MODULE 12: Network Components and Access Technologies

Lecture 12.1
Data Link Layer and MAC

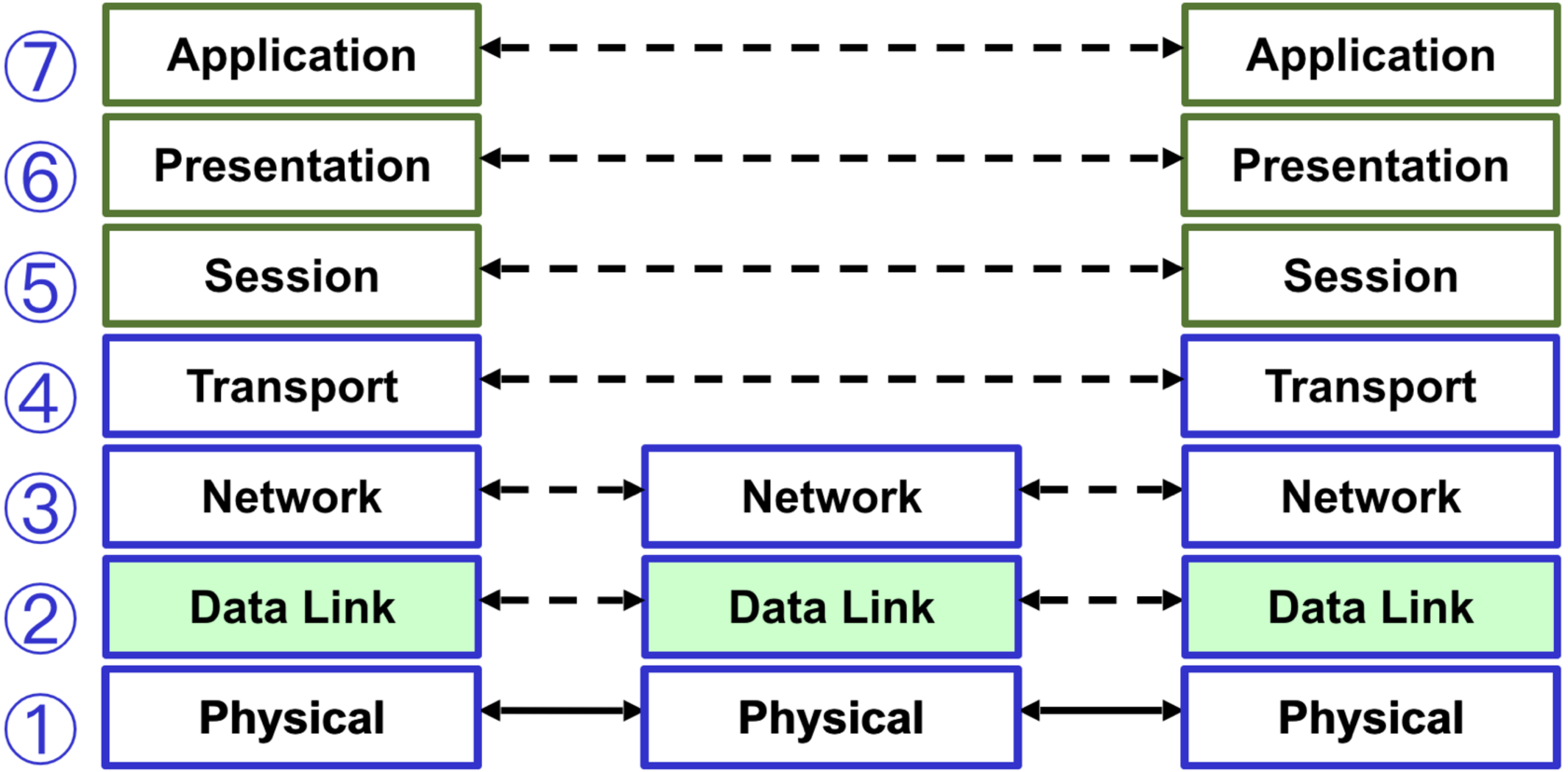
Prepared By:
- Scott F. Midkiff, PhD
- Luiz A. DaSilva, PhD
- Kendall E. Giles, PhD

Electrical and Computer Engineering
Virginia Tech

Lecture 12.1 Objectives

- Describe the role of reliable data transfer protocols
- Describe sources of errors that introduce the need for reliable transfer mechanisms
- Discuss basic approaches to error recovery, including stop-and-wait protocols
- Explain the need for framing at the data link layer
- Discuss the role of multiple access in networks
- Discuss basic features of contention-based multiple access schemes

OSI Seven-Layer Reference Model



Data Link Layer Functionality

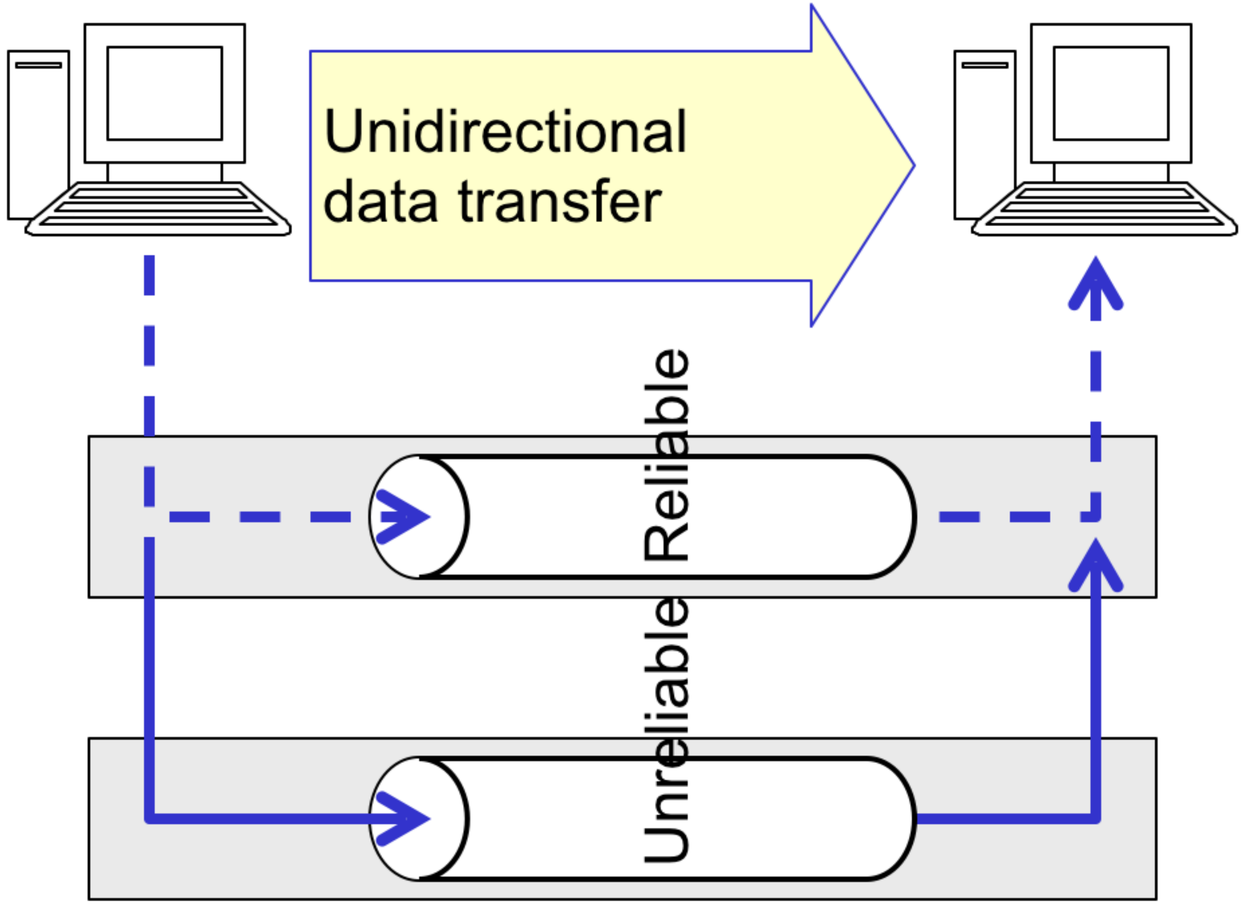
- The data link layer is responsible for the error-free transmission of packets between “adjacent” or directly-connected nodes
- The medium access control (MAC) function is a sub-layer of the data link layer
  - Allows multiple nodes to share a common transmission media
  - Supports addressing of nodes
- The logical link control (LLC) function is another sub-layer
  - Provides functions such as error recovery

Link Layer and MAC Topics

- Reliable data transfer – a logical link control function to provide reliable link-level transmission
- Framing – a logical link control function to allow the receiver to structure the received data stream
- Medium access control – the MAC function to allow multiple nodes to share the common transmission media

Reliable Data Transfer Protocols

- Link layer
  - Reliable link layer built on top of an unreliable physical layer
- Transport layer
  - Reliable transport layer (like TCP) built on top of an unreliable network layer (like IP)



CHECK POINT

As a checkpoint of your understanding, please pause the video and make sure you can do the following:

- Describe the role of reliable data transfer protocols

If you have any difficulties, please review the lecture video before continuing.

Why Do Errors Occur?

- Channel impairments
  - The physical layer cannot provide error-free transmission (more likely in wireless networks)
  - The link layer may detect errors, but may not correct errors
    - Ethernet detects, but does not correct
    - IEEE 802.11 detects and corrects, within limits
- Packet loss
  - Buffer overflow at the receiver
  - Buffer overflow at intermediate routers due to congestion

Correcting Errors

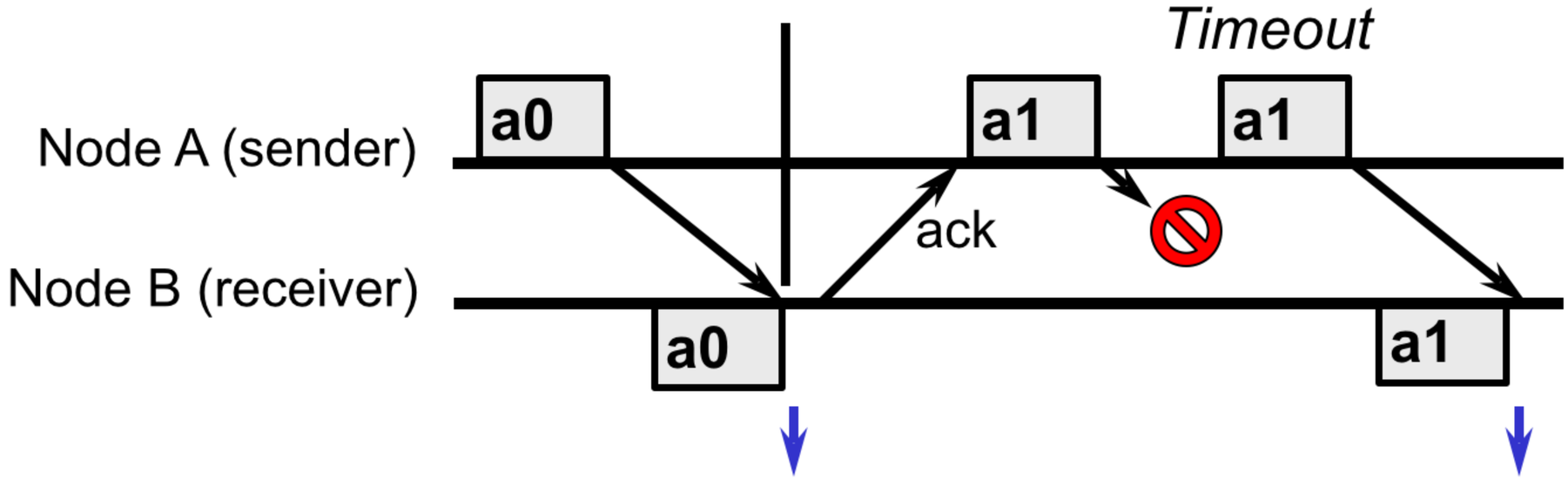
- Two basic approaches to error correction
  - Forward error correction
  - Retransmission
- Forward error correction (FEC)
  - Extra information must be sent to allow the receiver to correct bit errors (up to some limit)
  - Coding bits are always sent
  - Trades off channel capacity in exchange for reduced delay

Correcting Errors (cont'd)

- Retransmission – automatic repeat request (ARQ)
  - Packets are retransmitted when an error is detected
  - Need some kind of positive or negative acknowledgement
  - Delay for retransmission is introduced to correct an error

Example: Stop-and-Wait ARQ

- The sender transmits a packet and then waits for a reply from the receiver before sending the next packet
- The receiver replies with an acknowledgment (ACK) if the packet is error-free (it may reply with a negative acknowledgment, or NAK, if an error is detected)

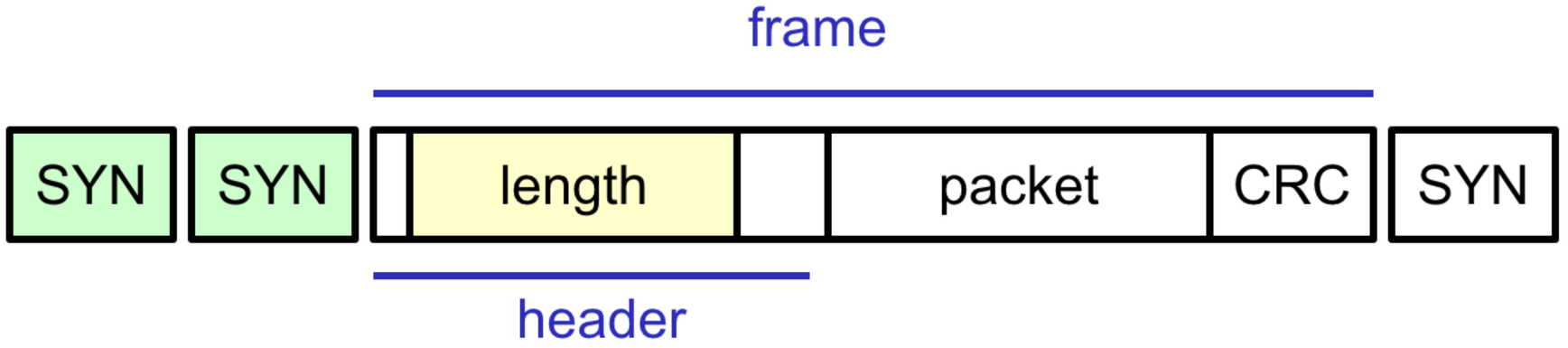


Framing

- The physical (PHY) layer simply delivers a bit stream to the destination; error detection is up to the data link layer
- Data link layer breaks the bit stream into frames and adds redundancy to enable error detection
  - Framing is the process of deciding where successive frames start and end
- There are a number of ways to realize framing
  - Character count, character stuffing, bit stuffing, framing with length fields, and physical layer coding violations for framing

Framing Example

- There are two aspects to framing:
  - Detecting the end of idle fill – can be done by transmitting a special character (e.g. SYN) or a constant bit stream (e.g. all 1's) that is interrupted when the frame begins
  - Detecting the end of the frame – can be done by sending length information (e.g. number of bytes in the frame) in the header



CHECK POINT

As a checkpoint of your understanding, please pause the video and make sure you can do the following:

- Describe sources of errors that introduce the need for reliable transfer mechanisms
- Discuss basic approaches to error recovery, including stop-and-wait protocols
- Explain the need for framing at the data link layer

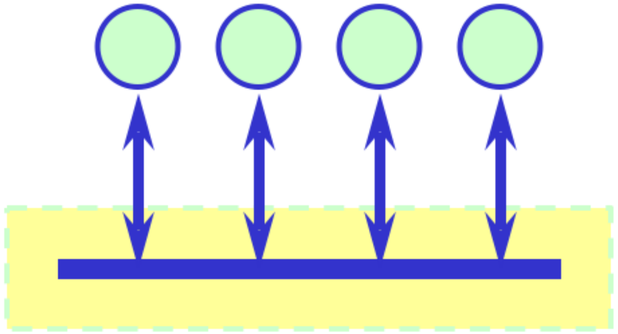
If you have any difficulties, please review the lecture video before continuing.

Need for Medium Access Control

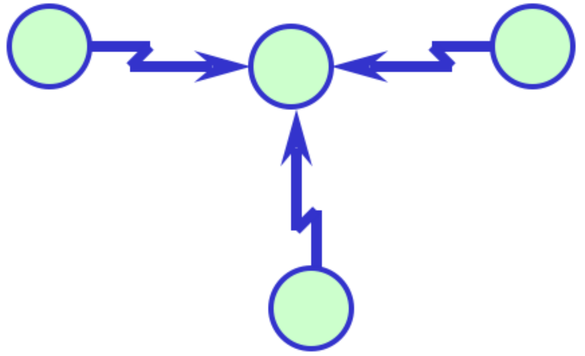
- Networks, especially local area networks, often share a single medium
  - Shared “bus,” often at a hub
  - Shared spectrum for wireless (RF) networks
- Sharing is driven by:
  - Connectivity – compared to N(N-1) links if not shared
  - Cost considerations
  - A limited resource, especially RF
- A scheme is needed for sharing the medium

Multiaccess Media Examples

Multitap bus (Ethernet)



Wireless (RF) network



Multiaccess media are communication media where the received signal is the sum of attenuated transmitted signals plus the effects of delay, distortion, and noise

Static Versus Dynamic Sharing

- Static channelization: specific capacity is dedicated to a connection
  - Examples: FDM, synchronous TDM
  - Not optimal for LANs since the transmission needs of stations are unpredictable and bursty
- Dynamic medium access control: capacity is allocated in a dynamic fashion
  - Reservation-based: round-robin and scheduled
  - Random access (contention-based)

Contention-Based Schemes

- Stations contend in some random manner for the shared medium
- Simple to implement as a distributed protocol
- Performance
  - Efficient under light to moderate load
  - Performance tends to collapse under heavy load
- Examples: CSMA, CSMA/CD

Contention-based (random access) schemes are widely used in both wired and wireless local area networks

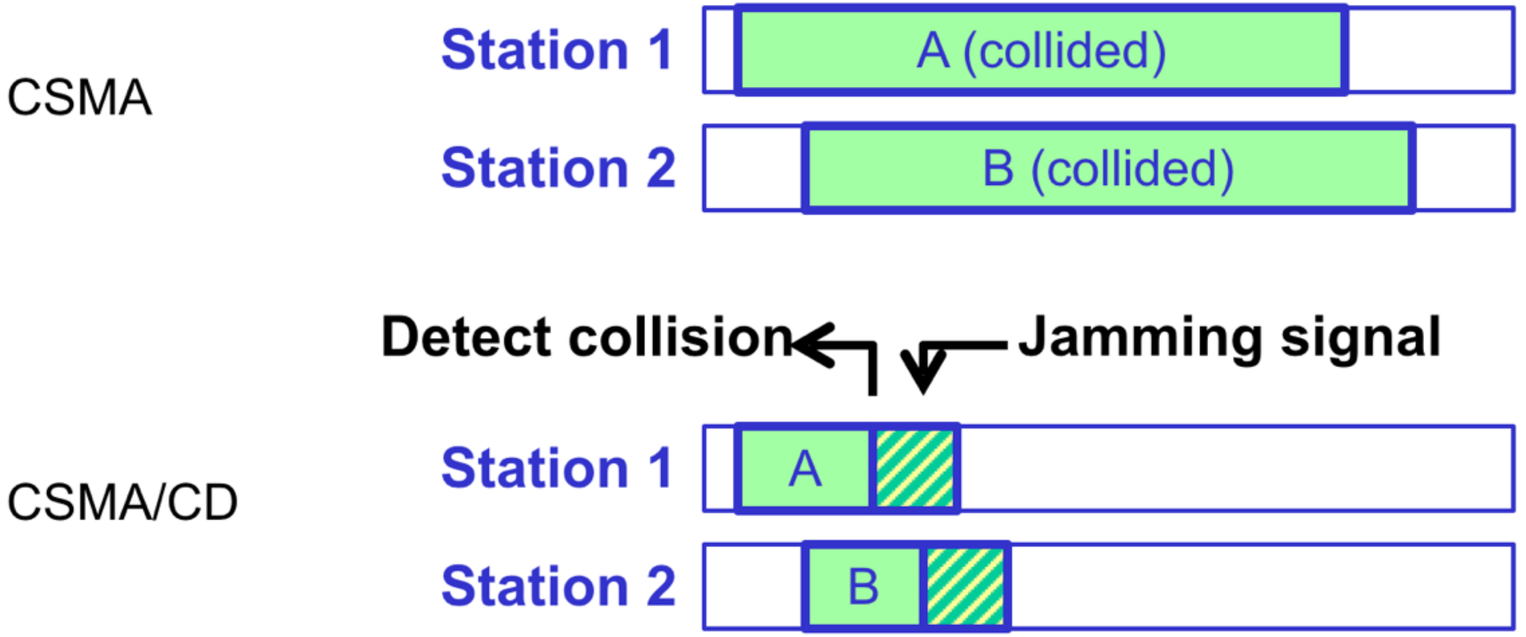
CSMA

- In carrier-sense multiple access (CSMA), nodes first listen for a carrier (a transmission) and only start transmitting if the channel is idle
  - "Listen before talking" approach
  - But, propagation delay means that collisions can still occur
  - A higher propagation delay implies a higher collision probability
- There are variations of CSMA: 1-persistent, non-persistent, and p-persistent

CSMA/CD

- Simple CSMA wastes time due to the fact that collided packets are transmitted in their entirety
- CSMA with collision detection (CSMA/CD) permits stations to monitor the network as they transmit (listen while talking)
  - If a collision occurs, stations send a short “jamming” signal and end the transmission early
- Ethernet (IEEE 802.3) uses CSMA/CD
  - Uses 1-persistent CSMA scheme (aggressive)
  - Truncated binary exponential backoff scheme for random waits after collisions ensures stability

CSMA and CSMA/CD



- With CSMA/CD Stations 1 and 2 detect the collision, send jamming signals, and stop transmission
- The full transmission time, which is wasted due to collision, is avoided

CHECK POINT

As a checkpoint of your understanding, please pause the video and make sure you can do the following:

- Discuss the role of multiple access in networks
- Discuss basic features of contention-based multiple access schemes

If you have any difficulties, please review the lecture video before continuing.

Summary

- Packets can be lost due to corrupted data or discarded packets
- ARQ schemes retransmit packets to recover from lost packets
- Stop-and-wait ARQ protocols illustrate basic principles of ARQ protocols, but are inefficient for general use
- Framing is the process of deciding where each frame starts and ends

Summary (contd.)

- Multiple access protocols allow multiple stations to share the wired or wireless medium
- Schemes may be synchronous or asynchronous
- Contention-based schemes are widely used due to simplicity of distributed implementation and efficiency in many LAN scenarios
- CSMA uses a “listen before talking” to reduce the probability of a collision
- CSMA/CD reduces the penalty of a collision by terminating transmission of collided packets

MODULE 12: Network Components and Access Technologies

Lecture 12.1
Data Link Layer and MAC

Prepared By:
- Scott F. Midkiff, PhD
- Luiz A. DaSilva, PhD
- Kendall E. Giles, PhD

Electrical and Computer Engineering
Virginia Tech