operate at up to 11 Mbps but will not be considered compliant above 2 Mbps
- IEEE 802.11b
  - Also called Wi-Fi™
  - It increased transmission capabilities to 11 Mbps
  - All 802.11b systems are backward compliant in that they also support 802.11 for 1 and 2 Mbps data rates for DSSS only
  - Achieves higher data throughput rate by using a different coding technique from 802.11
  - Operate within 2.4 GHz

Wireless LAN Standard

- IEEE 802.11a
  - Covers WLAN devices operating in the 5 GHz transmission band.
  - Using the 5 GHz
  - 802.11a is capable of supplying data throughput of 54 Mbps and with proprietary technology known as "rate doubling" has achieved 108 Mbps.
  - In practice, a more standard rating is 20-26 Mbps.

Wireless LAN Standard

- IEEE 802.11g
  - provides the same throughout as 802.11a (54Mbps) but with backwards compatibility for 802.11b
  - using Othogonal Frequency Division Multiplexing (OFDM) technology.
- IEEE 802.11n: next generation WLAN
  - provide double bandwidth than 802.11g, that is, 108Mbps, and theoretically up to 500-600Mbps

Wireless LAN Topology

- **Infrastructure mode** and **ad-hoc mode**

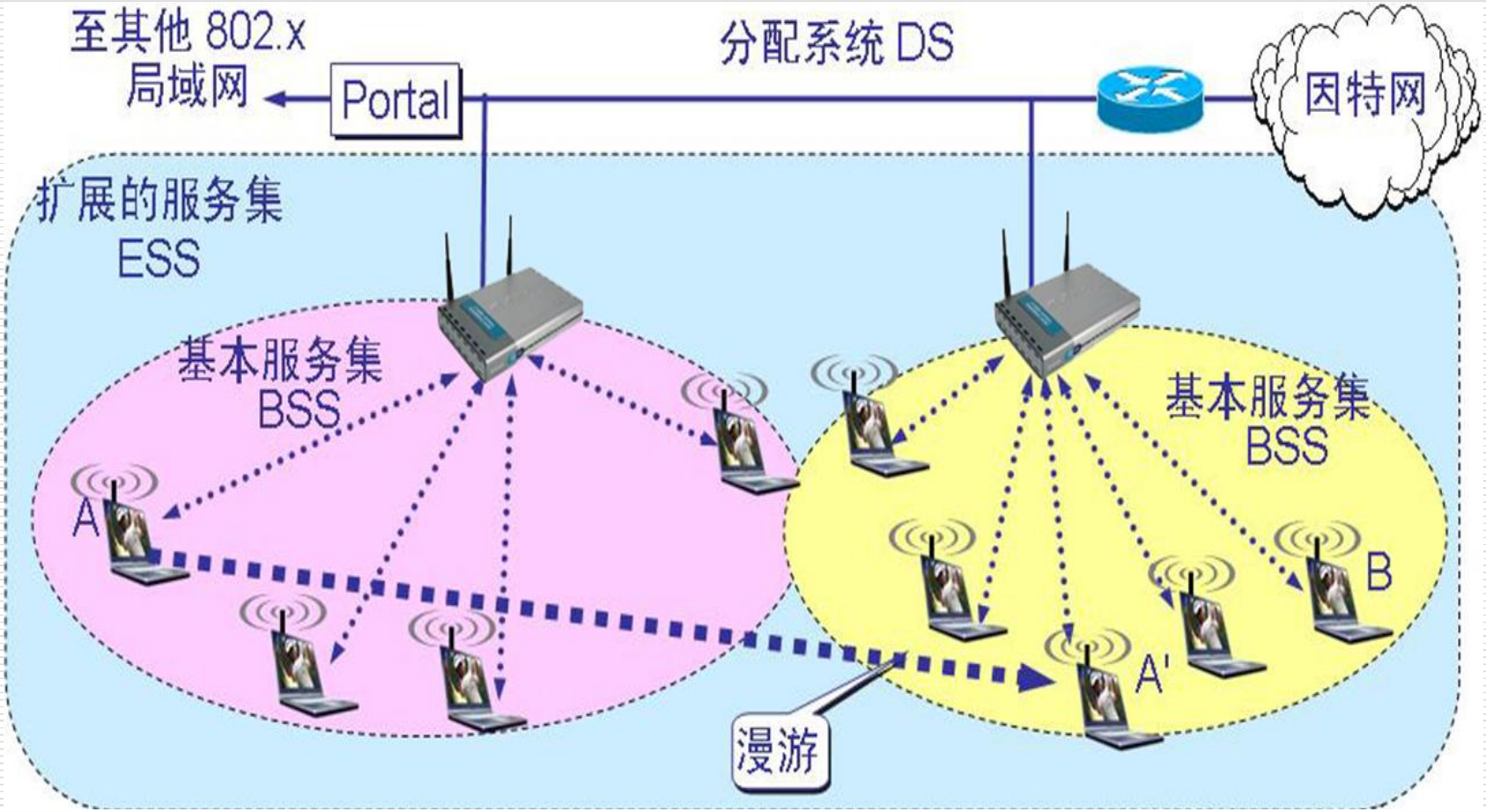


Fig. Infrastructure Mode

Wireless LAN: Infrastructure Mode

- A Basic Service Set(BSS) includes a Base Station(BS) and several wireless hosts
  - All hosts can communicate with each other directly in local BSS
- Access Point (AP) acts as a Base Station(BS) for infrastructure mode
  - AP is hard wired to the cabled LAN to provide Internet access and connectivity to the wired network
  - When an AP is installed, a Service Set Identifier(SSID) and a channel are assigned
  - The range of the cell will be from 91.44 to 152.4 meters (300 to 500 feet)
- A BSS can connect to another BSS via a Distribution System(DS), and constructs an Extended Service Set (ESS)

Accessing Procedure

- When a client is activated within the WLAN
  - it will start "listening" for a compatible device with which to "associate“
- This is referred to as "scanning"
  - Active scanning
  - Passive scanning

Active scanning

- Cause a probe request to be sent from the wireless node seeking to join the network.
- The probe request will contain the Service Set Identifier (SSID) of the network it wishes to join
- When an AP with the same SSID is found, the AP will issue a probe response
- The authentication and association steps are completed.

Passive scanning

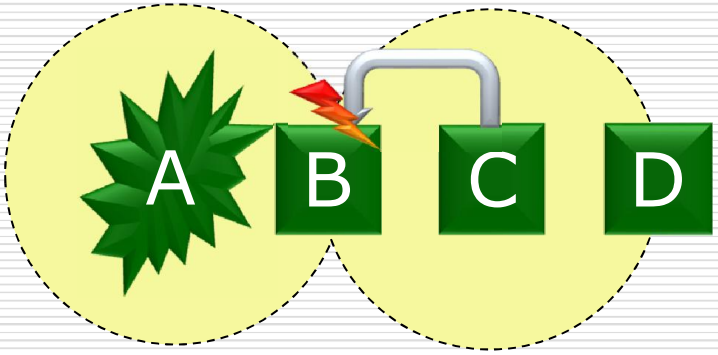
- Listen for beacon management frames (beacons), which are transmitted by the AP (infrastructure mode) or peer nodes (ad hoc)
- When a node receives a beacon that contains the SSID of the network it is trying to join, an attempt is made to join the network.
- Passive scanning is a continuous process and nodes may associate or disassociate with APs as signal strength changes.

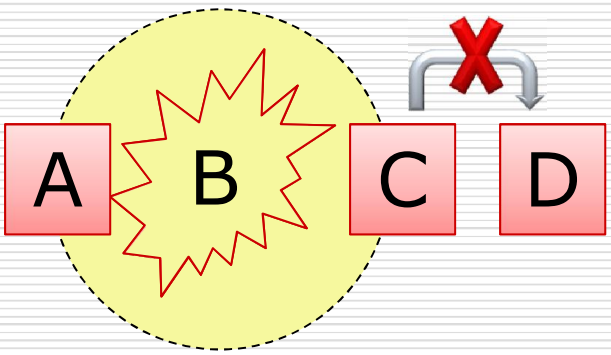
Frames in WLAN

- WLANs do not use a standard 802.3 frame.
- There are three types of frames
  - Control Frames
  - Management frames
  - Data frames(Only data frames are similar to 802.3 frames)
- The payload of wireless data frames and 802.3 frames is 1500 bytes
  - However, an Ether frame may not exceed 1518 bytes whereas a wireless frame could be as large as 2346 bytes.
  - Usually the WLAN frame size will be limited to 1518 bytes as it is most commonly connected to a wired Ethernet network.

Why We Need CSMA/CA?

- Collisions can occur in WLAN, but the stations can only know the transmission nearby, so CSMA/CD is not a good choice.
  - **Hidden Station Problem**
    - When A is transmitting data to B, C can't detect the transmission between A and B, so perhaps C will decide to transmit data to B and result in a collision at B.
  - **Exposed Station Problem**
    - When B is transmitting data to A, C can detect the transmission, so C will not transmit data to D. But that is a mistake.





Multiple Accessing Mechanism

- Ethernet
  - Signals is transmitted to all stations on the cable.
  - The sending station detects the collisions.
  - At a time, only an effective frame can be transmitted on the channel.
- WLAN
  - Signals is transmitted to stations near to the sending station on the cable
  - The MAC protocol must try it best to ensure only a sending station near to the receiving station
  - The receiving station detects the collisions.
  - At a time, multiple effective frames can be transmitted on the channel.

CSMA/CA

- CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）
  - 发送站点在发送数据前，以控制短帧刺激接收站点发送应答短帧，使接收站点周围的站点监听到该帧，从而在一定时间内避免数据发送
  - 基本过程
    - A向B发送RTS（Request To Send）帧，A周围的站点在一定时间内不发送数据，以保证CTS帧返回给A；
    - B向A回答CTS（Clear To Send）帧，B周围的站点在一定时间内不发送数据，以保证A发送完数据；
    - A开始发送
    - 若控制帧RTS或CTS发生冲突，采用二进制指数后退算法等待随机时间，再重新开始。

The Actual Throughput

- When a source node sends a frame, the receiving node returns a positive acknowledgment (ACK).
  - This can cause consumption of 50% of the available bandwidth.
  - This reduces the actual data throughput to a maximum of 5.0 to 5.5 Mbps on an 802.11b wireless LAN rated at 11 Mbps.
- Performance of the network will also be affected by signal strength
  - As the signal becomes weaker, Adaptive Rate Selection (ARS) may be invoked
  - The transmitting unit will drop the data rate from 11 Mbps to 5.5 Mbps, from 5.5 Mbps to 2 Mbps or 2 Mbps to 1 Mbps.

Layer2: Data Link Layer

- Overview of the Data Link Layer
- Ethernet and CSMA/CD
  - LLC and MAC Sub-layers
  - Media Access Control in MAC Sub-layer
  - Flow Control in LLC Sub-layer
  - Development of Ethernet
- Wireless LAN and CSMA/CA
- Layer 2 Devices

Layer 2 Devices—NICs

- NICs perform important Layer 2 data link layer functions:
  - Logical Link Control - communicates with upper layers in the computer
  - Media Access Control - provides structured access to shared access media
  - naming - provides a unique MAC address identifier
  - framing - part of the encapsulation process, packaging the bits for transport
  - signaling - creates signals and interface with the media by using built-in transceivers

Layer 2 Devices—Bridges

- Bridges divide traffic into segments and filters traffic based on the MAC address, not based on protocols.
- Bridges can improve network performance by *reducing large collision domains*.
- Bridges work best where traffic is low from one segment of a network to other segments.
  - When traffic between network segments becomes heavy, bridges can become a bottleneck and slow down communication.

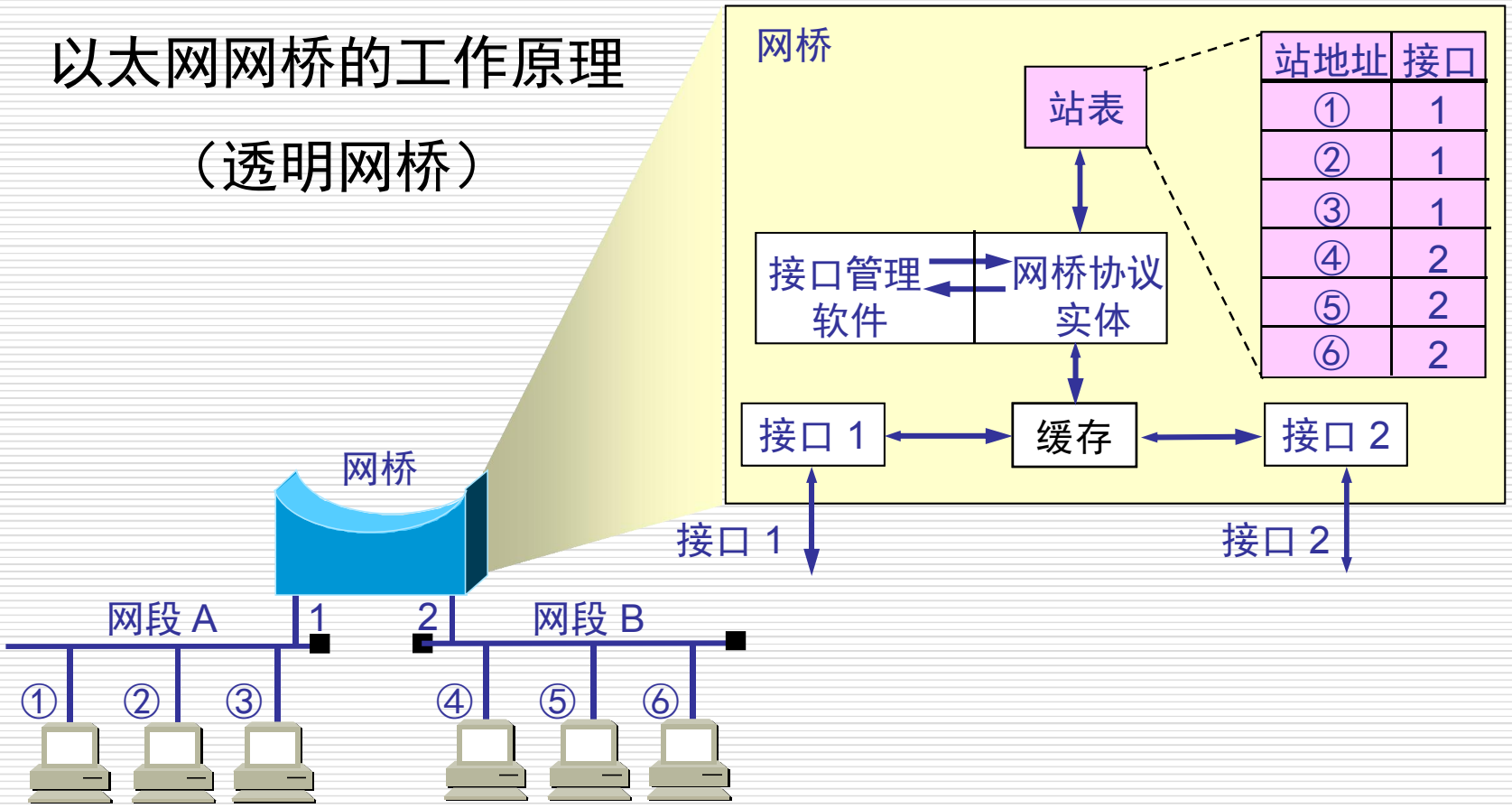
Layer 2 Devices—Bridges

- Transparent Bridge
  - “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的
  - 透明网桥是一种即插即用设备，其标准是 IEEE 802.1D
  - 目前以太网中使用得最多的网桥
- Source routing Bridge
  - 源路由(source route)网桥在发送帧时将详细的路由信息放在帧的首部中,从而使每个经过的网桥都了解帧的路径
  - 在令牌环网络中被广泛使用

Layer 2 Devices—Bridges

以太网网桥的工作原理

（透明网桥）



Transparent Bridge

- 若从 A 发出的帧从接口 x 进入了某网桥，那么从这个接口出发沿相反方向一定可把一个帧传送到 A。
- 网桥每收到一个帧，就记下其源地址和进入网桥的接口，作为转发表中的一个项目。
- 在收到一个新的帧时，将转发表中已收集到的地址记录取出，与此帧的目的地址匹配，找到对应的接口，并向该接口转发。
- 在网桥的转发表中写入的信息除了地址和接口外，还有帧进入该网桥的时间，其原因是：
  - 拓扑可能经常变化
  - 站点也可能会更换适配器（这就改变了站点的地址）
  - 工作站并非总是处于工作状态
- 把每个帧到达网桥的时间登记下来，就可以在转发表中只保留网络拓扑的最新状态信息，使得网桥中的转发表能反映当前网络的最新拓扑

Transparent Bridge

- Problem: When a device on a network wants to send data, but does not know the destination address.
  - Send out a broadcast to all devices on a network.
  - Since every device on the network has to pay attention to such broadcasts, bridges always forward them.
- Too many broadcasts can result in a broadcast storm, and it can cause:
  - network time-outs
  - traffic slowdowns
  - less than acceptable performance.

Source Route Bridge

- 透明网桥容易安装，但网络资源的利用不充分
- 源路由(source route)网桥在发送帧时将详细的路由信息放在帧的首部中
- 源站以广播方式向欲通信的目的站发送一个发现帧，每个发现帧都记录所经过的路由
- 发现帧到达目的站时就沿各自的路由返回源站
- 源站在得知这些路由后，从所有可能的路由中选择出一个最佳路由
- 凡从该源站向该目的站发送的帧的首部，都必须携带源站所确定的这一路由信息

Layer 2 Devices—Switches

- Perform two basic operations:
  - switching data frames: a frame is received on an input medium and then transmitted to an output medium
  - maintenance of switching operations: Switches build and maintain switching tables and search for loops. Routers build and maintain both routing tables and service tables.

Layer 2 Devices—Switches

- Switching is a technology that alleviates congestion in Ethernet LANs by *reducing traffic and increasing bandwidth.*
  - Switches create dedicated network segments, or point-to-point connections, and connecting these segments in a virtual network within the switch.
  - This is called a virtual circuit because it exists only when two nodes need to communicate and is established within the switch
  - You can think of each switch port as a micro-bridge; this process is called microsegmentation.
  - Each switch port gives the full bandwidth of the medium to each host

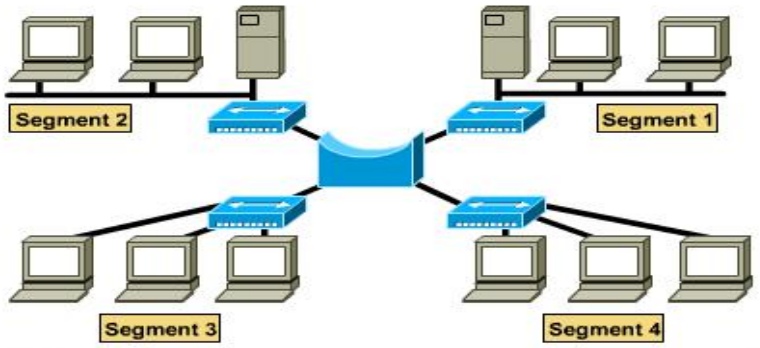
Layer 2 Devices—Switches

- LAN switch reduces the size of collision domains
- However, All hosts connected to the switch are still in the same broadcast domain.
  - That is, a broadcast from one node will still be seen by all other nodes connected through the LAN switch.

Segmentation of a Collision Domain

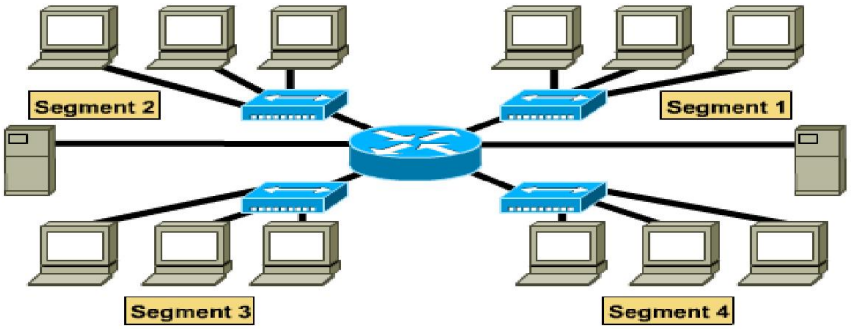
- We can create collision domains using:
  - Bridge (Layer 2)
  - Switch (Layer 2)
  - Router (Layer 3)

Segmentation with Bridges



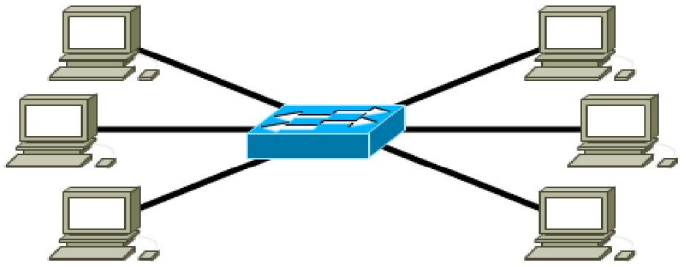
- Segmentation provides fewer users per segment
- Bridges store, then pass on all frames based on layer 2 addresses
- Layer 3 Protocol-independent
- Increase Latency on the network

Segmentation with Routers



- More manageable, greater functionality, multiple active paths
- Broadcast Domain
- Smaller Broadcast
- Operates at Layer 3 and 4

Segmentation with LAN Switches



- A switch eliminates the impact of collisions through microsegmentation
- Low latencey and high frame-forwarding rates at each interface port
- Works with existing 802.3(CSMA/CD) compliant network interface cards and cabling

Bridge Segmentation of a Collision Domain

- Ethernet LANs that use a bridge for segmenting the LAN provide more bandwidth per user because there are fewer users on the segment.
- Bridges pass on data frames regardless of which Layer 3 protocol is used.
- Bridges increase the latency (delay) in a network by *10 to 30 percent* because of the decision making that is required.
- A bridge is considered a store-and-forward device because it must receive the entire frame and verify the cyclic redundancy check before forwarding can take place

Switch Segmentation of a Collision Domain

- Switches are significantly faster because they switch in *hardware*, while bridges switch in *software*.
- A 10 Mbps Ethernet LAN and a 100 Mbps Ethernet LAN can be connected by using a switch.
- In a switched Ethernet implementation, the available bandwidth can reach close to 100 percent.
- Shared Ethernet networks perform best when kept to less than 30 to 40 percent of full capacity because of CSMA/CD.
- Some switches support cut-through switching, which reduces latency and delays, while bridges only support store-and-forward switching.

Router Segmentation of a Collision Domain

- Router can create the highest level of segmentation:
  - Create smaller collision domains
  - Create smaller broadcast domains: routers do not forward broadcasts unless programmed to do so.
- Routers accomplish forwarding of packets by examining the destination logical address on the data packet and then looking in its routing table for forwarding instructions
- Because routers perform more functions than bridges, they operate with a higher rate of latency.
- Routers can work as gateway:
  - be used to connect different networking media and different LAN technologies

谢 谢！