CSE 3231 / CSE 5231
Computer Networks

Chapter 4
Medium Access Sub-Layer
part 2

William Allen, PhD

Fall 2021

Bluetooth

- Very short range communication between mobile phones, PDAs, notebook computers and other personal or peripheral devices
  - Operates in the license-exempt band at 2.4 GHz
  - Has a range of 10 m to 100m with longer ranges for newer versions of the protocol
  - Versions run from 1.0 to (currently) 5.2
- Communication devices typically are associated with one individual or group
  - May be categorized as Personal Area Network (PAN)

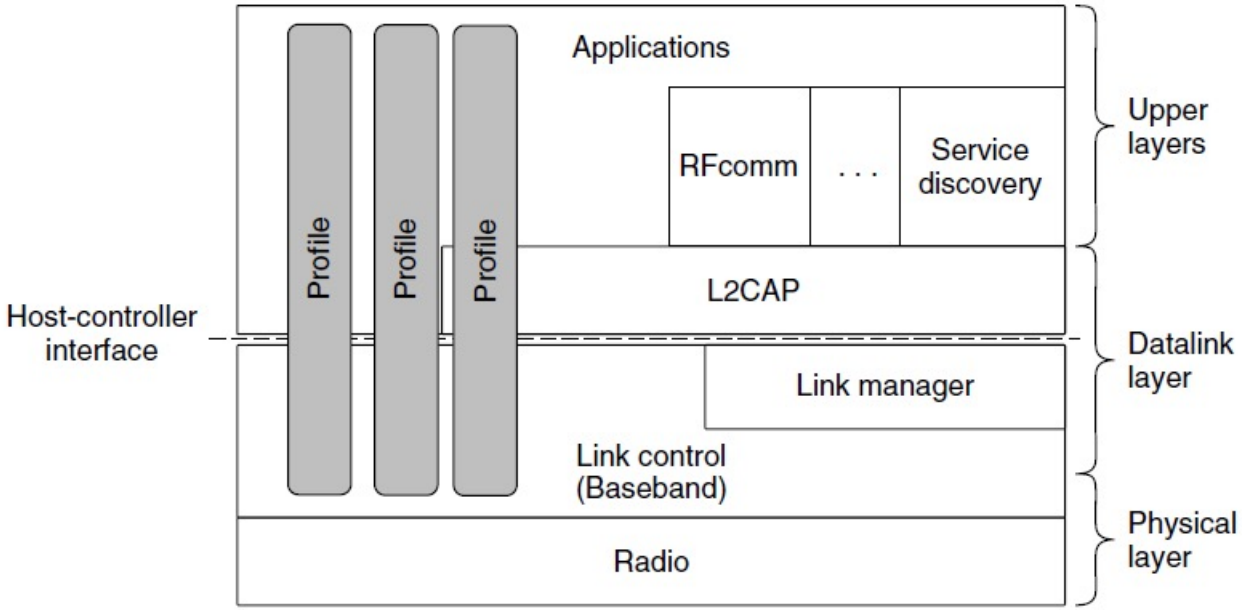
Bluetooth

- Originally specified by IEEE 802.15, now by an industry consortium called the Bluetooth Special Interest Group
- It specifies an entire suite of protocols, going beyond the link layer to define application protocols, which it calls *profiles*, for a range of applications
  - One profile gives a mobile computer access to a wired LAN
  - Another is a profile for synchronizing a PDA with personal computer, etc.
- The basic network configuration is called a *piconet*
  - Consists of a manager and up to seven connected devices
  - All communication is between the manager and other devices
  - Devices can be *parked*: set to an inactive, low-power state
  - Two piconets can be bridged into a *scatternet*

Bluetooth Applications / Protocol Stack

Profiles specify protocols for a given application

– Can have up to 25 profiles for devices like headset, streaming audio, remote control, intercom, personal area network, etc.



Bluetooth Radio / Link Layers

Radio layer:

- Uses adaptive frequency hopping in 2.4 GHz band

Link layer:

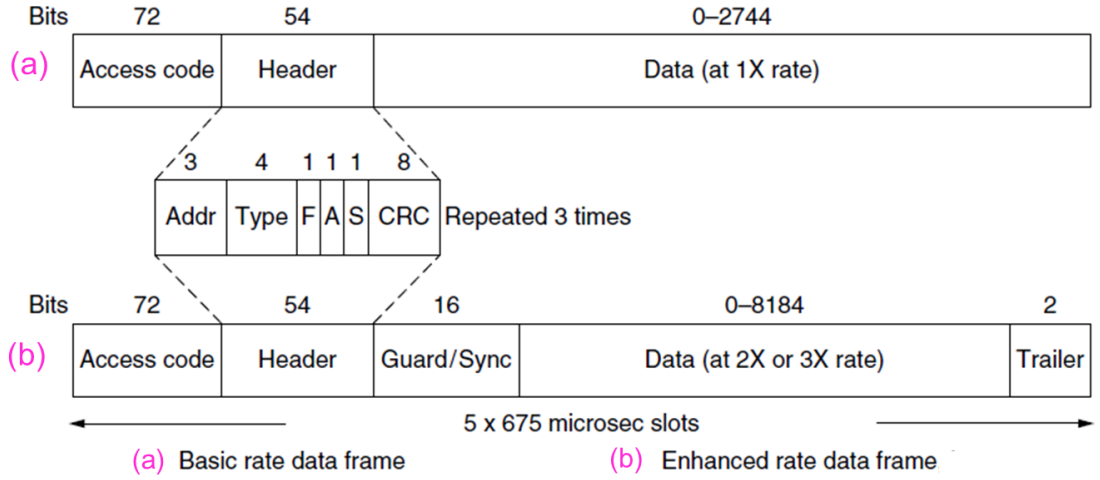
- TDM with timeslots for each device
- Synchronous Connection-Oriented link is used for real-time data and has a fixed slot in each direction
- Asynchronous Connection-Less link is used for packet-switched data with no fixed slots allocated
  - best-effort delivery: packets may be lost or delayed
- Links undergo pairing (user confirms with passkey or PIN) to authorize them before use

Bluetooth Frames

Time slots are fixed size, enhanced data rate just puts more data in the frame, reducing frame overhead

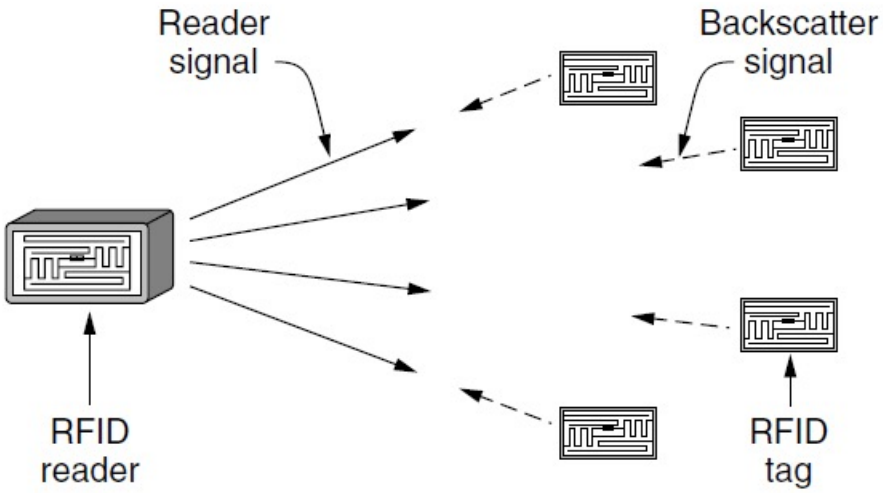
The header is actually repeated 3 times per frame

- With only 8 devices, addresses are 3 bits in length
- Flow control pauses transmissions when receiver is busy (F bit)
- Acknowledgements can be piggybacked (A bit)
- Uses a stop-and-wait protocol with 1-bit synchronization (S bit)



Radio Frequency Identification (RFID)

- Passive identification mechanism, widely used
- RFID reader transmits a signal that powers the tags, tags reply with a *backscatter* signal
- These slides describe the Electronic Product Code (EPC) version of RFID



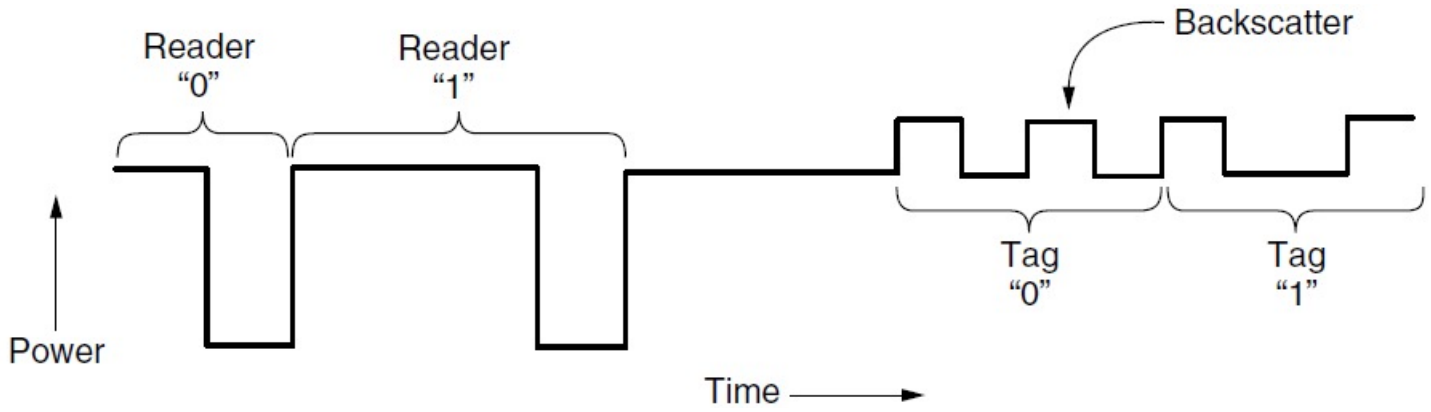
RFID (EPC) Gen 2 Physical Layer

The link is half-duplex with Amplitude Shift Keying

Reader is always transmitting a fixed carrier signal to power the tags and sends data to trigger a tag's reply

– Bits are transmitted in bursts of different lengths, for example, a 1 bit is longer than a 0 bit

Tags backscatter the reader's carrier signal and modulate it in pulses to send 0's and 1's



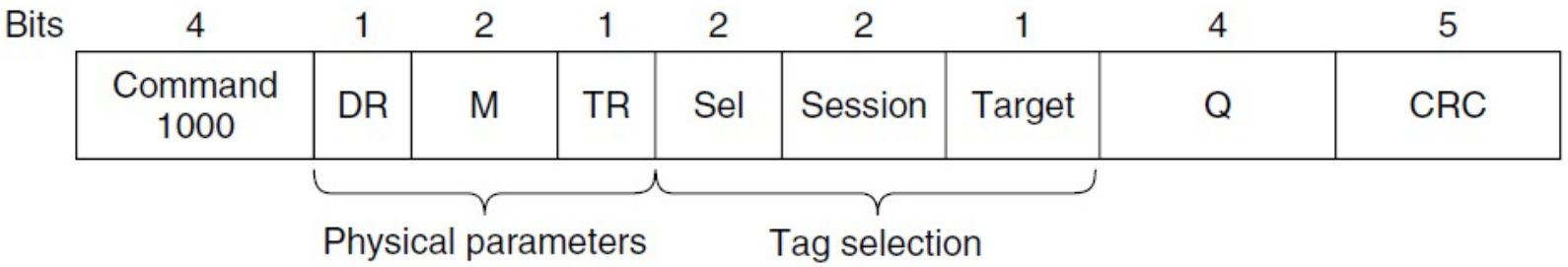
Gen 2 Frames

Reader frame formats vary depending on type

- Query frame has parameters and error detection
- Parameters indicate which tag, which slots to use for the reply, response rate, etc.

Tag responses are simply data

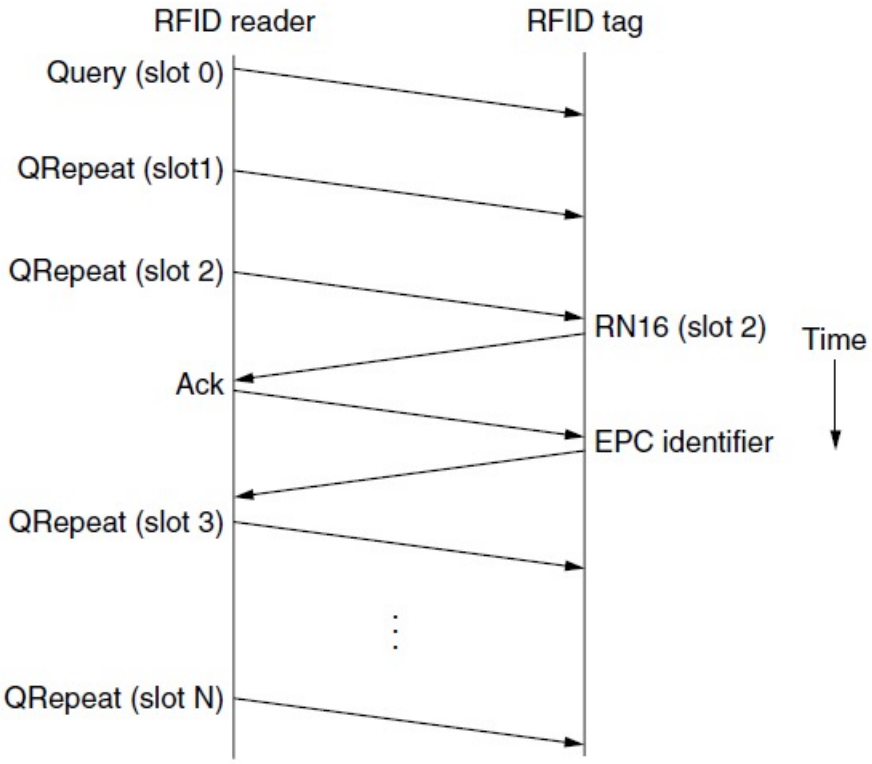
- Reader sets timing and knows the expected format



Query message

Gen 2 Tag Identification Layer

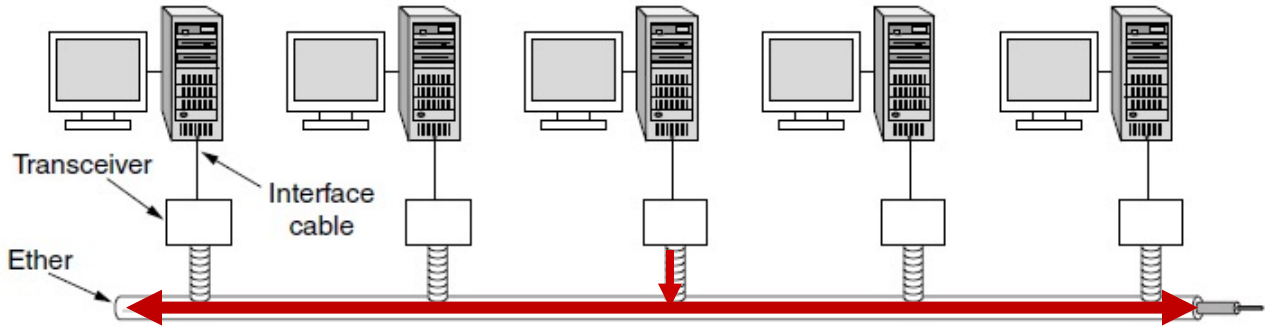
- Reader sends tag queries in slots it controls
- Tags reply with a random number in a random slot (they may collide)
- If no collision, reader then sends an ACK to ask the tag for its identifier
- This gives that tag the slot and it replies with its ID
- This process continues until all tags are ID'd



Classic Ethernet

Ethernet LANs used one shared coaxial cable to which all hosts are attached

- 10 Mbps, half-duplex with Manchester encoding
- Hosts ran the classic Ethernet protocol for (shared) access to the network
  - Any signal placed on the Ethernet by a host is broadcast over the entire network



Classic Ethernet

Ethernet technology evolved quickly

- Coaxial cables came in two varieties:
  - 10Base5 (10Mbps, 500 meter maximum length
  - 10Base2 (10Mbps, 200 meter maximum length)
- Twisted-pair cabling arrived with 10BaseT
  - T stands for twisted pair and, with 4 or more individual wires, twisted pair cables can support full-duplex transmissions
- The normal 10BaseT configuration has nodes connected to a special repeater called a *Hub*

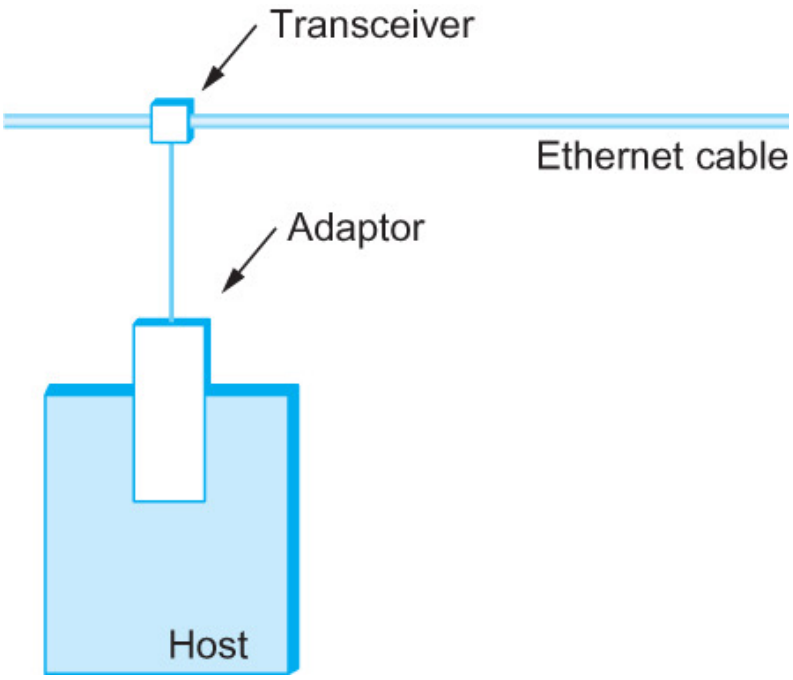
10Base2

10BaseT

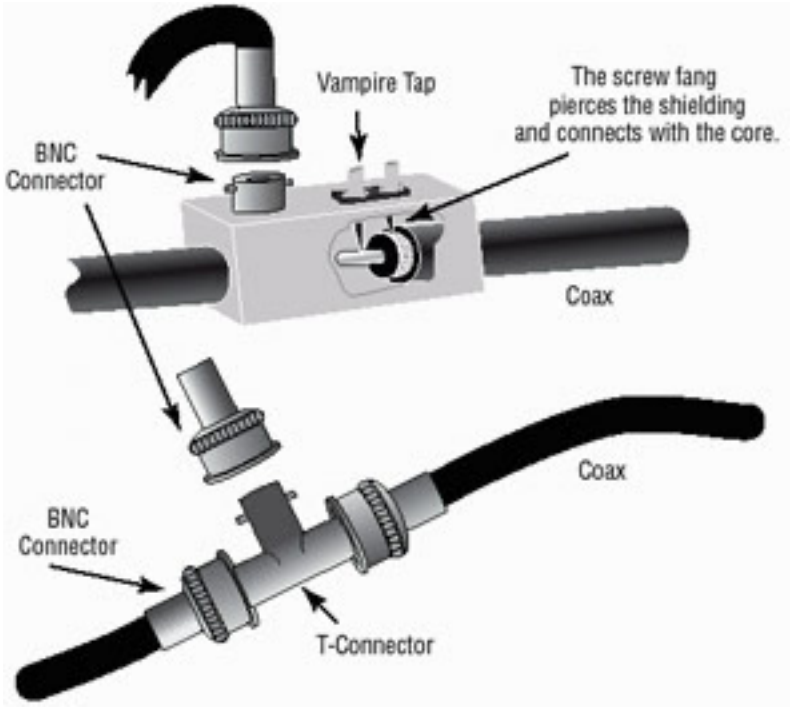
Classic Ethernet

- An original Ethernet segment was implemented on a coaxial cable of up to 500 meters
  - This cable is similar to the type used for cable TV except that it has an impedance of 50 ohms instead of cable TV's 75 ohms
- Hosts connect to an Ethernet segment by tapping into it.
  - A transceiver (a small device directly attached to the tap) detects when the line is idle and drives signal when the host is transmitting
  - The transceiver also receives incoming signal
  - The transceiver is connected to an Ethernet adaptor which is plugged into the host
  - The protocol is implemented on the adaptor

Classic Ethernet



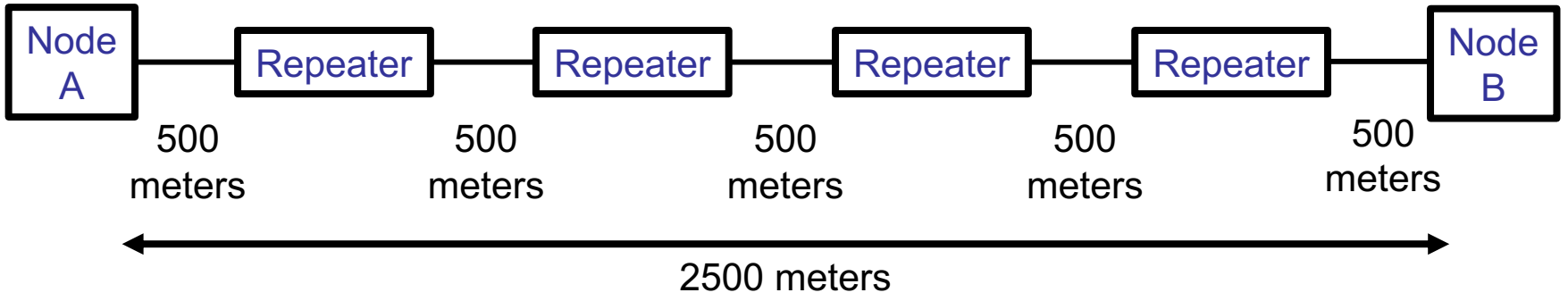
Ethernet transceiver and adaptor



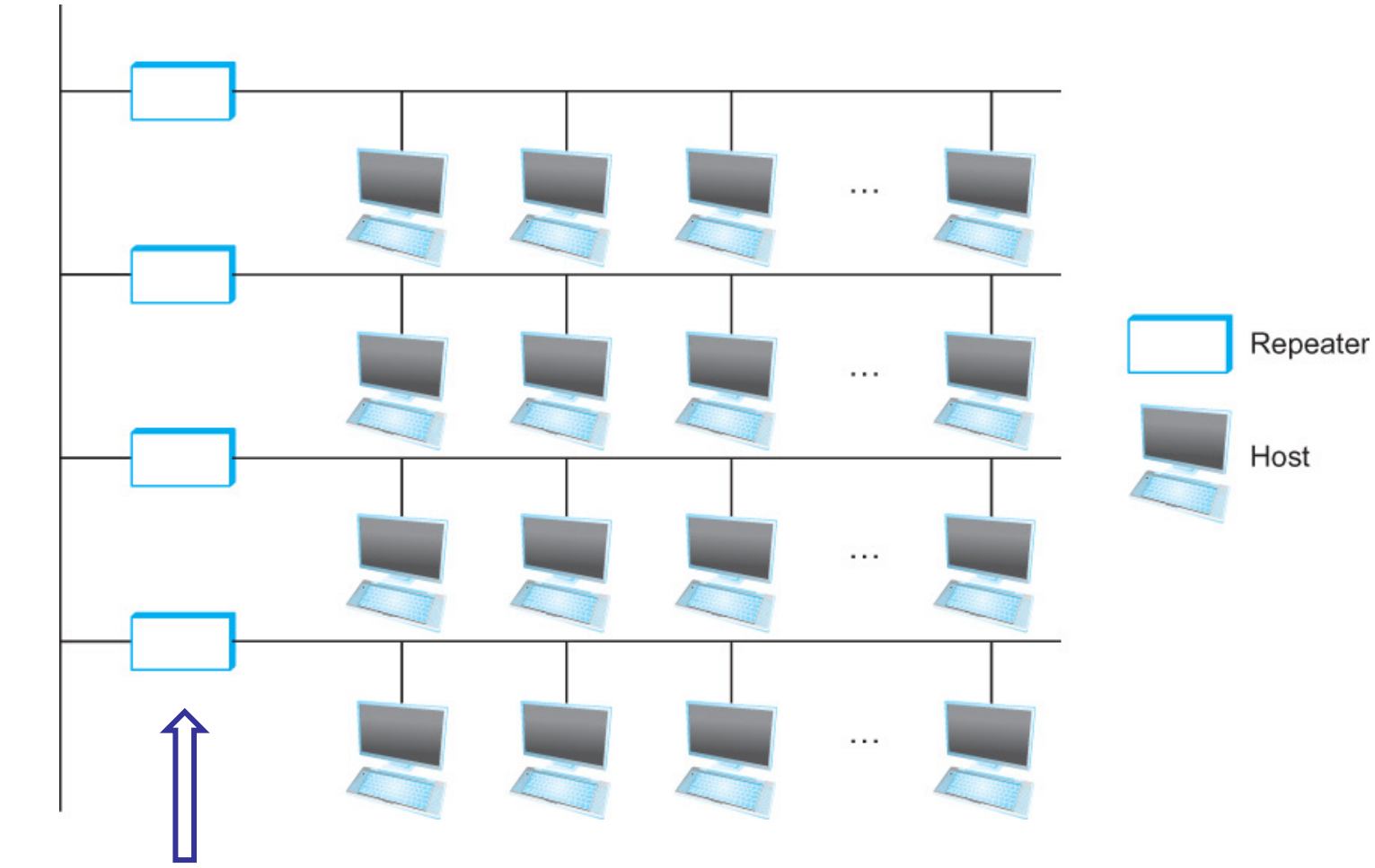
Physical connections to Ethernet cable

Classic Ethernet

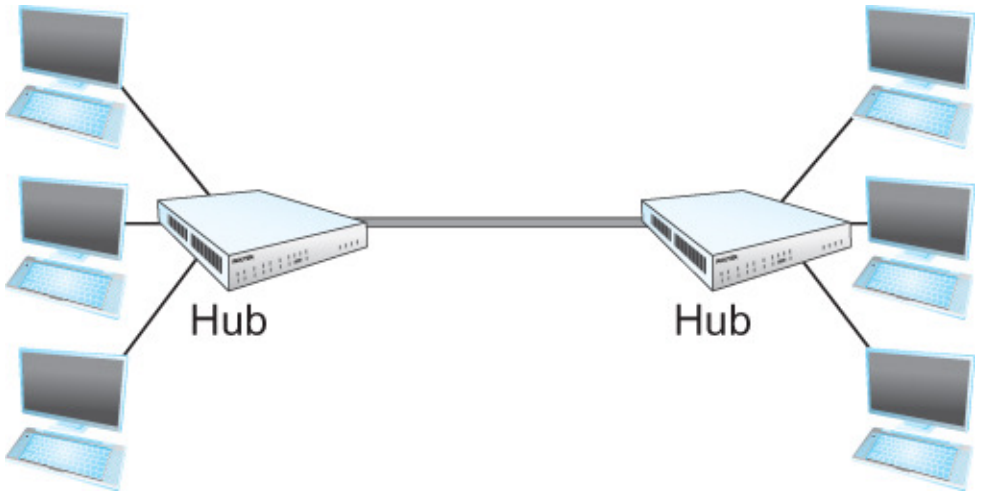
- Multiple Ethernet segments can be joined together by devices called *repeaters* that amplified and relayed the electronic signal
- No more than four repeaters may be positioned between any pair of hosts
  - A classic Ethernet LAN has a total reach of 2500 m



Classic Ethernet



Classic Ethernet

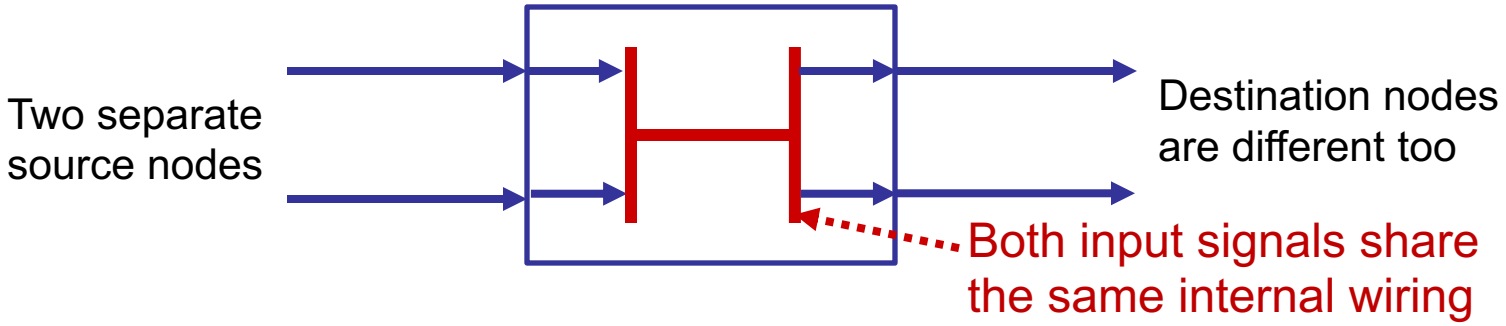


Multiple nodes connected to an Ethernet *Hub* where they were joined to the rest of the LAN. This removed the need to physically connect all nodes to the same long cable, but *all frames were still sent to all nodes* on the LAN.

Classic Ethernet

Basic hubs do not isolate traffic

- Unlike switches, hubs do not “know” which link connects to specific nodes, they just pass the input signals to all outputs
- Inputs from two different nodes can collide if they arrive at overlapping times
  - even if they are not connecting the same nodes



- Some hubs can also act as a repeater

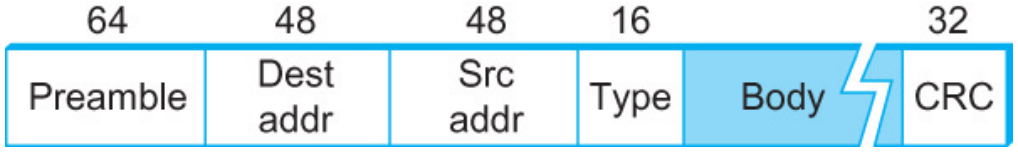
Ethernet Frame Format

Classic Ethernet follows the IEEE 802.3 standard

- This classic frame format is still used in modern LANs

Frame format

- A frame must contain at least 46 bytes (368 bits) of data to support collision detection (i.e., minimum length of 512 bits after Preamble)
- Preamble (64 bits): allows the receiver to synchronize with the signal (it contains a sequence of alternating 0s and 1s)
- Source (Host) and Destination Address (48 bits each)
- Packet type (16 bits): acts as a demultiplexor key to identify the higher level protocol contained in the frame
- Data (up to 1500 bytes)
- CRC (32 bits)



Ethernet Addresses

- Each host on an Ethernet (i.e., every Ethernet host in the world) has a unique 6-byte address.
- The address belongs to the *adaptor*, not the computer.
  - It is usually stored in ROM, but can often be spoofed (replaced)
- Ethernet addresses are typically printed in a human-readable format
  - As a sequence of six numbers separated by colons.
  - Each number corresponds to 1 byte of the 6 byte address and is given by a pair of hexadecimal digits, one for each of the 4-bit nibbles in the byte (leading 0s are not always shown)
  - For example, `8:0:2b:e4:b1:2` represents:

    `00001000 00000000 00101011 11100100 10110001 00000010`

Ethernet Addresses

- To ensure that every adaptor gets a unique address, each manufacturer of Ethernet devices is allocated a unique *prefix* that is prepended to the address on the adaptors they make
  - A 24-bit prefix allows up to 4 million different manufacturers, but many have more than one
    - AMD has been assigned the prefix 08:00:20
    - Some Dell computers have: 00:1E:4F
    - Apple devices may use: 00:1B:63 or 00:23:6C
  - The other 24 bits allow up to 4 million devices for each manufacturer code

Ethernet Addresses

- Each frame is received by the adaptor on every node so that it can read the MAC address
- If an adaptor sees its address is the destination, the Data Link layer processes the frame
- An Ethernet address where all bits are a `1` is treated as a *broadcast* address.
  - All adaptors will process broadcast frames
- An address with the first bit set to `1` followed by at least some `0`s is called a *multicast* address.
  - A host can configure its adaptor to accept a specific multicast address to join a multicast group

The Ethernet MAC Sublayer

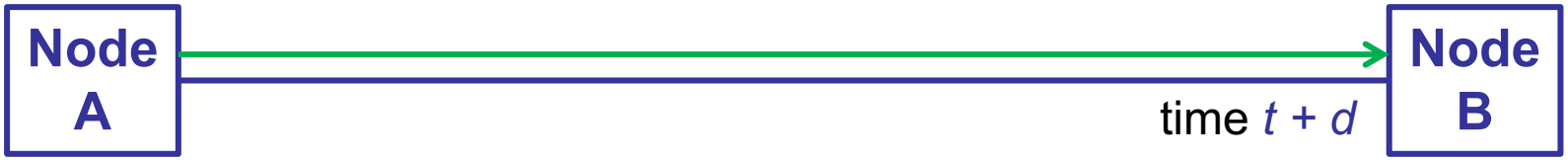
- Ethernet uses the CSMA/CD protocol
  - MAC uses *1-persistent* CSMA/CD
- When the adaptor has a frame to send, it first "listens" for activity (the *Carrier Sense* part)
- If the line is idle, it transmits the frame immediately (following the *1-persistent* rule)
  - The upper bound of 1500 bytes in the message means that each adaptor can occupy the line for a fixed length of time (for the *Multiple Access* part)
- If the line is busy, it waits for the line to go idle and then transmits immediately

Ethernet Collision Detection

- Since Ethernet supports collision detection, each sender is able to determine whether a collision is in progress.
- At the moment an adaptor detects that its frame is colliding with another, it first transmits a *jamming sequence* (a special bit pattern) and then stops transmission.
  - The jamming sequence ensures that a signal is being sent for a *long enough time* that all other nodes can detect that a collision is occurring

Ethernet Collision Detection

- Node A begins transmitting a frame at time *t*
  - *d* denotes the one-way link latency
  - the first bit of A's frame will arrive at B at time *t* + *d*



- Suppose that some time before Node A's frame arrives, Node B begins to transmit its own frame
  - B's frame will collide with A's frame and this collision will be detected by Node B soon after

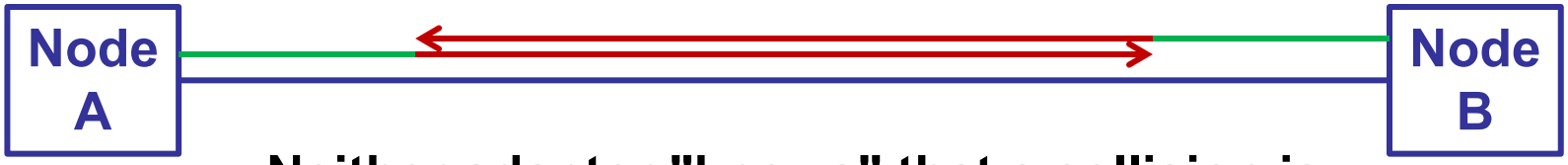
  - Node B will send the *jamming* sequence to notify all nodes (including Node A) of the collision

Ethernet Collision Detection

- If two hosts are close to each other, then a few bits provide enough overlap to detect a collision
  - If they were farther apart, they would have to transmit longer, sending more bits, to detect the collision.
  - The worst case scenario happens when the two hosts are at opposite ends of the Ethernet cable
- To know for sure that the sender's frame did not collide with another frame, the transmitter may need to send as many as 512 bits (64 bytes).
  - Ethernet frames are required to be at least 512 bits
    - 14 bytes of header + 46 bytes of data + 4 bytes of CRC

Ethernet Collision Detection

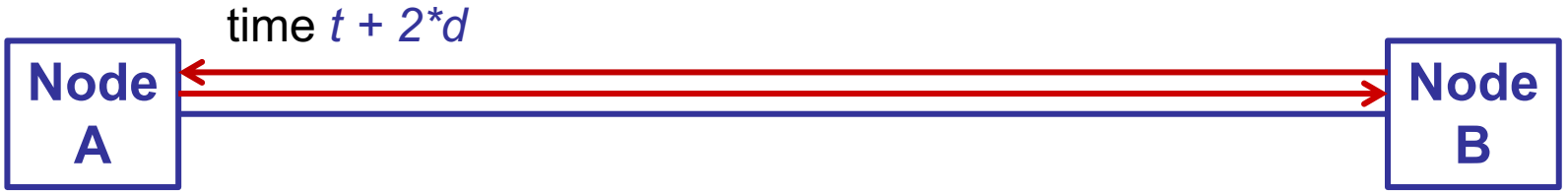
- Why 512 bits? Or, a related question is:
  - “Why is an Ethernet's length limited to 2500 m?”
- An adaptor can't tell a collision is happening until it "hears" the signal from the other node
  - The farther apart two nodes are, the longer it takes for a frame sent by one to reach the other, and the network is vulnerable to collision during that time



Neither adaptor "knows" that a collision is occurring until the other node's signal arrives

Ethernet Collision Detection

- Node A will not know that the collision occurred until B's frame reaches it, which may not happen until time *t + 2 * d*



- Node A will continue to transmit until it senses that a collision occurred
  - Therefore, Node A could transmit for as long as time *2*d* before it detects a collision with its frame
  - Node A, and all nodes between A and B, will "know" that Node B has detected a collision because Node B is now sending the jamming sequence

Ethernet Collision Detection

- Consider that an Ethernet is up to 2500 m between any two hosts (including repeaters)
  - The round trip delay for 2500m has been determined to be 51.2 μs
  - On 10 Mbps Ethernet, that corresponds to *512 bits*
- The other way to look at this situation:
  - We want to limit an Ethernet's maximum latency to a fairly small value (say, 51.2 μs) for the multiple access algorithm to work correctly
    - Hence the maximum length for an Ethernet is 2500 meters

Ethernet Collision Detection

- Once an adaptor has detected a collision, and stopped its transmission, it waits a certain amount of time and tries again.
  - Each time the adaptor tries to transmit but fails, it randomly selects the amount of time it waits before trying again
  - Thus, each node is more likely to wait a different length of time before resending
- The wait times are based on powers of 2, referred to as *Binary Exponential Backoff*

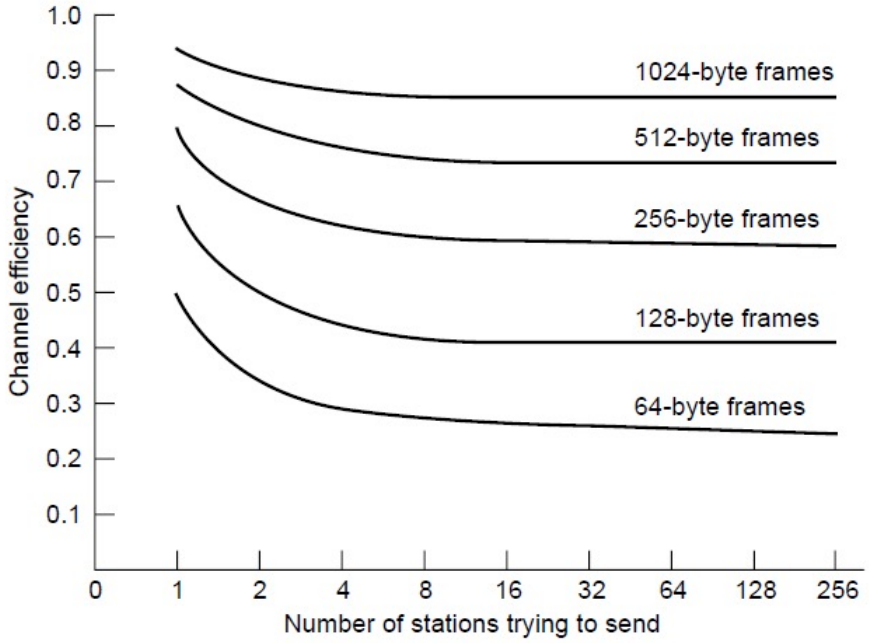
Ethernet Collision Detection

- After detection, the adaptor first delays either 0μs or 51.2μs, selected at random
  - If this fails, it randomly selects a wait time from 0, 51.2, 102.4μs before trying again;
  - This is k * 51.2μs for $k \in \{0, 1, 2\}$
  - After the third collision, it waits k * 51.2μs for $k \in \{0 \ldots 2^3 - 1\}$ (also selected at random)
- In general, the algorithm randomly selects a k between 0 and $2^n - 1$ and then waits for k * 51.2μs, where n is the number of collisions experienced so far

Classic Ethernet – Performance

Highly efficient with large frame sizes, even with many senders

- Degrades with small frames (and long LANs)



Frame Format Examples

- Cloudshark - cloud-based version of Wireshark

- Example frames:
  - PPP - frames 1-5 show steps in link configuration
  - Ethernet - frames 6-7 show an exchange of frames
  - WiFi - frames 8-9 show a TCP connection request and also show the protocol layers in TCP/IP

https://www.cloudshark.org/captures/d2e34d5f1c2e