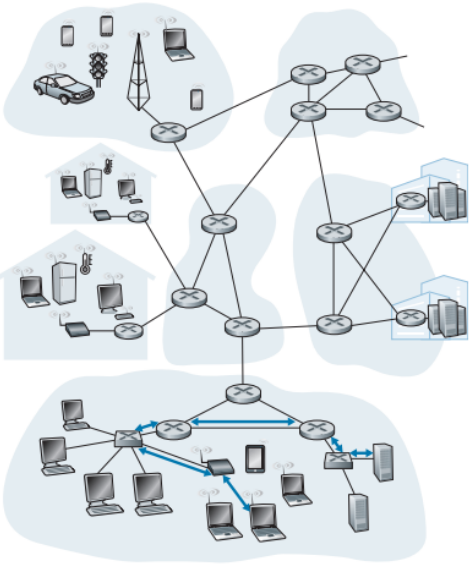
# Unit 4 - Link Layer, LANs and WLANs

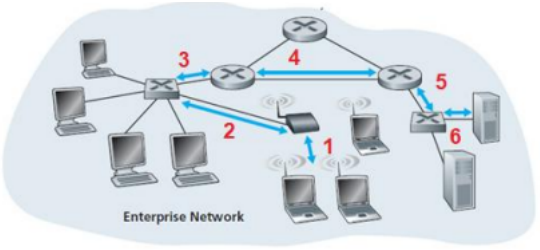
- ▼ Link Layer
  - The Link Layer is responsible for moving each datagram across each individual link in the path from source to destination
  - The Link Layer handles node-to-node delivery
  - ▼ Basic Link Layer Terminology
    - ▼ Node
      - Any device that runs a Link Layer protocol
      - Ex: End hosts, Routers, Switches, Wi-Fi Access Points
    - ▼ Link
      - A communication channel that connects adjacent nodes
      - Ex: Ethernet cable, Fiber link, Wi-Fi wireless medium, Co-axial cable
    - A packet from source to destination traverses multiple links, each using possibly different technologies



Wireless Host → Server (Sending a datagram from a Wi-Fi host a server)

▼ The transportation analogy (Link Layer Hopping)

- Assume a tourist (datagram) uses a travel agent (routing protocol) in some transportation mode (link-layer protocol)
- They travel in a cab (pes to blr airport), flight (blr to delhi), bus (delhi to jammu)
- Each segment uses different modes, provided by different companies, but each segment handles local, direct movement between 2 adjacent points
- Similarly, every link uses its own technology (Wi-Fi/Ethernet/Fiber), Routing handles end-to-end while Link Layer handles per-hop




▼ Services provided by Link Layer

- Although the Link Layer's basic service is to move from across a link, different link-layer protocols offer different capabilities

▼ Framing

- Every link-layer protocol encapsulates the datagram into a frame before transmission over the link,
- The frame is of the format:

| Header | Data (IP packet) | Trailer |
|---|---|---|

- Header field include addresses, type fields etc.,
- Ethernet, Wi-Fi, PPP all have different frame formats which are explained later

▼ Link access

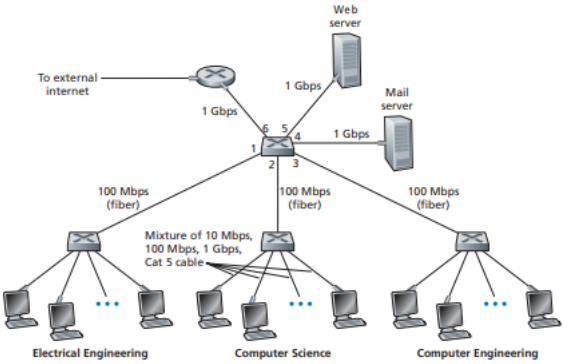
- It determines who gets to transmit next on the link
- a MAC protocol specifies the rules by which a frame is transmitted onto the link
- Two cases:

        - Point-to-Point : Only one sender & receiver, MAC is simple and the sender can send a frame whenever the link is idle
        - Multiple Access : Many nodes share one broadcast channel, MAC protocol needed to prevent collisions
    - ▼ Reliable delivery
        - Ensures datagram crosses the link without errors
        - Uses ACKs + retransmissions & Similar to TCP, but only for the link
        - It is used in wireless links (high bit error rate) and not in wired ethernet or fiber because the overhead for them isn't worth it
          Basically ethernet doesn't provide reliable delivery whereas Wi-Fi does
    - ▼ Error detection and Correction
        - Links may introduce bit errors due to noise, interference and attenuation
        - Link Layer typically provides Error Detection and Error Correction
        - The mechanism is that the sensor adds error-detection bits and receiver checks for integrity
          If error is detected, then that frame is discarded and possibly retransmitted
- ▼ Link Layer implementation
    - It is implemented on both hardware and software
    - ▼ Hardware (Mostly)
        - The network adapter or NIC (Network Interface Controller) handles most link-layer logic like framing, addressing, MAC protocol, Error detection, Flow control, Sending/Receiving frames
        - Ex: Intel Ethernet NICs, Atheros Wi-Fi NICs
        - NIC can be on motherboard chipset, on separate PCIe card or integrated into SoC
    - ▼ Software (Partially)
        - Link Layer software in OS provides interface to NIC driver, Assembles Link Layer addressing, Passes datagrams down to NIC, Handles interrupts and errors, Passes received datagrams up to network layer
    - Link Layer = Hardware + Software Collaboration
- ▼ Summary and Tips
    - Link Layer = Hop-by-Hop ; Network Layer = End-to-End
    - NIC is the hardware implementation of link layer
    - MAC protocols solve the "Who can transmit" problem
    - Wi-Fi uses link-layer reliability whereas Ethernet doesn't
    - Framing is the encapsulation at Link Layer

| Topic | Meaning |
|---|---|
| Node | Any device running link-layer protocol |
| Link | Physical channel between adjacent nodes |
| Frame | Link Layer encapsulation of IP datagram |
| MAC | Control access to shared medium |
| Error Detection | CRC checks in hardware |
| Reliable Delivery | Used on wireless, not on wired |
| NIC (Hardware) | Hardware implementing Link Layer functions |
| Software | Driver + OS interacting with NIC |

- ▼ Switched LANs
    - LAN (Local Area Network) is a popular access network consisting of hosts and switches connected by a common physical medium (channel)
    - Switched LANs used Link Layer switches (NOT routers) to forward the frames (NOT IP packets)

- Switches perform Link Layer forwarding using MAC addresses (NOT IP addresses) and don't use routing protocols like OSPF and RIP
- They connect multiple departments, servers, hosts and routers in large LANs like in the image below

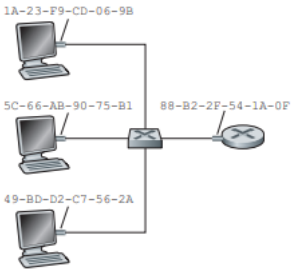



▼ Link Layer Addressing and ARP

- To forward a frame through a LAN, switches uses MAC address
- We used both MAC and IP addresses because they give network-layer and link-layer addresses respectively making both of them indispensable

▼ MAC address

- MAC (Media Access Control) address or physical address serve the purpose of providing a way to uniquely identify the interfaces of sender and receiver




- So, we can say that MAC address belong to network interface (NIC) and not the host
- If a host has multiple NICs, It has multiple MAC & IP Addresses
- Switches don't have MAC address on their ports (see the above image) because they forward frames transparently
- The format is a 48 bits (6 bytes) representation in hexadecimal. Ex: `1A-23-F9-CD-06-9B`. This gives 2^48 or 281 trillion possibilities
- No 2 NICs can have the same MAC address, and IEEE controls MAC allocation. Companies buy a block of addresses (first 24 bits fixed → OUI)
- MAC address can never change, but IP address can change when you move networks

▼ Frame delivery

- When sending a frame:
  - Sender inserts destination MAC address in frame header
  - Frame is broadcast or switched inside LAN
  - Every NIC checks if destination MAC matches its own
  - If match, frame is accepted, Else dropped silently
- MAC Broadcast address: `FF-FF-FF-FF-FF-FF` is used to send a frame to all adapters on LAN

▼ ARP - Address Resolution Protocol

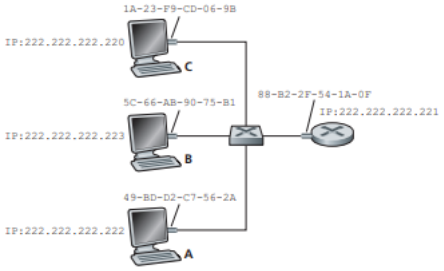
- ARP maps IP address to MAC address
- It is used only within the same subnet
- ARP vs DNS

| | Function | Scope |
|---|---|---|
| ARP | IP → MAC | Local subnet only |
| DNS | Hostname → IP | Internet-wide |

- Every node keeps an ARP table with IP address, MAC address, TTL (Time To Live) Entries expire usually with a lifetime of 20 minutes

▼ Example

- Let's consider the following network and assume some cases




▼ When sender's ARP table contains the entry

- In the above image, Host `222.222.222.220` wants MAC of `222.222.222.222`
- If ARP entry already exists, Sender uses the MAC directly

▼ When ARP table doesn't contain destination

- Sender broadcasts ARP query:
  - Construct ARP request packet
  - Insert broadcast MAC address `FF-FF-FF-FF-FF-FF`
  - Every node receives request
  - Only the node with matching IP replies
- Process:
  - Sender broadcasts ARP Request: "Who has IP X? Tell me your MAC"
  - All the LAN nodes receive it
  - Only the destination replies with ARP reply (unicast MAC)
  - Sender updates ARP table
  - Sender transmits original IP datagram inside a link-layer frame
- Why ARP request is broadcast and ARP reply is Unicast
  - Request must reach all devices (broadcast)
  - Reply should go only to original sender (unicast)

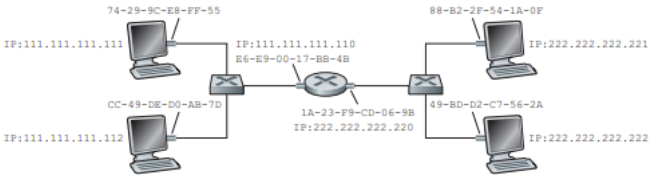
▼ ARP is Plug-and-Play

- No configuration needed
- ARP tables fill themselves automatically
- Entries expire automatically
- No human intervention required

▼ Is ARP link-layer or network-layer?

- Encapsulated in link-layer frame → link-layer behavior
- Contains IP address → network-layer behavior
- So it is best described as between link layer and network layer (straddles both layers)

▼ Sending to another subnet




- Host `111.111.111.111` (Subnet 1) sends to `222.222.222.222` (Subnet 2)
- The host can't directly ARP for the MAC for final destination because ARP works only within same subnet

▼ The step-by-step procedure

1. Check destination subnet
   Destination IP: `222.222.222.222`
   Sender's subnet: `111.111.111/24` (Destination is not in same subnet)
2. Sender must send to its default gateway (router interface)
   Router interface on subnet 1 has IP : `111.111.111.110` and MAC: `E6-E9-00-17-BB-4B`
3. Sender ARPs for router's MAC address (not for destination host)
4. Sender encapsulates the IP datagram
   Frame destination MAC = router's MAC
   Frame source MAC = sender's MAC
   IP destination = `222.222.222.222` (unchanged)
5. Router receives frame
   It extracts the datagram and checks forwarding table and decides to forward via interface on Subnet 2
6. Router ARPs on Subnet 2 for final host and gets MAC : `49-BD-D2-C7-56-2A`
7. Router sends Ethernet frame to final host
   Thus, communication uses 2 ARP resolutions:
   sender → router
   router → destination host

- Note that MAC changes at each hop, IP doesn't because
  MAC = link-layer hop-by-hop
  IP = network-layer end-to-end

▼ Ethernet

- Ethernet is the dominant wired LAN technology
- It is successful because it is simple, cheap, evolved continuously (10 Mbps → 10 Gbps → 40 Gbps), backward compatible, and commodity hardware
- It has evolved from bus topology → Hub-based start topology → Switch-based star topology
- Ethernet Frame structure
  Preamble - Synchronizes sender & receiver clock
  Destination MAC - NIC checks this: if not matching, discards
  Source MAC - origin
  Type - Identifies payload protocol (IP, ARP, IPv6, etc.,)
  Data - IP datagram
  CRC - Error detection (Cyclic Redundancy Check)

| Preamble | Destination Address (MAC) | Source Address (MAC) | Type | Data | CRC |
|---|---|---|---|---|---|
| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 46-1500 bytes | 4 bytes |

▼ Ethernet Services

- Connectionless → No handshake before sending
- Unreliable → No ACK/NACK, Frame dropped silently if CRC fails and reliability handled by upper layers (TCP) if needed

▼ Ethernet Technologia

- BASE = baseband (ethernet only) | T = Twisted pair | FX/LX = Fiber optic variants
- **10BASE-T** → 10 Mbps (Twisted pair)
- **100BASE-TX** → Fast Ethernet (100 Mbps)
- **1000BASE-T** → Gigabit Ethernet
- **10GBASE-T** → 10 Gbps Ethernet
- **40GBASE-T** → 40 Gbps Ethernet

▼ Link Layer Switches

▼ Switch

- Switch is a store and forward device that forwards frames based on MAC address
- Switch is transparent : Hosts send frames to each other, not to switch. It only intercepts & forwards them
- Switch Output buffers : Used to store frames if incoming rate > outgoing capacity (similar to router queueing)

▼ Core Switch Functions

- Filtering : Decide whether to drop or forward frame
- Forwarding : Decide which interface(s) the frame should go to

Both are done using switch table (MAC table) : MAC Address → Interface → Timestamp

▼ Forwarding Logic

- Frame arrives with destination MAC D on interface x:

1. Case : No entry for D
   Broadcast to all ports except x
2. Case : Destination D is on interface x
   Drop (frame already on correct segment)
3. Case : Destination D is on interface y ≠ x
   Forward only to interface y

- Switches eliminate unnecessary broadcasting once table is populated

▼ Self-Learning ( How switch tables are built)

- Switches are plug-and-play
- Learning algorithm
  - Table initially empty
  - For each received frame, Read source MAC, map it to incoming interface, store with timestamp
  - If no frames from a MAC for “aging time” (300s) → delete entry

▼ Properties & Advantages of Switches

- Elimination of collisions
  - Each link is isolated
  - Full-duplex
  - No CSMA/CD required (more about this in wireless networks)

- Heterogeneous link support
  - Switch can mix Copper (UTP), Fiber, Different speeds (10 Mbps → 40 Gbps)
- Better Management
  - Switches can Detect jabbering NICs
  - Collect traffic statistics
  - Isolate faults (cable cuts etc.)
- Higher aggregate throughput
  - Each port = independent collision domain

▼ Security: Switch Poisoning (MAC Flooding)

- Attacker sends numerous fake source MACs → switch table overflows → switch reverts to broadcasting → attacker sniffs traffic.
- Still safer than hubs or wireless

▼ Switches vs Routers

| Feature | Switch (Layer 2) | Router (Layer 3) |
|---|---|---|
| Uses | MAC addressing | IP addressing |
| Path selection | No routing | Routing algorithms |
| Topology | Must use **spanning tree** (no loops) | Can use **arbitrary topology** |
| Collision domains | Eliminates collisions | N/A |
| Traffic isolation | Limited | Strong isolation |
| Plug-and-play | Yes | No |
| Broadcast storms | Vulnerable | Immune |

▼ Question

- Let's consider the operation of a learning switch in the context of a network in which 6 nodes labeled A through F are star connected into an Ethernet switch.
  Suppose that (i) B sends a frame to E, (ii) E replies with a frame to B, (iii) A sends a frame to B, (iv) B replies with a frame to A.
  The switch table is initially empty. Show the state of the switch table before and after each of these events. For each of these events, identify the link(s) on which the transmitted frame will be forwarded, and briefly justify your answers

| **Action** | **Switch Table State** | **Link(s) packet is forwarded to** | **Explanation** |
|---|---|---|---|
| B sends a frame to E | Switch learns interface corresponding to MAC address of B | A, C, D, E, and F | Since switch table is empty, so switch does not know the interface corresponding to MAC address of E |
| E replies with a frame to B | Switch learns interface corresponding to MAC address of E | B | Since switch already knows interface corresponding to MAC address of B |
| A sends a frame to B | Switch learns the interface corresponding to MAC address of A | B | Since switch already knows the interface corresponding to MAC address of B |
| B replies with a frame to A | Switch table state remains the same as before | A | Since switch already knows the interface corresponding to MAC address of A |

▼ Virtual Local Area Networks (VLAN)

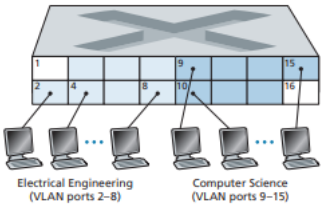
- Real networks have problems like broadcast traffic spreading everywhere, Hard to manage users moving across departments, Wastes switch ports
- VLAN fixes these problems by dividing a physical switch into multiple logical LANs
- Each VLAN has its own broadcast domain and provides traffic isolation
- For example, VLAN 10 → ECE Dept., VLAN 20 → CSE Dept., Hosts in VLAN 10 behave as if they share a switch exclusively

▼ Benefits of VLAN

- Traffic isolation - ARP, DHCP, Broadcasts stay inside VLAN
- Efficient use of hardware - One switch can serve many departments
- User mobility - If employee moves, only VLAN software configuration changes
- Security - Prevents sniffing across departments

▼ Port-Based VLANs

- Network admin assigns switch ports to VLANs
- Switch ensures only ports in same VLAN can communicate
- For example,
  Ports 2-8 → VLAN ECE
  Ports 9-15 → VLAN CSE

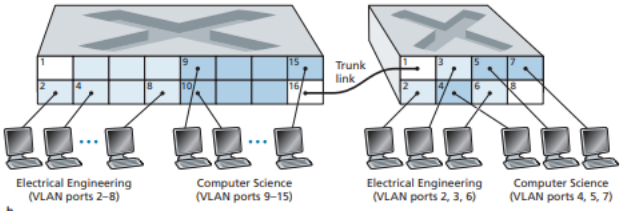



▼ Inter VLAN communication

- VLANs are isolated → to talk between VLANs, traffic must go through a router (Layer 3 device)
- But, Modern switches include Layer 3 functionality nowadays (router + switch combo)

▼ VLAN Trunking (IEEE 802.1Q)

- The problem in hand is to connect two switches with N VLANs
- The naive method to solve this is using N cables (one per VLAN)
- Better solution is Trunk link




- Trunk port characteristics
  - Carries frames belonging to all VLANs
  - Uses 802.1Q tagging
- 802.1Q Frame format
  - Tag protocol identifier (TPID) field has a fixed hexadecimal value of `0x8100`
  - 2-byte Tag Control Information field contains a 12-bit VLAN identifier field

- 3-bit priority field similar in intent to IP datagram TOS field

| Preamble | Destination Address (MAC) | Source Address (MAC) | Tag Protocol Identifier | Tag Control Information | Type | Data |
|---|---|---|---|---|---|---|
| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 2 bytes | 2 bytes | 46-1500 b |

▼ Other types of VLANs

- MAC-based VLANs: Based on MAC address instead of port
- Protocol-based VLANs: Based on IPv4/IPv6/Appletalk
- VLANs across routers: VLAN can span across geographically separated LANs

▼ Summary

| Topic | Key Points |
|---|---|
| Link-Layer Addressing | MAC addresses, flat structure, broadcast MAC |
| ARP | Resolves IP → MAC within subnet, uses broadcast request + unicast reply |
| Ethernet | Frame format, unreliable, connectionless, MTU = 1500 bytes |
| Ethernet Evolution | Bus → Hub → Switch, CSMA/CD now obsolete |
| Switches | Forward/filter using MAC table, self-learning, plug-and-play |
| Switch Advantages | No collisions, full-duplex, heterogeneous links |
| Switch vs Router | L2 vs L3, spanning tree vs routing, traffic isolation |
| VLANs | Logical LANs, traffic isolation, 802.1Q tagging, trunking |

▼ Link Virtualization

- Till now we have seen the meaning of link as “Physical wire between two hosts” to “A shared medium (Ethernet hub)” to “A switched LAN that looks like a simple link to hosts even though inside it is a complex network of switches”
- The key idea is that host always see a simple link-layer connection even if internally the infrastructure is really huge and complex
  Like when you use a dial-up modem, it uses the entire telephone network but the internet only sees it as just “one link” or like when a VLAN uses many switches but looks like one LAN link to host
- Similarly MPLS (Multi-Protocol Label Switching) acts a virtual link layer, even though it is a full network underneath, this is called virtualization of links

▼ MPLS

- Stands for Multi-Protocol Label Switching
- It is a mechanism that allows routers to forward packets using short fixed length labels instead of long IP addresses
- It was originally invented to speed up IP router forwarding because it requires longest prefix matching which was slow. MPLS solves this using simple label lookups
- Now it is mainly used for traffic engineering, VPNs, Fast failover. Not for speed
- So it is the basically the hybrid of virtual-circuit networks (labels + predetermined paths) and IP networks (addressing + routing)

▼ MPLS Header

- When an MPLS-capable router sends a frame to another MPLS router, it inserts an MPLS header between Layer 2 and IP

| PPP or Ethernet Header | MPLS Header | IP Header | Remainder of Link-Layer Frame |
|---|---|---|---|

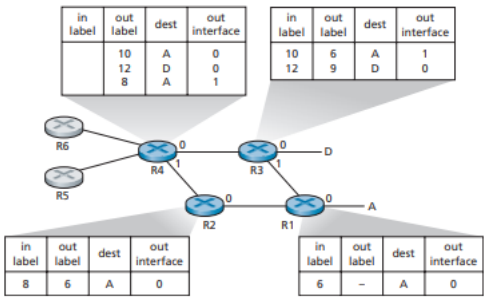
- MPLS Header is further divider

| Label | Exp | S | TTL |
|---|---|---|---|
| 20 bits | 3 bits | 1 bit | 8 bits |
| The MPLS label used for forwarding | Experimental – often used for QoS | Bottom-of-stack (1 = Last MPLS header) | Limits looping, just like IP TTL |

- MPLS headers are only understood by MPLS-capable routers

▼ MPLS Forwarding

- Consider 4 MPLS capable routers (R1, R2, R3, R4)




- Each MPLS router maintains a Label Forwarding Information Base (LFIB). It maps
  Incoming Label → Outgoing Label + Outgoing Interface
- R1 says "To reach A, use label 6"
  R2 says "To reach A, use label 8"
  R3 says "To reach A, use label 10"
  R4 says "To reach A, use label 12"
  Now when R4 wants to forward a packet to A, it has 2 choices (Interface 0 → Label 10 & Interface 1 → Label 8)
  MPLS allows multiple possible paths to same destination
- The key difference between MPLS and IP is that IP routing picks one least-cost path, whereas MPLS can install multiple parallel paths for traffic engineering

▼ MPLS Labels Distribution

- Routers must exchange labels so that they know which label corresponds to which destination and which neighbor understands MPLS
- It is done using RSVP-TE (Resource Reservation Protocol - Traffic Engineering)
  It is the main MPLS signaling protocol (As per RFC 3468)
- OSPF is extended to distribute Link bandwidth availability and other traffic engineering parameters

▼ Advantages

- MPLS Traffic Engineering
  - It allows operators to override normal IP routing
  - Force specific flows to specific paths
  - Balance loads
  - Avoid congested paths
- Fast Restoration/Failover
  - MPLS can precompute backup paths
  - Automatic rerouting within milliseconds when a link fails (Faster than IP routing convergence)
- VPNs (Virtual Private Networks)
  - ISPs use MPLS to create customer-isolated VPNs with independent addressing and routing running over the same ISP backbone
  - This givens the foundation of MPLS Layer 3 & 2 VPNs

▼ MPLS vs SDN

- It was popular before SDN existed
- But now SDN can also do Traffic engineering, Flexible forwarding and Centralized decision making
- So, we are not sure if MPLS will continue to co-exist with SDN

▼ Summary

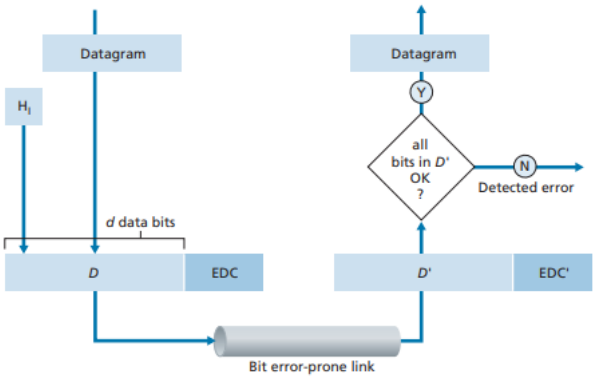
- Link Virtualization - Internet often treats complex networks (telephone network, VLAN network, MPLS network) as if they were simple link layers.
- MPLS
  - Adds a 4-byte label header between L2 and IP
  - Routers can forward based on labels, not IP addresses
  - Requires both sender and receiver to be MPLS-capable
  - Allows multiple paths, enabling traffic engineering
- Benefits
  - Multiple parallel paths
  - Fast rerouting
  - VPN support
  - Better bandwidth management
- Label Distribution
  - MPLS routers use RSVP-TE and extended OSPF to distribute labels and link-state information.

| Topic | Key Point |
|---|---|
| Link Virtualization | Complex networks treated as simple links |
| MPLS | Label-based forwarding + traffic engineering |
| MPLS Header | Label (20), Exp (3), S (1), TTL (8) |
| LSR | Router that switches using labels |
| Label Distribution | RSVP-TE + extended OSPF |
| MPLS Strength | TE, fast failover, VPNs |
| MPLS vs IP | Label lookup (fast) vs prefix matching (slow) |
| MPLS vs SDN | Coexist; SDN more flexible |

▼ Error Detection and Correction

- A link-layer frame travels across a single physical link between 2 directly connected nodes and during this transmission, it can get corrupted because of attenuation, noise, interference, cross talk, hardware imperfections etc.,
- So the receiver may receive bits different from what the sender has transmitted
- We need error-control mechanisms to detect that an error has occurred, correct it if possible or discard the frame and ask for retransmission
- Error control at the link layer is usually implemented in hardware (NIC) so it must be fast

▼ General Model




- We check if all bits in D' are OK
  This is because some errors may remain undetected

- Tradeoff: Stronger codes lead to more EDC bits, which means more computation and less undetected error probability

▼ Techniques used

- There are 3 techniques that link layer uses

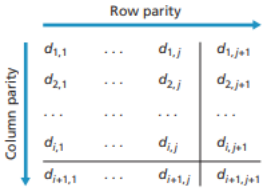
▼ Parity

▼ Single-bit Parity check

- Sender counts the number of 1s in data bits D (length D)
- Add 1 parity bit at the end so that
  - even parity : total number of 1s in the d+1 bits become even
  - odd parity : total number of 1s in the d+1 bits become odd
- Example
  if Data : `0111000110101011`
  then number of 1s : 10 (even)
  Parity bit : 0
  (similarly if number 1s was odd, parity bit : 1)
- Receiver count received number of 1s and if parity rule is broke, then error detected
  - So if it failed an even parity, and it detected an error, it means there were odd number of bit flips
- This entire mechanism is weak because real channels often have burst (multiple consecutive bits corrupted → high undetected error probability) errors, not independent bit errors

▼ Two Dimensional Parity

- It extends parity to a matrix
- Data bits are arranged as i x j grid




- Total parity bits = i row parities + j column parities + 1 global parity
- It can detect any 2-bit errors but can't correct it
- It can correct single-bit error
  The row with parity error identifies row index and the column with parity error identifies column index
  That bit is flipped to fix the error
- It can even detect burst errors better
- This is Forward Error Correction (FEC) because correction happens at the receiver without retransmission
- It is used in CDs, DVDs, deep-space communication, real-time apps

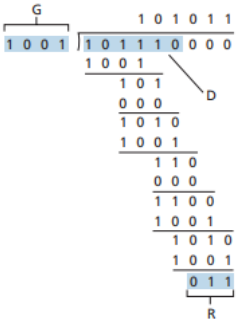
▼ Checksums

- Very common in TCP/UDP and sometimes link layer
- Procedure
  1. Divide data bits into k-bit words (TCP/UDP: k = 16 bits)
  2. Add all words using 1s complement addition
  3. Take 1s complement of that result (checksum)
  4. Receiver adds received data words + checksum
  5. If result = all 1s, then no error detected

- Advantages
  - Simple, Fast, Very low overhead
- Disadvantages
  - Weak at detecting some errors, Mainly designed for accidental corruption, CRC is stronger
- Since transport layer must run in software, checksum is preferred over CRC

▼ Cyclic Redundancy Check

- Strongest and Most widely used (Used in Ethernet, Wi-Fi, ATM, 802.11, switched LANs, Fiber links, and almost all NIC hardware)
- CRC views bits as a polynomial with coefficients 0/1
- Key terms
  - D = Data bits (length d)
  - G = Generator polynomial (length r+1)
  - R = CRC remainder (length r)
- Goal
  - Sender finds R such that `(D × 2^r) XOR R` is exactly divisible by G
- Sender Process
  - Append r zeros to `D` → `D x 2^r`
  - Divide using modulo-2 arithmetic (XOR instead of subtraction)
  - Remainder = R
  - Send `[D || R]` (d+r bits)
- Receiver Process
  - Divide received bits `[D' || R']` by same G
  - If remainder ≠ 0, then error detected
- Example
  - D = `101110`, d = 6, G = `1001`, r = 3
    The 9 bits transmitted are `101 110 011`




  - Receiver divides `101110011` / `1001`
    If remainder = 0 → No error detected
- CRC is powerful because it can detect all burst errors < (r+1) bits, any odd number of errors, burst errors longer than (r+1) with probability ≥ 1 - 2^(−r)
  For CRC-32 (r=32):
  Bust < 33 bits → always detected
  Large bursts → detected with probability > 99.99999999999%

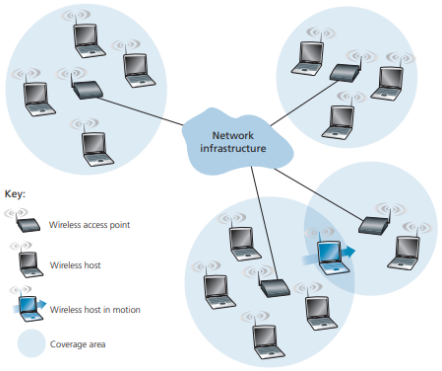
▼ Why different layers use different techniques

- Link Layer (Hardware - NIC) can compute CRC fast, so it uses CRC

- Transport Layer (Software) finds CRC too heavy, hence uses checksum

▼ Wireless Links and Network Characteristics

- Wireless networks differ from wired networks primarily in how hosts connect and how they communicate




▼ Core Components of a Wireless Network

▼ Wireless Hosts

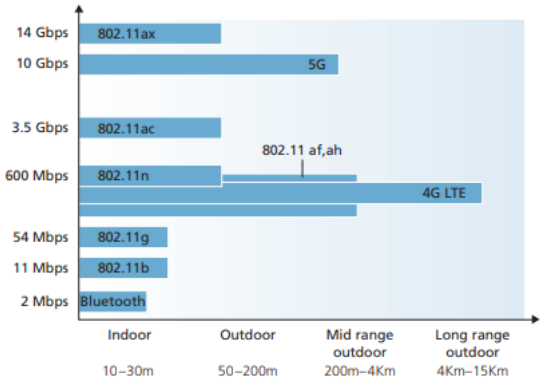
- These are the end systems that run applications like Smartphones, Laptops, Tablets, IoT devices, Robots, Drones etc.,
- A wireless host maybe mobile (moving across location) or stationary (wireless but fixed position)
- A wireless host has no inherent difference at higher layers from a wired host
- Mobility is what introduces complex issues (routing, handover, IP addressing etc.,)

▼ Wireless Links

- Wireless Hosts connect to either a base station or another wireless host directly (ad-hoc link)
- There are many types of wireless links

| Technologia | Range | Data Rate |
|---|---|---|
| Bluetooth | ~10m | ~2 Mbps |
| Wi-Fi (802.11) | 10-200m | 54 Mbps → 10 Gbps |
| 4G LTE | ~1km | 100 Mbps |
| 5G | 10m - 1km | 1-14 Gbps |

- The variation comes from Frequency bands, Power levels, Modulation used, Environment, Number of users sharing medium etc.,




▼ Base Station (AP/Cell Tower)

- A base station is a special network node that
  - sends data to wireless hosts

        - receives data from wireless host
        - Coordinates shared medium access (MAC)
        - Connects wireless devices to wired network
    - Examples include Wi-Fi Access Point, 4G/5G Cell Tower, Home router with Wi-Fi, Enterprise wireless controllers
    - When a wireless host is associated with a base station, it is within radio coverage and uses that base station as its relay to the rest of the internet
    - When a device enters range of another base station, it performs handoff
    - ▼ Infrastructure Mode
        - There is a base station (AP/Cell Tower)
        - Devices communicate through the base station
        - Routing, IP addressing, management happens through network
        - Examples : Home Wi-Fi, Campus Wi-Fi, 4G/5G cellular networks
    - ▼ Ad-hoc Mode
        - No base station
        - Nodes directly communicate with other nodes
        - Nodes must self-organize
            - Routing
            - Address management
            - Forwarding
            - Discovery
        - Examples : Bluetooth personal networks, MANETs, VANETs, Disaster relief networks
- ▼ Types of Wireless Network Architectures
    - Wireless networks can be classified using 2 criteria
      i) Number of hops (single/multi hop)
      ii) Presence of infrastructure
      This gives 4 categories
    - ▼ Single-hop, Infrastructure-based
        - Most common
        - Device connects directly to AP or cell tower
        - Examples : Wi-Fi in cafes, universities, 4G LTE data networks, 5G NR connectivity
        - Device → One wireless hop → base station → internet
    - ▼ Single-hop, Infrastructure-less
        - No base station
        - One node acts as coordination (master)
        - Examples : Bluetooth piconet, Some sensor networks, Wireless USB
    - ▼ Multi-hop, Infrastructure-based
        - A base station exists
        - But some nodes can’t reach it directly
        - Nodes relay traffic for each other
        - Examples : Wireless mesh networks, Smart home mesh devices like Google nest Amazon Eero etc., Sensor networks
    - ▼ Multi-hop, Infrastructure-less

- No base station
- Nodes route for each other
- Nodes may be mobile
- Examples : MANET (Mobile Ad-hoc NETwork), VANET (Vehicular Ad-hoc NETwork), Soldier battlefield networks
- Research area: routing, addressing, security

▼ Wireless Links and Network Characteristics

- Wireless and Wired channels differ due to multiple physical effects

▼ Key Challenges in Wireless Links

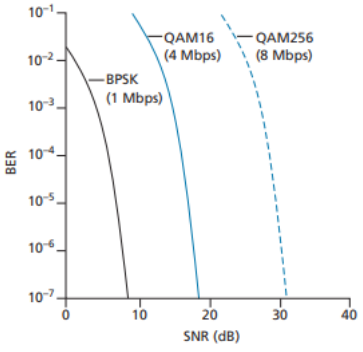
- Decreasing Signal Strength
  - Signal can attenuate due to Distance (path loss), Obstacles (wall, buildings), Weather (fog, rain)
  - This results in signal becoming weaker and bits getting corrupted leading to higher bit error rate
- Interference
  - Interference comes from other wireless transmitters in same band, appliances like microwaves ovens at 2.4 GHz, Bluetooth devices, Motors and electronic noise
- Multipath Propagation
  - A transmitted signal may arrive along a direct path or reflected path (ground, walls, objects)
  - These multiple signals interfere and cause fading, phase shifts, time distortion
  - This leads to random fluctuations in received signal strength

▼ Signal-to-Noise Ratio (SNR)

- $SNR = \frac{received\ signal\ power}{noise\ power}$
- Measured in dB (decibels)
- High SNR → Easier to decode bits
- Low SNR → High bit error rate (BER)

▼ BER vs SNR

- The given graph shows BER curve for BPSK, QAM16, QAM256




- Observations:
  - Higher SNR = Lower BER
  - Higher data rate modulation → needs higher SNR
  - At low SNR, only simple modulation is usable
  - Adaptive modulation changes rate based on SNR

▼ Adaptive Modulation

- The main idea is that a device chooses the highest possible bit rate for current SNR that keeps BER acceptable

- It is used in All Wi-Fi (802.11), 4G LTE, 5G
- Examples :
  High SNR = QAM256 (814 Gbps)
  Medium SNR = QAM16 (100-600 Mbps)
  Low SNR = BPSK/QPSK (Reliable but slow)

▼ Hidden terminal problem

- It occurs when A and C can't hear each other, both transmit to B and collision occurs at B
- The causes could be because of physical obstacles like (mountains/buildings), or fading because signal is too weak to be detected

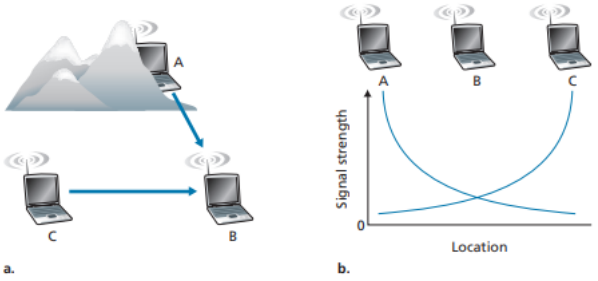



**Figure 7.4** ♦ Hidden terminal problem caused by obstacle (a) and fading (b)

- This makes multiple access far more complex in wireless networks than wired networks

▼ CDMA

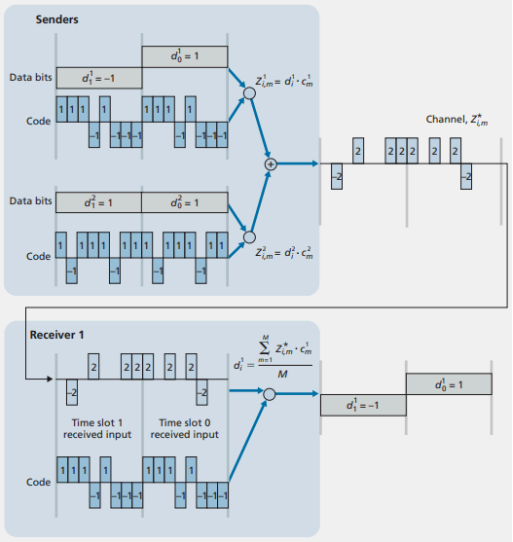
- Code Division Multiple Access is a channel partitioning technique that divides the medium using codes, not time or frequency

▼ Basic Idea

- Each sender gets a **unique code** of ±1 values.
- Data bits also represented as:
  - 1 → +1
  - 0 → −1
- During one bit time:
  - That bit is multiplied by the entire code sequence
  - Result is a chipped signal
  - Receiver uses correlation with same code to recover bit

▼ Requirement

- Codes must be orthogonal
- All users must have roughly equal power at receiver (power control is a major issue in cellular network)




A two-sender CDMA example

▼ Multiple Access Links and Protocols

- Now the fundamental problem of broadcast networks is about how multiple nodes share a single communication channel without destroying each other's transmissions
- This is the multiple access problem

▼ Why Multiple Access Protocols exist

- Links in networks are either

1. Point-to-Point links
   One sender ↔ One receiver
   Examples: PPP, HDLC, point-to-point fiber links
   No contention because only 2 nodes share the link
2. Broadcast Links
   Multiple senders + Multiple receivers all share a single shared broadcast channel
   When one node transmits, all other nodes receive
   Examples: Ethernet, Wi-Fi, Cable TV upstream, Satellite communication

- But when multiple nodes transmit on same channel at same time, signals collide and then no frame is usable, causing the entire transmission to be wasted
- Now to ensure nodes know when to speak, when to wait, and how to recover after collision, we use rules called Multiple Access Protocols
- The goal of a good Multiple Access Protocol is that it must ideally satisfy the following:
  1. Single node active = it gets full rate R
  2. M nodes active = each gets fair share R/M
  3. Full decentralized = No master controller and Nodes operate independently (no single point of failure)
  4. Simple and inexpensive to implement

▼ Classification of Multiple Access Protocols

▼ Channel Partitioning Protocols

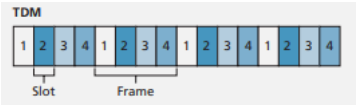
- The idea of dividing the channel into separate pieces so each node gets a piece, eliminates collisions completely

▼ The 3 main techniques

▼ TDM - Time Division Multiplexing

- Time is divided into frames
- Each frame divided into N time slots
- Each slot assigned to one node

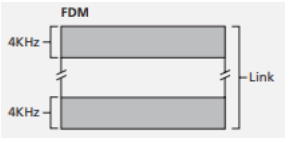
- A node can transmit only in its slot




- Advantages
  - No collisions
  - Perfect fairness
  - Each node gets $\frac{R}{N}$ bps
- Disadvantages
  - Wastes bandwidth when only few nodes have data
  - Node must wait until its slot even if idle channel

▼ FDM - Frequency Division Multiplexing

- Divide the channel into N frequency bands
- Each band has bandwidth $\frac{R}{N}$
- Each node gets one band
- Nodes transmit continuously on their band
- Advantages & Disadvantages same as TDM




▼ CDMA - Code Division Multiplexing Access

- Allocate a unique code to each node
- Nodes encode their data using their code
- Multiple nodes can send simultaneously
- If codes are orthogonal, receivers decode correctly

▼ Random Access Protocols

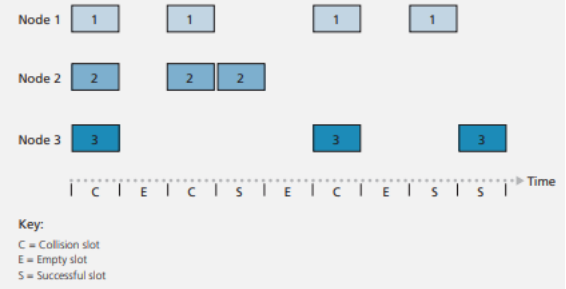
- Here nodes don't divide the channel
- Instead any node transmits at full R bps, but if collision occurs it retransmits after random delays
- It is decentralized and simple and most widely used (Ethernet, Wi-Fi)

▼ 2 Major Families

▼ ALOHA

▼ Slotted ALOHA

- Assumes that all frames = L bits, Time divided into slots of duration $\frac{L}{R}$ , nodes transmit only at slot boundaries and nodes detect collisions
- Protocol:
  If you have a frame → transmit at next slot start
  If collision → with probability p, retransmit next slot
  With probability (1-p), wait another slot

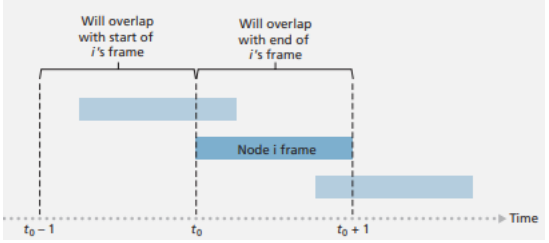



Nodes 1, 2, and 3 collide in the first slot. Node 2 finally succeeds in the fourth slot, node 1 in the eighth slot, and node 3 in the ninth slot

- Efficiency Analysis
  - Slot is successful if exactly ONE node transmits in the slot
  - with N nodes, each transmitting with probability $P(success) = N * p * (1-p)^{N-1}$
  - Maximum efficiency occurs at p = $\frac{1}{N}$
  - As N → ∞, Maximum efficiency = $\frac{1}{e}$ = 0.37 = 37%
- This means that
  Channel is bust 100% of time and only 37% is useful
  37% slots → successful
  26% slots → collision
  37% slots → empty

▼ Pure ALOHA

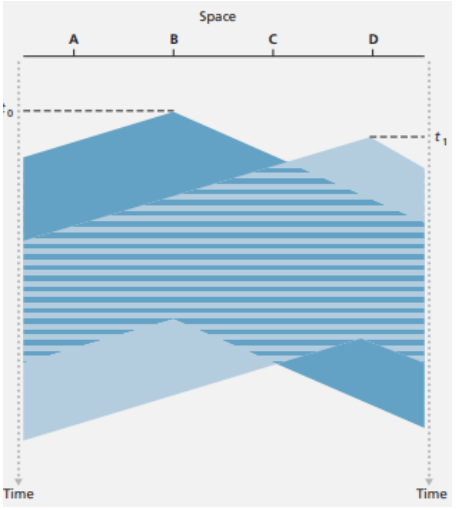
- No slot boundaries
- Nodes transmit immediately when frame arrives
- Vulnerability window: A frame of duration T collides with any transmission beginning within T before or T after → 2T vulnerable period
  Hence collision probability doubles
- Efficient = $\frac{1}{2e}$ = 18.4%
- Pure ALOHA is simple but very inefficient




▼ CSMA (Carrier Sense Multiple Access)

▼ CSMA

- ALOHA is like people talking without listening whereas CSMA add politeness
- The main rule is to listen before transmission
  If channel is busy, wait
  Still, collisions occur because of propagation delay




Space-time diagram of two CSMA nodes with colliding transmissions

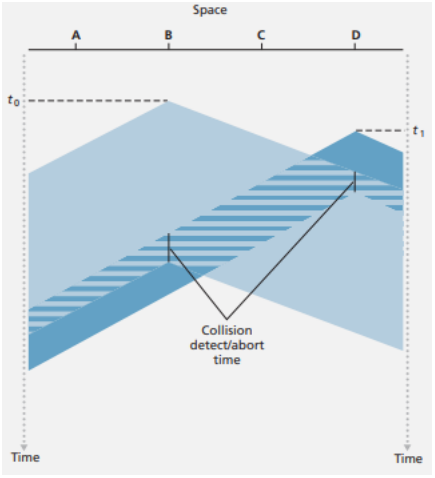
- In the above Space-Time diagram
  Node B starts transmitting at t0
  Bits take time to reach D
  at t1, D senses channel idle and transmits
  B's signal arrives later, and causes collision
- CSMA only reduces collisions, but can't eliminate them

▼ CSMA/CD

- Carrier Sense Multiple Access/Collision Detection
- It improves CSMA by the following

1. Carrier Sense
   - Check before sending
2. Collision Detection
   - If collision detected, abort transmission
3. Binary Exponential Backoff
   - Wait random time before retransmission
   - After n collisions:
   Choose K from {0,1,2,…,2^n – 1}
   Backoff time = K × 512 bit-times

- Binary exponential backoff solves the issue of collision
  if many nodes transmitting → large wait window
  if few nodes transmitting → small wait window



▼ Operation

1. Get datagram from network layer
2. Listen to channel
   - Idle → send
   - Busy → wait
3. While transmitting → listen
4. If collision detected →
   - Abort transmission
   - Jam signal (old Ethernet)
   - Backoff using exponential rule
5. Try again from step 2

▼ Advantages

- Higher efficiency than ALOHA
- No need for central controller
- Scales to hundreds of nodes
- Simpler than Token Passing

▼ Disadvantages

- Doesn't work well on wireless (hidden terminal problem)
- Requires wired shared medium (Ethernet bus, hub)

- This is why Wi-Fi uses CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- Taking Turn Protocols (3rd not there in syllabus)

▼ Wi-Fi: 802.11 Wireless LANs

▼ Introduction

- Wi-Fi is the dominant wireless LAN technology used in homes, offices, colleges, airports etc.,
- Many WLAN technologia already existed in 1990s but 802.11 became to universal standard because of open standardization, backward compatibility, low-cost hardware, support for high data rates, operation in unlicensed spectrum

▼ IEEE 802.11 Standards Overview

- Different versions of Wi-Fi that have appeared over time

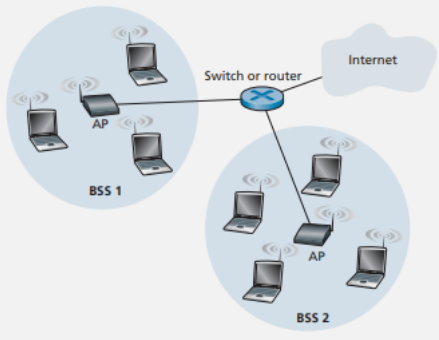
| IEEE 802.11 Standard | Year | Max Data Rate | Range | Frequency |
|---|---|---|---|---|
| 802.11 b | 1999 | 11 Mbps | 30 m | 2.4 GHz |
| 802.11 g | 2003 | 54 Mbps | 30 m | 2.4 GHz |
| 802.11 n (WiFi 4) | 2009 | 600 Mbps | 70 m | 2.4, 5 GHz |
| 802.11 ac (WiFi 5) | 2013 | 3.47 Gbps | 70 m | 5 GHz |
| 802.11 ax (WiFi 6) | 2020 (expected) | 14 Gbps | 70 m | 2.4, 5 GHz |
| 802.11 af | 2014 | 35–560 Mbps | 1 km | unused TV bands (54–790 MHz) |
| 802.11 ah | 2017 | 347 Mbps | 1 km | 900 MHz |

- Common feature among all versions are
  - Same MAC protocol: CSMA/CA
  - Same frame structure
  - Adaptive data rate (Reduce rate to increase range)
  - 2 Modes supported (Infrastructure & Ad-hoc modes)
- Differences

- PHY (modulation, bandwidth, antennas)
- Range & speed
- Interference susceptibility

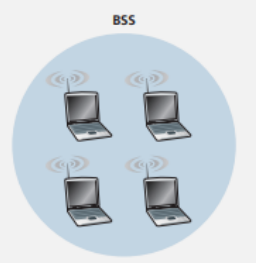
▼ Basic Wi-Fi Architecture

- Basic Service Set
  - This is the foundation of 802.11 WLAN architecture
  - Includes:
    - One or more wireless hosts
    - An Access Point (AP) → central controller
  - Each AP/host has a unique MAC address
- Infrastructure Wireless LAN
  - Most common type
  - AP connects wireless hosts to wired network




IEEE 802.11 LAN architecture

- Ad Hoc Network
  - No AP
  - Formed “on the fly” when devices are near each other
  - No centralized control




An IEEE 802.11 ad hoc network

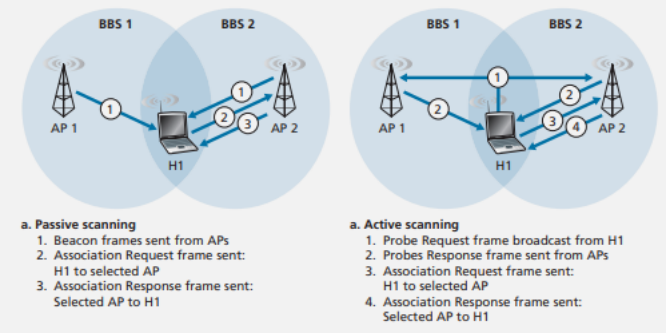
▼ AP Configuration

- SSID (Service Set IDentifier)
  - Network administrator assigns an SSID to each AP.
  - AP broadcasts its identity using SSID.
- Channels
  - Wi-Fi operates in 2.4 GHz – 2.485 GHz band.
  - 802.11 defines 11 partially overlapping channels.

- Admin assigns a specific channel number to each AP to reduce interference.

- Association Requirement
  - A wireless device must associate with exactly one AP to gain Internet access.
  - Only the associated AP:
    - Sends frames to the device.
    - Receives frames from the device.

▼ AP Discovery (Scanning Processes)




- Passive Scanning
  - AP periodically sends beacon frames containing:
    - SSID
    - MAC address
  - Wireless station scans channels (1–11) and listens for beacons.
  - Device/user chooses AP based on:
    - Strongest signal
    - Low load (not specified by 802.11 standard)
- Active Scanning
  - Wireless station broadcasts a probe request frame.
  - All APs nearby respond with probe response frames.
  - Station compares responses → chooses an AP.
  - Station sends association request, AP replies with association response.

▼ Authentication & IP Allocation

- Authentication
  - Optional step before association
  - Common methods like MAC address filtering, Username/Password Authentication (WPA2)
- IP Address Assignment/Allocation
  - After association, wireless station sends DHCP discovery through AP
  - Receives an IP address of the Wi-Fi network's subnet

▼ IEEE 802.11 MAC Protocol

▼ Why CSMA/CD Cannot Be Used in Wi-Fi

- Ethernet uses CSMA/CD → requires simultaneous transmit + receive.
- In Wi-Fi:
  - Received signal is very weak compared to transmitted signal → collision detection hardware is expensive/impractical.

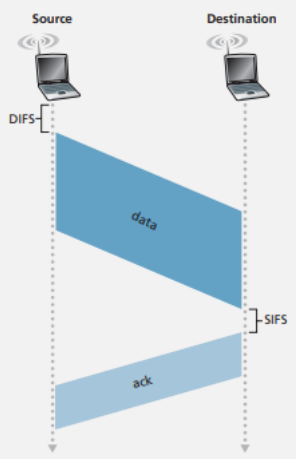
    - Hidden terminal & fading make collision detection unreliable.
- Hence Wi-Fi uses CSMA/CA (Collision Avoidance), not CSMA/CD.

▼ CSMA/CA Operation

1. Station senses the channel:
    - If IDLE → wait for DIFS (Distributed Inter-Frame Space)
    - If BUSY → choose random backoff (binary exponential backoff).
2. Backoff Countdown:
    - Timer decrements only when channel is idle.
    - Freezes when channel is busy → prevents multiple stations from hitting zero at the same time.
3. Transmission:
    - When backoff reaches zero → transmit the entire DATA frame.
4. Acknowledgment:
    - Receiver sends ACK after SIFS (Short Inter-Frame Space).
    - SIFS < DIFS → ensures no other device interrupts ACK.
5. If no ACK:
    - Station assumes collision → re-enters backoff → retransmits.

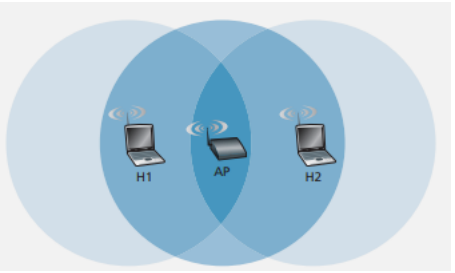
▼ Why Acknowledgment Is Needed

- Wireless links have high bit error rate.
- ACK + retransmission (ARQ) ensures reliability (unlike Ethernet).



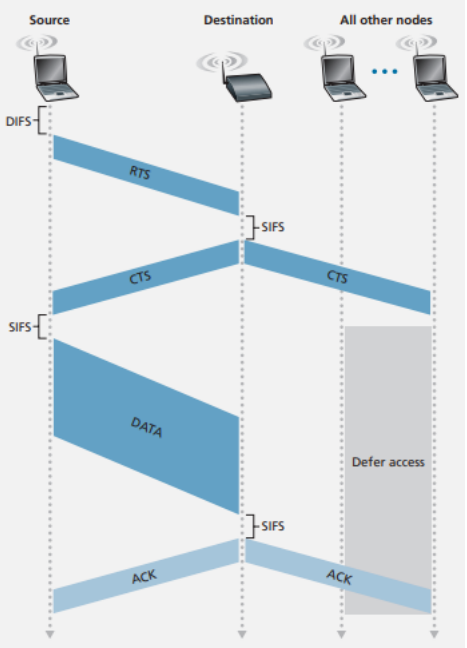

▼ Hidden Terminal Problem

- Example: H1 and H2 sending to AP but cannot hear each other.
- Both think channel is idle → they transmit → collision at AP.
- **Solution:** Use RTS/CTS mechanism.



▼ RTS/CTS Mechanism (Distributed Coordination Function – DCF)

- Process
  1. Sender sends RTS (Request to Send) to AP.
  2. RTS includes NAV (Network Allocation Vector) duration = time required for:
     - Data frame + ACK.
  3. AP responds with CTS (Clear to Send):
     - Grants permission to sender.
     - Broadcasts reservation → all stations update NAV → go silent.
- Purpose
  - Prevent hidden terminals.
  - Ensure exclusive use of channel during communication.



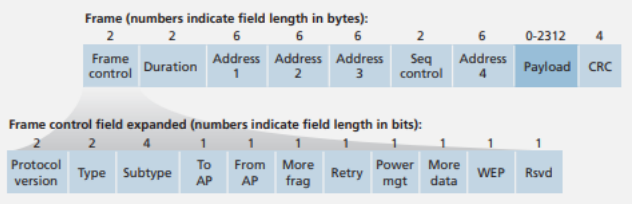

▼ Properties of RTS/CTS

- Small size → collisions cost less than data frame collision.
- After DIFS, communication uses SIFS gaps, so no external station can start transmission until communication finishes.
- If RTS Collides, No CTS from AP → sender backs off → safe recovery.

▼ When is RTS/CTS Used?

- Used only for long data frames.
- Stations maintain an RTS threshold.
- Many devices set threshold > maximum frame length → RTS/CTS often disabled to reduce overhead.

▼ IEEE 802.11 Frame Structure



▼ Payload Section

- Contains IP datagram / ARP packet.
- Max size allowed: 2312 bytes.
- Usually less than 1500 bytes (to match Ethernet MTU).

▼ CRC

- 32-bit CRC for error detection.

▼ Sequence Number Field

- Helps receiver distinguish:
  - New frame vs.
  - Retransmitted frame.

▼ Duration Field

- Used for NAV.
- Indicates reserved channel time needed for:
  - Data frame transmission
  - ACK transmission

▼ Frame Control Fields

- Type + Subtype identify:
  - RTS
  - CTS
  - ACK
  - DATA frames
- To/From DS bits determine semantics of address fields.

▼ Address Fields (4 MAC Addresses)

| Field | Meaning |
|---|---|
| Address 1 | Receiver (destination wireless station) |
| Address 2 | Transmitter (the node that sent the frame) |
| Address 3 | Used for internetworking — router interface MAC |
| Address 4 | Used in special cases (e.g., wireless distribution systems) |

▼ AP as a Link-Layer Device

- AP does not understand IP.
- AP only converts 802.3 (Ethernet) frames ↔ 802.11 frames.

▼ Frame Encapsulation Example

- Case 1: Router (R1) → H1
  1. R1 creates an Ethernet frame:
     - Src MAC: R1
     - Dest MAC: H1
  2. AP converts to 802.11 frame:
     - Address 1 = H1
     - Address 2 = AP
     - Address 3 = R1
- Case 2: H1 → Router (R1)
  1. H1 creates 802.11 frame:

- Address 1 = AP
- Address 2 = H1
- Address 3 = R1

2. AP converts to Ethernet frame → sends to R1.