

Local Area Networks

Local Area Networks

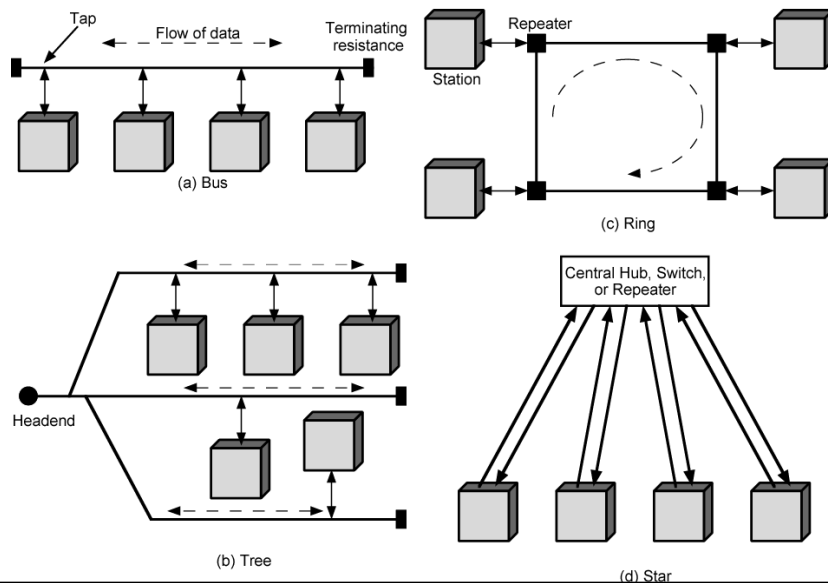
- Interconnection network with scope limited to single or cluster of buildings
- Typically owned and managed by a single organization
- Shared medium or broadcast networks
 - Medium access control in addition to other link layer functions
- Greater data rates shared among limited users
- Different types of architectures and protocols
 - Ethernet (Wired LANs) – IEEE 802.3
 - WiFi (Wireless LANs) – IEEE 802.11
 - Token Rings – IEEE 802.5

LAN Applications

- Applications of LAN

- Personal computer LANs
 - Share resources (e.g., printers)
 - Share information (e.g., files)
 - "Limited" data rate (10Mbps – 1000Mbps)
- Backend networks
 - Interconnecting large systems (mainframes and large storage devices)
 - High data rate
- Storage Area Networks
 - A separate network to handle storage needs
 - Hard disks, tape libraries, CD arrays
 - Detaches storage tasks from specific servers

LAN Topologies



Ring Topology

- Consists of a set of repeaters in a closed loop
 - Repeater: a simple device that receives data on the incoming link and retransmits on the outgoing link
 - Links are unidirectional
 - Stations attach to repeaters
- Frame
 - Circulates around the ring and pass all stations
 - Destination recognizes its address and copies frame
 - Circulates back to source and is then removed
- **Medium access control** determines when a station can insert frame into the ring

Bus Topology

- Consists of a set of stations tapped to a medium
 - Station sends frame on medium which is “heard” by all other stations
 - Frame is transmitted till the end of wire, where it is absorbed
 - No other station can transmit while transmission is ongoing
- Frame
 - Travels from source to destination in both directions
 - Destination recognizes its address and copies frame
 - Frame absorbed at the end points by terminator
- **Medium access control** determines if a station can insert frame or not
 - Typically listen and transmit if free, retransmit if collision.

Star Topology

- Each station is directly connected to a **central node**
 - Usually via two point-to-point links (full duplex transmission)
- Two types of central node
 - Simple one: operate in a broadcast fashion
 - Transmission of a frame from one station to the central node is retransmitted on all of the outgoing links
 - Only one station can transmit at a time
 - The central node is referred to as a **hub**
 - Complex one: act as switching device
 - An incoming frame is buffered in the central node and then retransmitted on the outgoing link to the destination station
 - Intelligence to selectively transmit frames
 - More than one stations can transmit at the same time
 - Buffer required at the central node to resolve conflict
 - The central node is referred to as a **switch**

Hubs

- Central element of a star topology
- Each station connects to hub by two lines
 - Transmit and receive
 - So **a link consists of two unshielded twisted pairs (UTP)**
- Hub acts as a repeater
 - When one station transmits, hub repeats signal to each station
 - **Physically star, logically bus**
- Limited to about 100 m
 - High data rate and poor transmission qualities of UTP
 - Optical fiber may be used for about 500 m
- Transmission from any station received by all other stations
 - Stations can receive frames to any destination
 - If two stations transmit at the same time, collision

Buses and Hubs

- Similarity:
 - All stations share capacity of bus (e.g. 10Mbps)
 - Transmission from any station received by all stations
 - Only one station transmitting at a time
- Difference:
 - Hub uses star wiring to attach stations to hub
 - Easy installation: each floor has a wiring closet and a hub can be placed there to connect all stations in this floor
 - Easy maintenance: hub can recognize a malfunctioning station and auto-cut it out of the network
 - Hub can form a tree topology: head hub, intermediate hubs
- Improve performance with layer 2 switch

Choice of Topology

- Transmission medium
 - Twisted pair: popularly used by today's Ethernet
 - Baseband coaxial cable (digital signaling): was used by the original Ethernet
 - Broadband coaxial cable (analog signaling): not popular due to the cost
 - Optical fiber: popularly used by Ethernet
 - Air: used in wireless LANs
- Installation and maintenance
 - For bus and ring topology, installation also means removing some existing links, so it is costly
 - For ring topology, a failure of one link disable the entire network
 - For **star topology**, it can take advantage of the natural layout of wiring in a building, and installation/maintenance of one link does not affect other links
 - Star topology is the most popular one today

LAN Protocol Architecture

- LAN protocol only concerns physical layer and data link layer.
- IEEE 802 protocols are the industrial standard on the specification of different LANs. It consists of three layers
 - Logical link control (LLC)
 - Medium access control (MAC)
 - Physical

IEEE 802 Layers

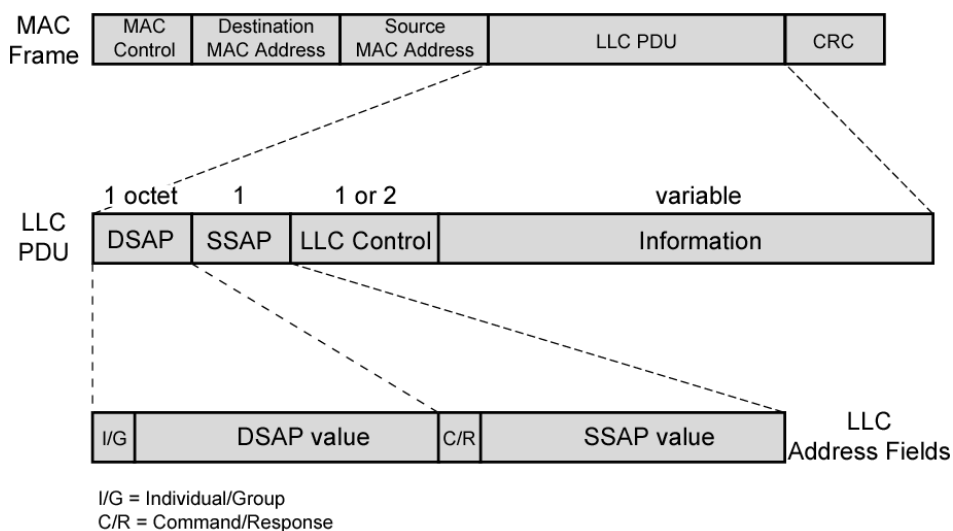
- Physical Layer
 - Encoding/decoding of signals
 - Preamble generation/removal
 - for synchronization
 - Bit transmission/reception
 - Transmission medium and topology
- Medium Access Control
 - Manage access to a shared-access medium
 - Not found in traditional point-to-point layer 2 data link protocol
- Logical Link Control
 - Provide interfaces (called “services”) to higher layers
 - Perform flow and error control



Medium Access Control

- To control access to the shared transmission medium to provide an orderly and efficient use of the capacity.
- Different types of medium access control schemes
 - Centralized scheme: a controller is designated that has the authority to grant access to the network, e.g., 802.16 (WiMax)
 - Advantages:
 - Greater control
 - Simple access logic at station
 - Avoids problems of co-ordination
 - Disadvantages:
 - Single point of failure
 - Potential bottleneck
 - Distributed scheme (or decentralized scheme): stations collectively determine dynamically the order
 - Synchronous scheme
 - a specific capacity is dedicated to a connection, like TDM, FDM
 - Asynchronous scheme
 - able to allocate capacity in response to demand

Generic MAC Frame Format



Bridges

- Need to expand beyond the confines of a single LAN.
- Devices used to interconnect LANs: bridges and routers
 - Bridges work at Layer 2, whilst routers work at Layer 3
- Bridge
 - Read all frames transmitted on one LAN and accept those addressed to any station on the other LAN, retransmit them on the second LAN
 - Can interconnect different types of LANs, can convert one frame format to another

Why Not One Large LAN?

- Reliability
 - A fault on the network may disable communication for all devices.
 - Bridge partitions into self-contained units
- Performance
 - Performance declines with number of devices or the length of the wire.
 - Smaller LANs improve performance if intra-network traffic exceeds internetwork traffic.
- Security
 - Multiple LANs may improve security.
- In summary
 - Bridges provides an extension to the LAN without modification to stations.
 - Virtually single LAN though physically connected with bridges

Layer 2 Switches

- Switches selectively forward frames
 - Incoming frame from a particular station switched to appropriate output line
- More than one station can transmit at a time
 - Increased capacity of LAN
- Two types of layer 2 switches
 - Store-and-forward switch
 - Cut-through switch - begins transmitting the incoming frame as soon as it recognizes the destination address

Layer 2 Switch v Bridge

- Layer 2 switch functions as a multiport bridge.
- Differences
 - Bridge handles frames in software, switch performs address recognition and frame forwarding in hardware
 - Bridge only analyzes and forwards one frame at a time, switch has multiple parallel data paths, so it can handle multiple frames at a time
- Bridge has suffered commercially
 - New installations typically adopt layer 2 switches with bridge functionality

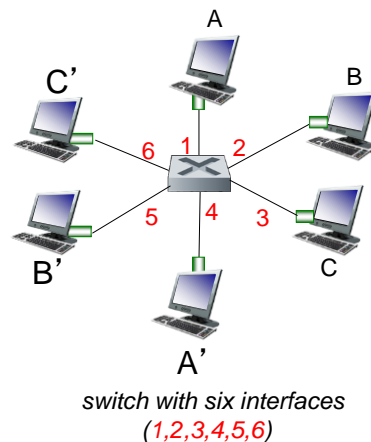
Layer 2 Switch

- **link-layer device: takes an *active* role**
 - store, forward frames
 - examine incoming frame's address, **selectively** forward frame
- **transparent**
 - hosts are unaware of presence of switches
- **plug-and-play, self-learning**
 - switches do not need to be configured



Switch: *Multiple* Simultaneous Transmissions

- hosts have **dedicated, direct connection** to switch
- switches buffer packets
- **Ethernet protocol** used on *each* incoming link, but no collisions; **full duplex**
 - each link is its own collision domain
- **switching**: A-to-A' and B-to-B' can transmit simultaneously, without collisions

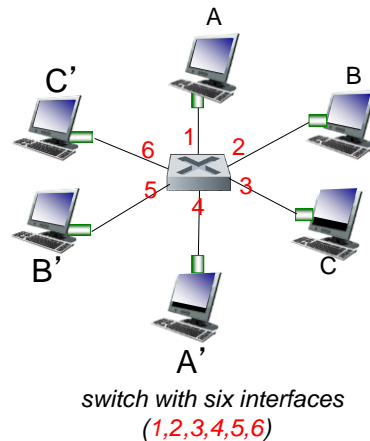


Switch Forwarding Table

how does switch know A' reachable via interface 4, B' reachable via interface 5?

- each switch has a **switch table**, each entry:
 - (MAC address of host, interface to reach host, time stamp)
 - looks like a routing table!

how are entries created, maintained in switch table?



Self Learning

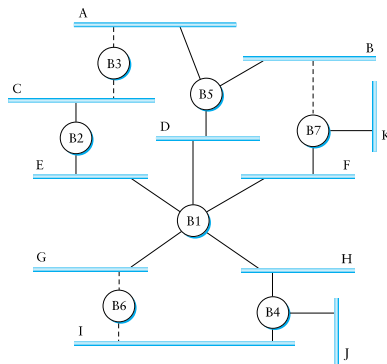
- A bridge/switch has a **forwarding (or switch) table**
- entry in forwarding table:
 - (MAC Address, Interface, Time Stamp)
 - stale entries in table dropped (TTL can be 60 min)
- Bridge/switch **learns** which hosts can be reached through which interfaces
 - when frame received, switch “learns” location of sender: incoming LAN segment
 - records sender/location pair in forwarding table

Filtering/Forwarding

when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
 - then {
 - if destination on segment from which frame arrived
 - then drop frame
 - else forward frame on interface indicated by entry
 - }
 - else flood /* forward on all interfaces except arriving interface */

Spanning Tree



- Need to disable some ports for forwarding, so that no loops in network
- Like creating a spanning tree in a graph
 - View switches and segments as nodes, ports as edges

Distributed Spanning Tree Algorithm


- Every switch has a unique ID (Ethernet address)
- Goal:
 - Switch with the smallest ID is the root
 - Each segment has one designated switch, responsible for forwarding its packets towards the root
 - Switch closest to root is designated switch
 - If there is a tie, switch with lowest ID wins

Spanning Tree Protocol

- Send message when you think you are the root
- Otherwise, forward messages from best known root
 - Add one to distance before forwarding
 - Don't forward over discarding ports (see next slide)
- Spanning Tree messages contain:
 - ID of switch sending the message
 - ID sender believes to be the root
 - Distance (in hops) from sender to root
- Switches remember best config msg on each port
- In the end, only root is generating messages

Limitations of Switched LAN

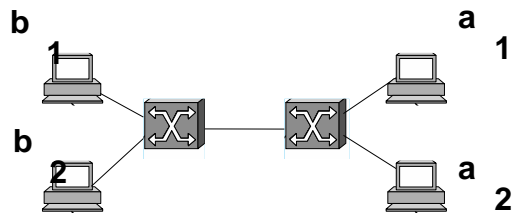
• Scaling

- Spanning tree algorithm doesn't scale
- Broadcast does not scale
- No way to route around congested links, *even if path exists* 

• May violate assumptions

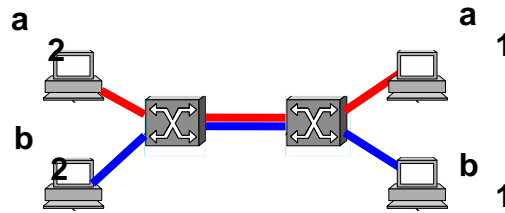
- Could confuse some applications that assume single segment
 - Much more likely to drop packets
 - Makes latency between nodes non-uniform
- Beware of transparency

VLANs



- Company network, A and B departments
 - Broadcast traffic does not scale
 - May not *want* traffic between the two departments
 - Topology has to mirror physical locations
 - What if employees move between offices?

VLANs



- Solution: Virtual LANs
 - Assign switch ports to a VLAN ID (color)
 - Isolate traffic: only same color
 - Trunk links may belong to multiple VLANs
 - Encapsulate packets: add 12-bit VLAN ID
- Easy to change, no need to rewire

Ethernet

Ethernet

- Most widely used high-speed LANs
 - **Ethernet** (10Mbps, 100Mbps, 1Gbps, 10Gbps)
 - Fibre channel
 - High-speed wireless LANs
- Ethernet protocol is developed by IEEE 802.3 standards committee, consisting of
 - Medium Access Control (MAC) Layer (CSMA/CD protocol)
 - Physical Layer
- Earlier MAC schemes
 - ALOHA
 - Slotted ALOHA
 - CSMA

ALOHA

- ALOHA protocol developed for *packet radio networks*, applicable to any shared medium
- Sender
 - When station has frame, it sends
 - Station listens for an amount of time (just more than RTT)
 - If no ACK received, it retransmits the frame after a random time
 - If no ACK after several transmissions, it gives up
 - Frame check sequence used for error detection
- Receiver
 - If frame is OK and address matches receiver, sends ACK
 - Otherwise, ignores this frame and does nothing
- Frame may be **damaged by noise or by another transmission** at the same time (collision)
- ALOHA is simple, but very inefficient
 - Assuming random traffic, the maximum channel utilization is only about 18%

Slotted ALOHA

- To improve efficiency, a modification known as ***slotted ALOHA***, was developed.
- Time organized into **uniform slots, size equal to the frame transmission time**
 - Need a central clock (or other **sync** mechanism)
- Transmission begins only at a slot boundary
 - Consequence: frames either miss or overlap totally
- Maximum channel utilization can be improved to about 37%

CSMA

- Why ALOHA and slotted ALOHA are so inefficient?
 - Stations don't check the channel status.
- A station should "sense" the channel status (free or not).
- CSMA: **Carrier Sense Multiple Access**
 - Stations listen to the channel (**carrier sense**)
 - Stations "**know**" whether the channel is free or not
 - Stations transmit only if the channel is free
 - Collisions become rare
 - Only if two or more stations attempt to transmit at about the same time

CSMA (Cont.)

- In LANs, propagation time is much less than frame transmission time
 - **May not be true for 1Gbps and 10Gbps Ethernet**
- All stations know about a transmission start by "carrier sense"
- Details of CSMA
 - Stations first listen for clear medium (carrier sense)
 - If medium is idle, transmit the frame
 - If two or more stations start at about the same instant, there will be a collision.
 - To account for this, a station waits for an ACK
 - If no ACK after a reasonable time, then retransmit
- What should a station do if the medium is found busy?
 - Three approaches: non-persistent CSMA, 1-persistent CSMA, and p -persistent CSMA

Non-persistent CSMA

- A station wishing to transmit listens to the medium and
 1. If medium is idle, transmit; otherwise, go to step 2
 2. If **medium is busy**, wait an amount of time drawn from a probability distribution and repeat step 1
- The use of random delays reduces probability of collisions
- Capacity wasted because medium remains idle following the end of a transmission, if there are one or more stations waiting to transmit.

1-persistent CSMA

- To **avoid idle channel time, 1-persistent** protocol can be used
- A station wishing to transmit listens to the medium and
 1. If medium is idle, transmit; otherwise, go to step 2
 2. If **medium is busy**, **continue to listen until the channel is sensed idle**; then transmit immediately.
- 1-persistent stations are selfish
 - If two or more stations are waiting to transmit, a collision is guaranteed.

p -persistent CSMA

- p -persistent CSMA attempts to reduce collisions, like nonpersistent, and reduce idle time, like 1-persistent
- Rules:
 1. If the medium is idle, transmit with probability p , and delay one time unit with probability $(1 - p)$
 - The time unit is typically equal to the maximum propagation delay
 2. If the **medium is busy**, continue to listen until the channel is idle and repeat step 1
 3. If transmission is delayed one time unit, repeat step 1
- Question:
 - What is an effective value of p ?

Value of p ?

- Assume n stations are waiting to transmit while a transmission is taking place
- At the end of transmission, expected number of stations attempting to transmit is np
- If $np > 1$, on average there will be a collision
 - Repeated attempts to transmit almost guarantee more collisions
 - Retries compete with new transmissions from other stations
 - Eventually, all stations try to send
 - Continuous collisions; zero throughput
- So $np < 1$ for expected peak of n
- Drawback of p -persistent:
 - If heavy load is expected, p should be small
 - As p is made smaller, stations wait longer to attempt transmission

CSMA/CD: CSMA with Collision Detection

- In CSMA, a collision occupies medium for the duration of a frame transmission
 - not good for long frames.
- **Collision Detection**
 - stations continue to listen while transmitting. If collision detected, stop transmission immediately.
- **CSMA/CD**
 1. If the medium is idle, transmit; otherwise, go to step 2
 2. If the medium is busy, continue to listen until the channel is idle, then transmit immediately
 3. If a collision is detected during transmission, transmit *jamming signal* and cease transmission
 4. After transmitting the jamming signal, wait random amount of time (called ***backoff***), then attempt to transmit again (go to step 1)

Collision Detection

- On baseband bus
 - Produces higher voltage signal
 - Detected if signal strength greater than that transmitted by a single station
 - Signal attenuated over distance: max 500m or 200m.
- Start topology with twisted pair
 - Activity on more than one port
 - Special collision signal sent on all ports

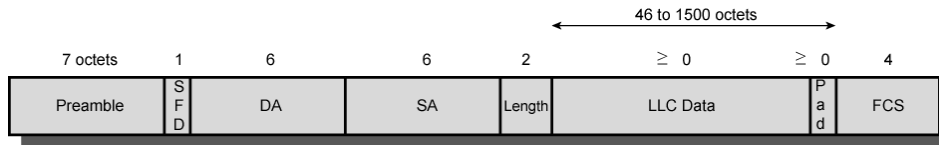
Which Persistence Algorithm?

- IEEE 802.3 uses 1-persistent
- Both non-persistent and p -persistent have performance problems
- 1-persistent seems to be more unstable than p -persistent, due to the greed of the stations
- But wasted time due to collisions is short (if frames are long relative to propagation delay)
- With random backoff, stations involved in a collision are unlikely to collide on next tries
 - To ensure backoff maintains stability, IEEE 802.3 and Ethernet use binary exponential backoff

Binary Exponential Backoff

- Rules of binary exponential backoff
 - A station attempts to transmit repeatedly in the face of repeated collisions
 - For the first 10 attempts, the mean value of the random delay is doubled
 - The mean value then remains the same for 6 additional attempts
 - After 16 unsuccessful attempts, the station gives up and reports an error
- With congestion, stations backoff longer to reduce the probability of collision
 - At low load, 1-persistence guarantees that a station can seize channel as soon as the channel goes idle
 - At high loads, it is stable due to backoff
- Problem: Backoff algorithm gives last-in, first-out effect
 - Stations with no or few collisions will have a chance to transmit earlier

IEEE 802.3 Frame Format



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

Preamble: 7 octets of 10101010

SFD: 10101011

Length: the maximum frame size is 1518 octets, excluding the preamble and SFD.

Pad: octets added to ensure that the frame is long enough for collision detection

FCS: 32-bit CRC, based on all fields except preamble, SFD, and FCS

10Mbps Specification (Ethernet)

- IEEE 802.3 defined a number of physical configurations.

	10BASE5	10BASE2	10BASE-T	10BASE-FP
Transmission medium	Coaxial cable (50 ohm)	Coaxial cable (50 ohm)	Unshielded twisted pair	850-nm optical fiber pair
Signaling technique	Baseband (Manchester)	Baseband (Manchester)	Baseband (Manchester)	Manchester/on-off
Topology	Bus	Bus	Star	Star
Maximum segment length (m)	500	185	100	500
Nodes per segment	100	30	—	33
Cable diameter (mm)	10	5	0.4 to 0.6	62.5/125 μ m

100Mbps Fast Ethernet

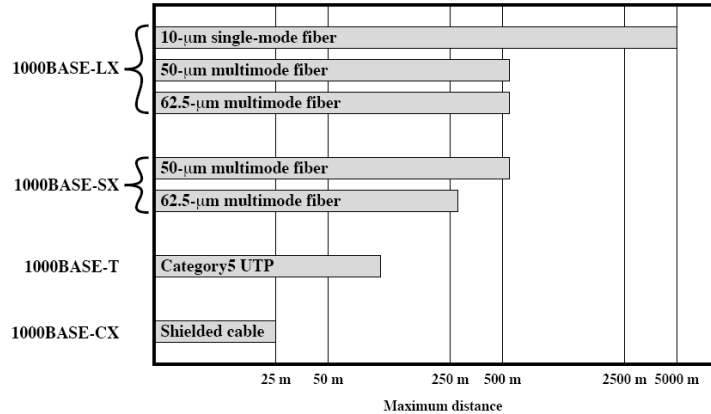
- Use IEEE 802.3 MAC protocol and frame format
- 100BASE-X refers to a set of options that use two physical links: one for transmission and one for reception
 - 100BASE-TX for twisted pair
 - 100BASE-FX for optical fiber
- 100BASE-T4 can use Category 3 UTP cable
 - Uses four twisted-pair lines between nodes
- Star topology

	100BASE-TX		100BASE-FX	100BASE-T4
Transmission medium	2 pair, STP	2 pair, Category 5 UTP	2 optical fibers	4 pair, Category 3, 4, or 5 UTP
Signaling technique	MLT-3	MLT-3	4B5B, NRZI	8B6T, NRZ
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m

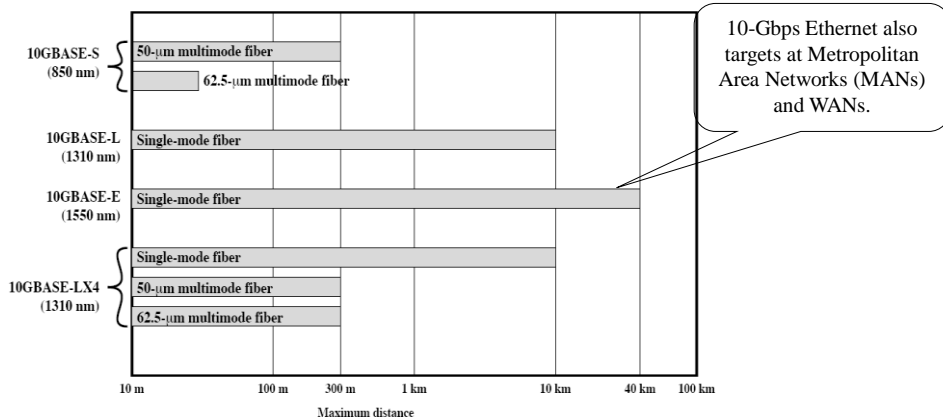
Gigabit Ethernet

- The Gigabit Ethernet uses the same CSMA/CD frame format and MAC protocol as used in the 10Mbps and 100Mbps version of IEEE 802.3.
- For shared-medium hub operation, there are two enhancements to the basic CSMA/CD
 - Carrier extension
 - Appends a set of special symbols to the end of short MAC frames so that the resulting block is at least 4096 bit-times in duration (512 bit-times for 100Mbps)
 - Frame bursting
 - Allows for multiple short frames to be transmitted consecutively (up to a limit) without giving up control for CSMA/CD between frames. It avoids the overhead of carrier extension when a single station has a number of small frames ready to send.

Gigabit Ethernet Configuration

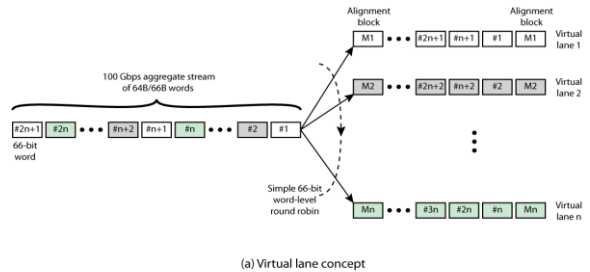


10-Gbps Ethernet Configuration



40 & 100Gbps Ethernet

- Same CSMA/CD protocol by IEEE 802.3ba.
- Applications like, Internet exchanges, VoD service providers, data centers
- Two enhancements to Gigabit Ethernet
 - Multilane distribution
 - Parallel channels between nodes, like separate cables or wavelengths on fiber
 - Specified as Physical Medium Attachment (PMA) sublayer of PHY
 - Virtual lanes
 - Data stream in words split into virtual streams
 - Alignment blocks identify lanes and aggregate
 - Virtual lanes are mapped to physical lanes for distribution



Media Options for 40-Gbps and 100-Gbps Ethernet

	40 Gbps	100 Gbps
1m backplane	40GBASE-KR4	
10 m copper	40GBASE-CR4	1000GBASE-CR10
100 m multimode fiber	40GBASE-SR4	1000GBASE-SR10
10 km single mode fiber	40GBASE-LR4	1000GBASE-LR4
40 km single mode fiber		1000GBASE-ER4

Naming nomenclature:

Copper: K = backplane; C = cable assembly

Optical: S = short reach (100m); L - long reach (10 km); E = extended long reach (40 km)

Coding scheme: R = 64B/66B block coding

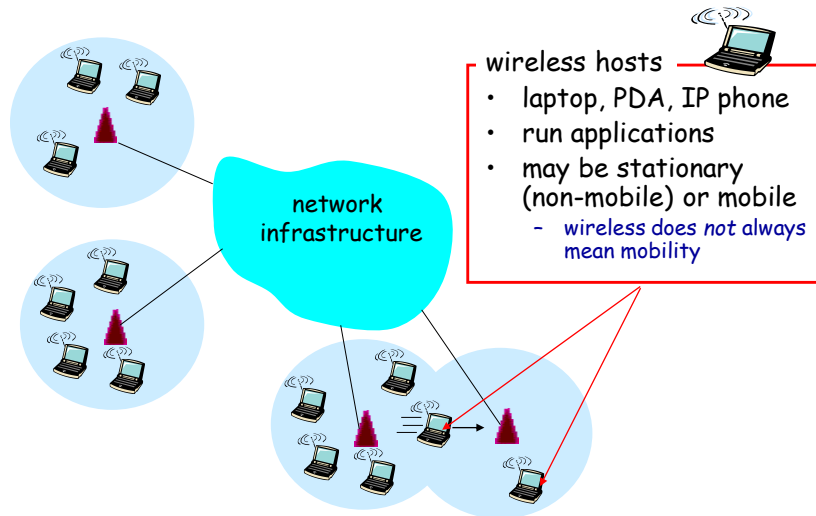
Final number: number of lanes (copper wires or fiber wavelengths)

Wireless LAN

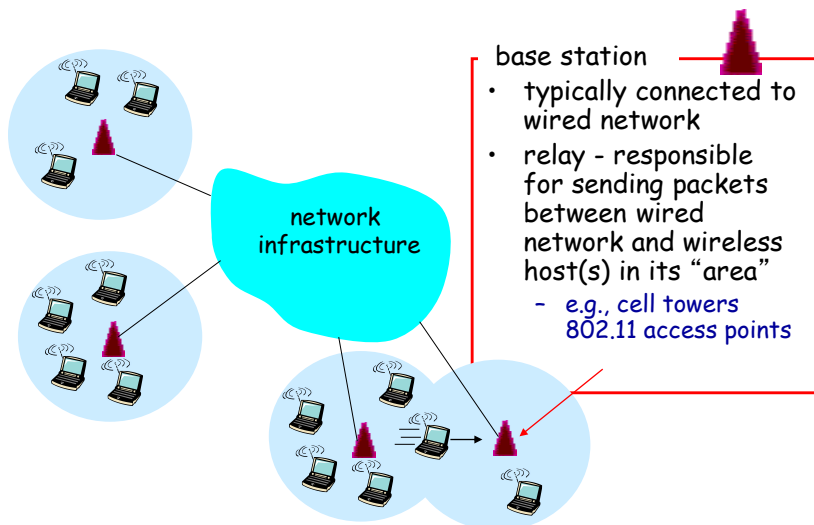
Wireless LANs

- Wireless LAN makes use of a wireless transmission medium.
- Wireless LAN applications
 - LAN Extension
 - Cross-building Interconnection
 - Nomadic access
 - Ad Hoc Networking
 - peer-to-peer network (without centralized server) set up temporarily

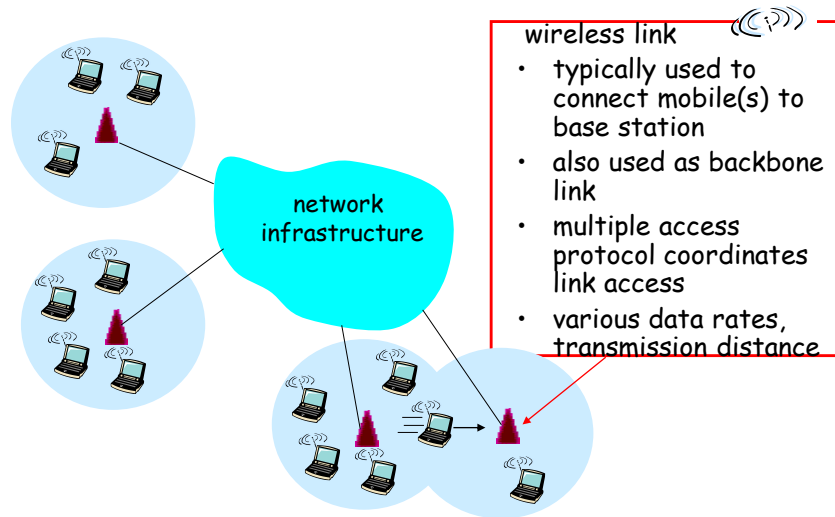
Elements of a Wireless Network



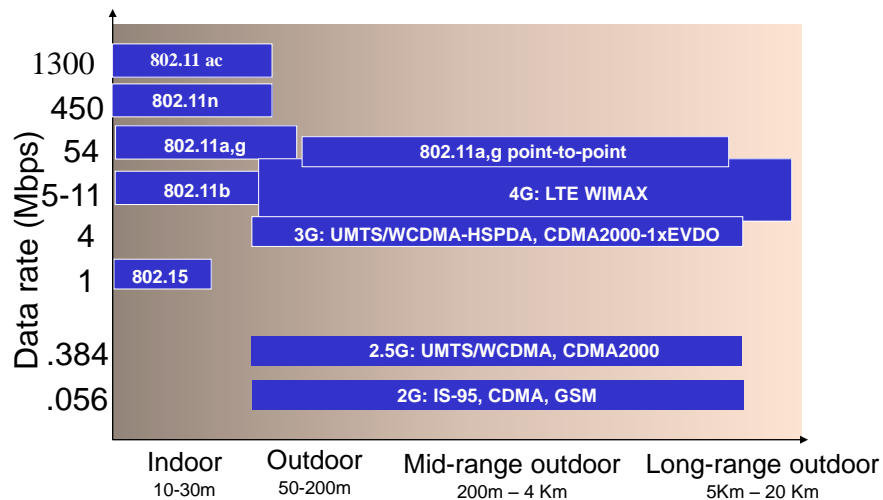
Elements of a Wireless Network



Elements of a Wireless Network



Characteristics of selected wireless links



Wireless Link Characteristics (1)

Differences from wired link

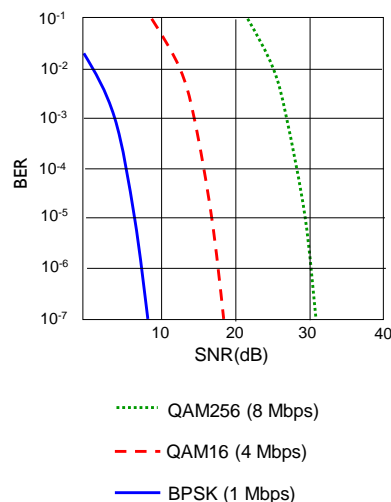


- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources:** standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **multipath propagation:** radio signal reflects off objects ground, arriving at destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”

Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
 - larger SNR – easier to extract signal from noise (a “good thing”)
- **SNR versus BER tradeoffs**
 - *given physical layer:* increase power -> increase SNR->decrease BER
 - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
 - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



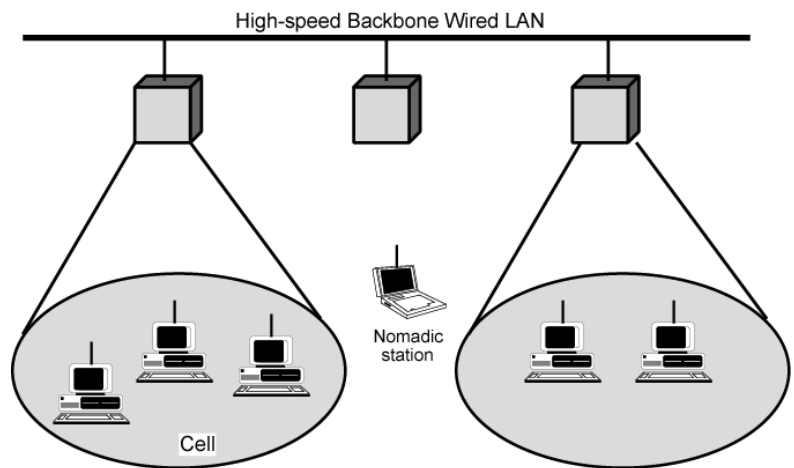
Wireless Networks: A Taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: <i>mesh net</i>
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Infrastructure Wireless LAN

infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

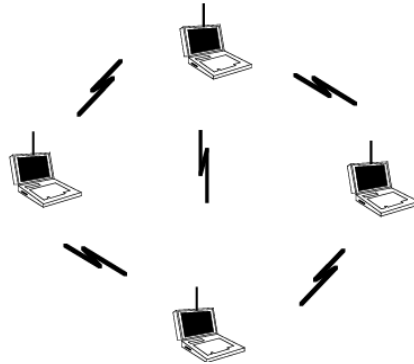


(a) Infrastructure Wireless LAN

Ad Hoc WLAN Configuration

Ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves



11

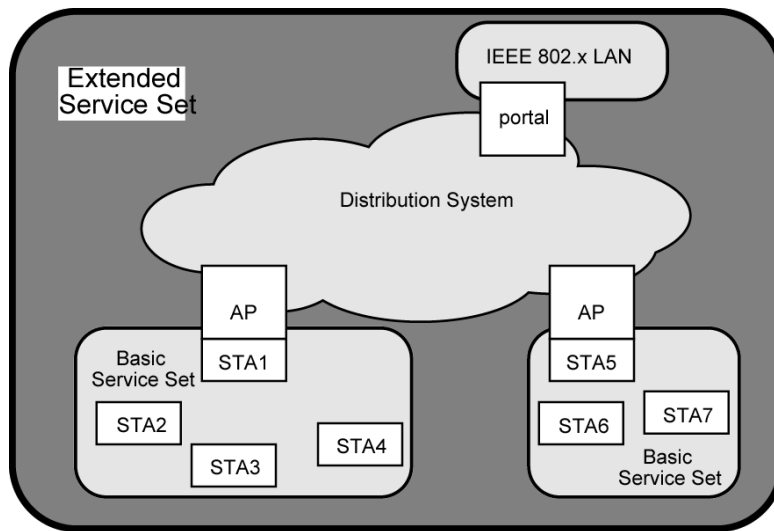
Wireless LAN Technology

- Infrared (IR) LANs
 - An individual cell of an IR LAN is limited to a single room, because infrared light does not penetrate opaque walls
- Spread spectrum LANs
 - The most popular type
 - In United States, three microwave bands for unlicensed use
 - 915-MHz band (902-928 MHz) ---- 26 MHz of bandwidth
 - 2.4-GHz band (2.4-2.4835 GHz) ---- 83.5 MHz of bandwidth
 - 5.8-GHz band (5.725-5.825 GHz) ---- 100 MHz of bandwidth

IEEE 802.11

- Specifies MAC and physical layer protocols for wireless LANs
- Wi-Fi Alliance (Wi-Fi: Wireless Fidelity)
 - An industry consortium to certify interoperability for 802.11 products
- IEEE 802.11 Architecture
 - The smallest building block is **Basic Service Set (BSS)**
 - A number of stations executing the same MAC protocol
 - Shared wireless medium
 - BSS corresponds to a cell
 - A BSS may be isolated, or may connect to a **Backbone Distribution System (DS)** through an **Access Point (AP)**
 - AP functions as a bridge and a relay point
 - AP could be a station which has the logic to provide DS services
 - AP corresponds to a Control Module (CM)
 - DS can be a switch, wired network, or wireless network
 - An **Extended Service Set (ESS)** consists of two or more BSSs interconnected by a DS.

IEEE 802.11 Architecture

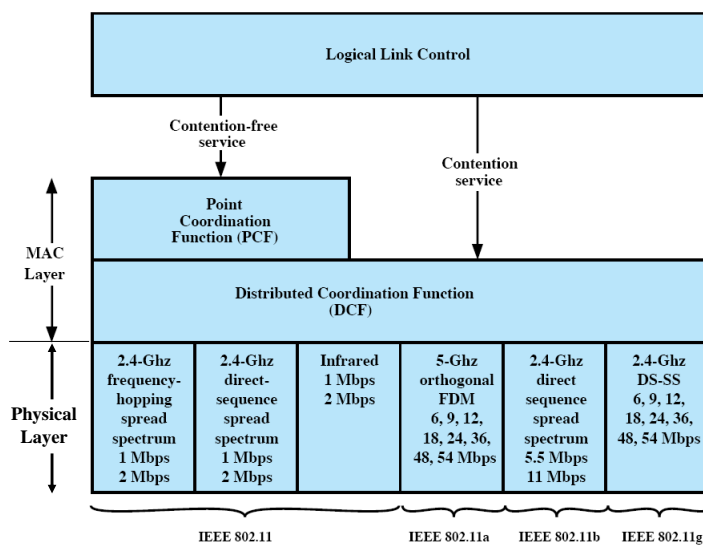


STA = station
AP = access point

IEEE 802.11 Wireless LAN

- **802.11b**
 - 2.4-5 GHz unlicensed radio spectrum
 - up to 11 Mbps
 - direct sequence spread spectrum (DSSS) in physical layer
 - all hosts use same chipping code
 - widely deployed, using base stations
- **802.11a**
 - 5-6 GHz range
 - up to 54 Mbps
- **802.11g**
 - 2.4-5 GHz range
 - up to 54 Mbps
- **802.11n**
 - MIMO, 20/40MHz channels in 2.4 GHz
 - up to 600 Mbps
- **802.11ac**
 - wider RF band per station (80/160 MHz), more MIMO, multi-user MIMO, 5 GHz
 - at least 1 Gbps total, 500 Mbps per link
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

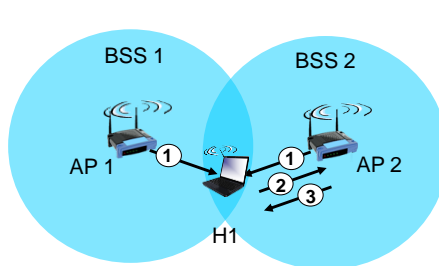
IEEE 802.11 Protocol Architecture



802.11: Channels, Association

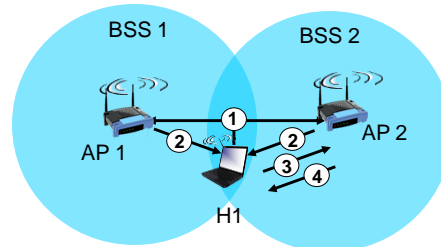
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication
 - will typically run DHCP to get IP address in AP's subnet

802.11: Passive/Active scanning



passive scanning:

- (1) beacon frames sent from APs
- (2) association Request frame sent: H1 to selected AP
- (3) association Response frame sent from selected AP to H1

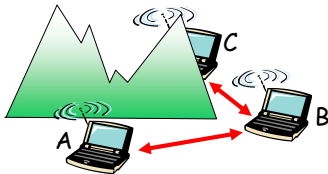


active scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probe Response frames sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent from selected AP to H1

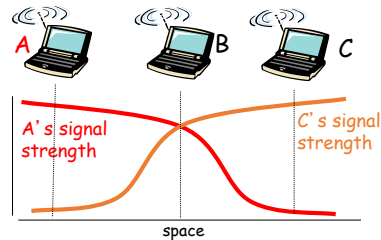
Wireless Network Characteristics (again!)

Multiple wireless senders and receivers create additional problems



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other
means A, C unaware of their
interference at B

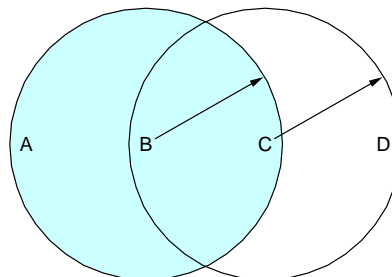


Signal fading:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other
interfering at B

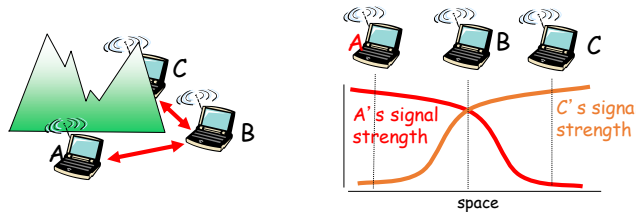
Hidden and Exposed Terminal Problems

- Wireless networks: *hidden* and *exposed* nodes
 - A → B and C → B: A can't hear C's transmission
 - C hidden from A, can cause collision (at B)!
 - B → A and C → D: won't interfere with each other, despite B can hear C's transmission
 - C exposed to B, unnecessary backoff by B!



IEEE 802.11: Multiple Access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- 802.11: **no collision detection!**
 - difficult to receive (sense collisions) when transmitting due to weak received signals (fading);
 - often need to switch between transmitting vs. receiving mode
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: **avoid collisions**: CSMA/C(ollision)A(voidance)



Collision Avoidance Mechanisms

- Problem:
 - two nodes, hidden from each other, transmit complete frames to base station
 - wasted bandwidth for long duration !
- Solution:
 - small reservation packets
 - nodes track reservation interval with internal “network allocation vector” (NAV)

Avoiding Collisions (cont' d)

idea: allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
 - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- RTS heard by all nodes
 - sender transmits data frame
 - other stations defer transmissions

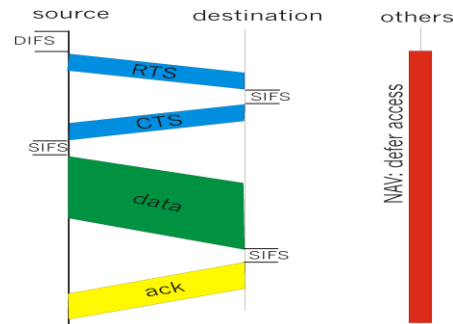
Avoid (large) data frame collisions
using small reservation packets!

Collision Avoidance: Some Details

- Sender transmits **RequestToSend** (RTS) frame
- Receiver replies with **clearToSend** (CTS) frame
- Neighbors...
 - see CTS: keep quiet
 - see RTS but not CTS: ok to transmit
- Receiver sends ACK when has frame
 - neighbors silent until see ACK
- Collisions
 - no collisions detection
 - known when don't receive CTS
 - exponential backoff

Collision Avoidance: RTS-CTS Exchange

- sender transmits short RTS (request to send) packet: indicates duration of transmission
- receiver replies with short CTS (clear to send) packet
 - notifying (possibly hidden) nodes
- hidden nodes will not transmit for specified duration: NAV



Medium Access Control

- Two sublayers
- Lower sublayer is **distributed coordination function** (DCF)
 - Uses a contention algorithm to provide access to all traffic
- Higher sublayer is **point coordination function** (PCF)
 - Uses a centralized algorithm
 - Contention free
 - Implemented on top of DCF
- Remark: PCF has not been popularly implemented in today's 802.11 products. DCF is widely used.

Distributed Coordination Function: CSMA/CA

- DCF sublayer uses CSMA/CA protocol, where CA refers to as **Collision Avoidance**
 - Sense the medium. If medium is idle, wait for a time equals to a delay called **Interframe Space** (IFS). If so, the station may transmit.
 - If the medium is busy, defer transmission till the end of ongoing transmission.
 - After the transmission, the station delays another IFS. If medium remains idle, then **back off a random amount of time** and again sense. If the medium is still idle, the station may transmit.
 - During the backoff time, if the medium becomes busy, the backoff timer is halted and resumes when the medium becomes idle.
 - If the transmission is unsuccessful (no ACK), assume collision occurred.
- To ensure that backoff maintains stability, **binary exponential backoff** is used.

IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

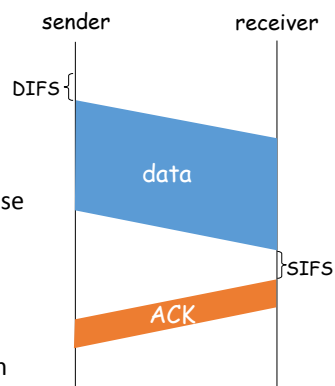
2 if sense channel busy then
start random backoff timer
timer counts down while channel idle
transmit when timer expires

if no ACK (e.g., due to collision or bit error), increase
random backoff interval, repeat 2

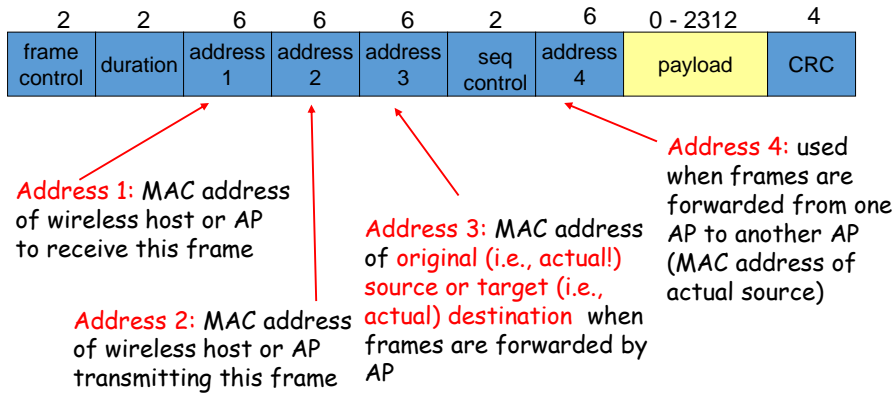
802.11 receiver

- if frame received OK

return ACK after **SIFS** (ACK needed due to hidden
terminal problem)



802.11 Frame: Addressing



802.11 Frame (contd.)

