Module 5
(Wireless LAN)

(Data Link Layer and Medium Access Sub Layer: Error Detection and Error Correction - Fundamentals, Block coding, Hamming Distance, CRC; Flow Control and Error control protocols - Stop and Wait, Go back – N ARQ, Selective Repeat ARQ, Sliding Window, Piggybacking, Random Access, Multiple access protocols -Pure ALOHA, Slotted ALOHA, CSMA/CD,CDMA/CA; Wired LAN, Wireless LANs, Connecting LANs and Virtual LANs)

Dr. Nirnay Ghosh

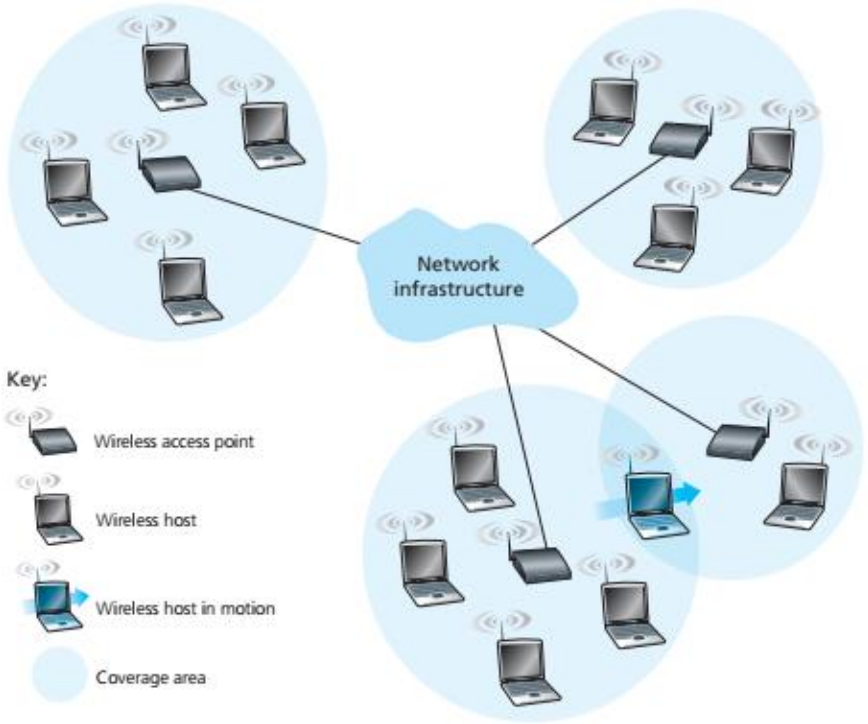
Assistant Professor

Department of Computer Science & Technology

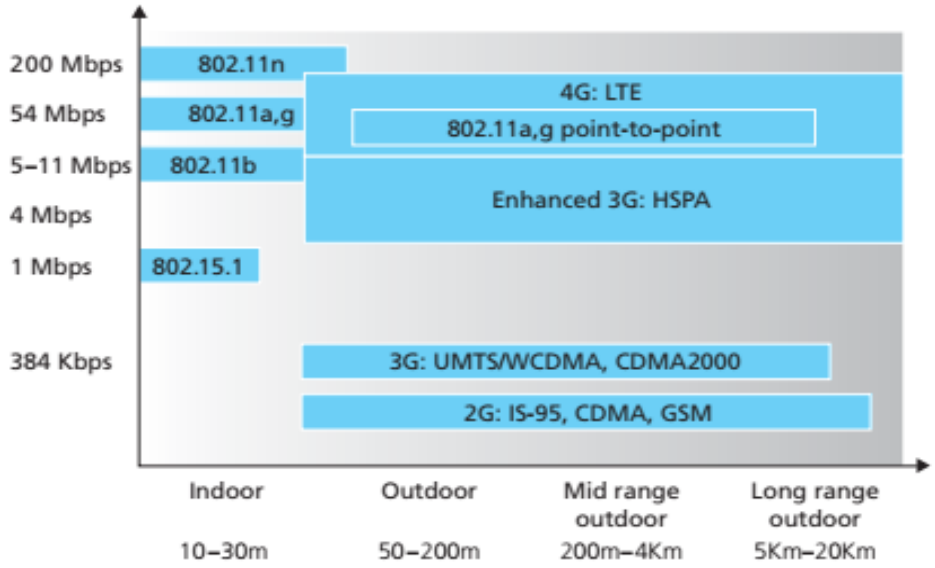
IIEST, Shibpur

Wireless LAN

- Major components
  - Wireless hosts
  - Wireless links
  - Base station



Elements of Wireless Network



Link Characteristics of Selected Wireless Standards

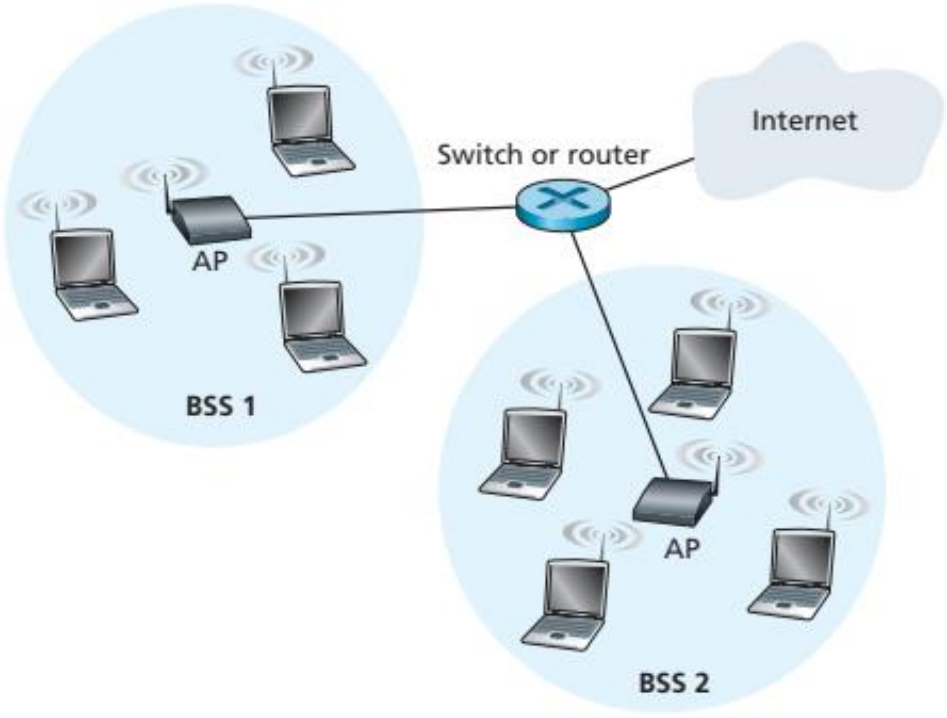
- Types of networks:
  - Single-hop infrastructure-based (802.11 networks, 3G/4G, etc.)
  - single-hop infrastructure-less (Bluetooth networks, 802.11 networks in ad hoc mode)
  - multi-hop infrastructure-based (Wireless sensor networks)
  - multi-hop infrastructure-less (MANET, VANET)
- Replacing a wired LAN (Ethernet) with wireless LAN (802.11 networks)
  - Wireless network interface → wired Ethernet interface
  - Access point → Ethernet switch
- *No change needed at the network layer or above*

Wi-Fi: 802.11 Wireless LANs

- Several 802.11 standards: 802.11b, 802.11a, and 802.11g
  - CSMA/CA medium access protocol
  - Same frame structure for link-layer frames
  - Reduces transmission rates to reach out over greater distances
  - New standard: 802.11n
    - MIMO antennas: enables transmitting/receiving different signals
    - Transmission rate: few hundred mbps
- Architecture: basic service sets (BSS) – wireless stations and base station (access point), interconnection device (switch/router), Internet

Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

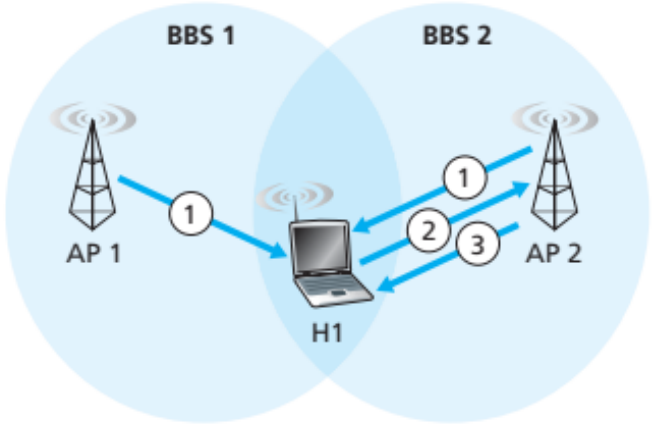
Summary of IEEE 802.11 Standards



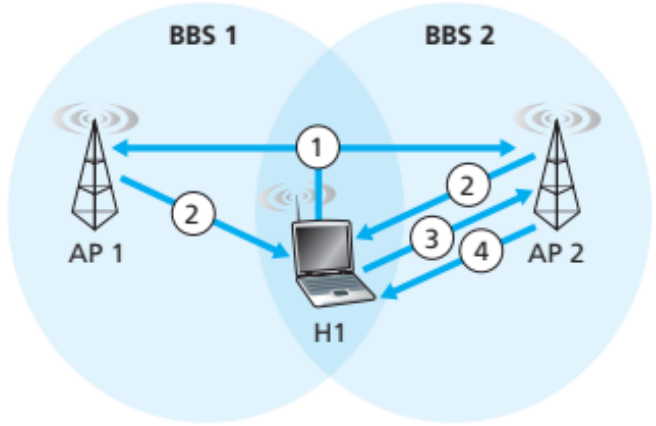
IEEE 802.11 LAN Architecture

Wi-Fi: 802.11 Wireless LANs

- Access point (AP):
  - Service Set Identifier (SSD): administrator assigned name
  - Channel number
- Wi-Fi jungle: location where a wireless station receives signals from two or more APs.
  - Different IP subnets
  - Independently assigned channels
- Wireless station *associates* with exactly one AP
  - AP sends periodic beacon frames (containing SSID + MAC)
  - Wireless station scans 11 channels and listens for beacon frames from the APs
    - Scanning: passive; active
  - Selects one of the APs for association



a. Passive scanning
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1



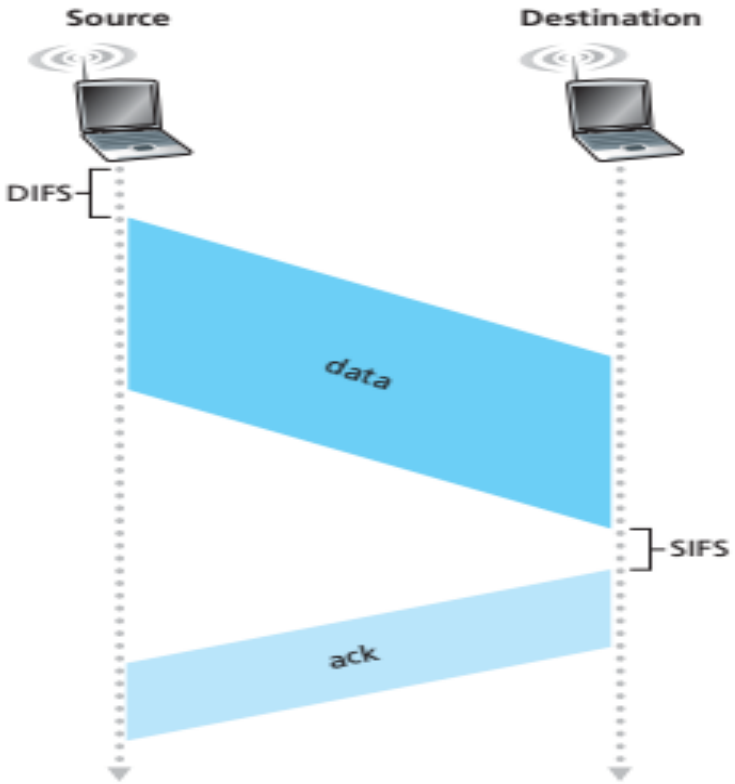
a. Active scanning
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Active and Passive Scanning for APs

- Wireless station sends discovery message to the DHCP server via the AP
  - IP address of the subnet
- Authentication: AP relays credentials to a separate authentication server
  - MAC address, Username/Password

Wi-Fi: 802.11 Wireless LANs

- Multiple stations may transmit data frames at the same time over the same channel
- Medium access control (MAC) protocol: coordinates transmissions
- Access method: CSMA/CA
  - Wireless channels: relatively high bit error rates
    - Link-layer acknowledgment/retransmission (ARQ) scheme.
- Protocol:
  - Distributed Inter-frame Space (DIFS)
  - Generates a random back-off value using the binary exponential back-off algorithm
  - Channel busy: counter value remains frozen.
  - Channel idle: counter value starts to diminish
  - Counter reaches zero (note that this can only occur while the channel is sensed idle) - station transmits the entire frame and then waits for an acknowledgment.
  - Receiving station: computes CRC; If passes, it waits a short period of time known as the Short Inter-frame Spacing (SIFS); sends the acknowledgement

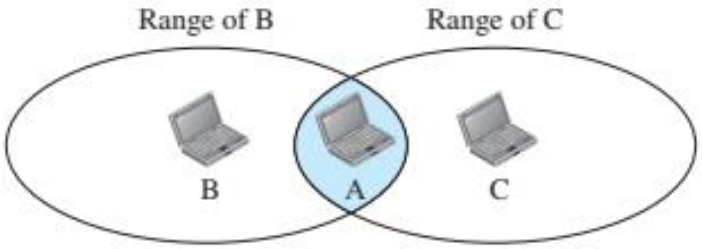


802.11 uses Link-layer Acknowledgements

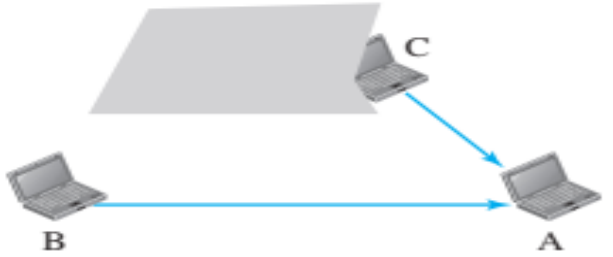
- Acknowledgment received: frame is correctly received at the destination station.
- Acknowledgment not received: transmitting station reenters the back-off phase in with the random value chosen from a larger interval.

Wi-Fi: 802.11 Wireless LANs

- Exposed station problem
  - Two stations in the transmission range of the third station
  - Third station transmits frame to one of these stations
  - Other senses channel; stops sending frames to the fourth one
- Hidden station problem
  - A station may not be aware of another station's transmission
    - Obstacles or out of transmission range
  - Cannot detect any collision that may occur

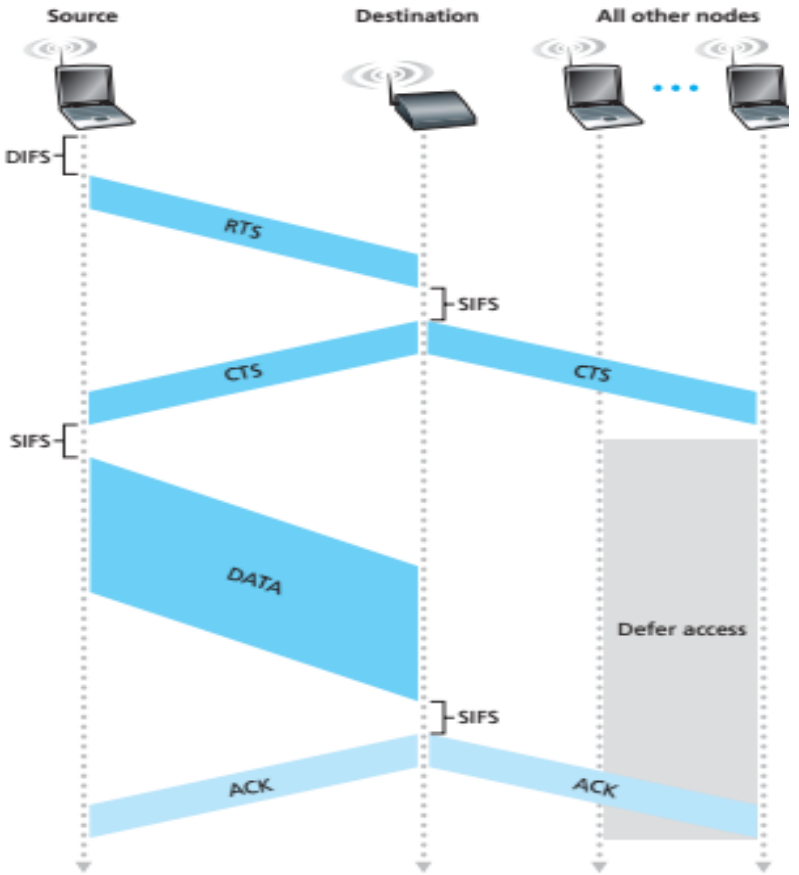


a. Stations B and C are not in each other's range.



b. Stations B and C are hidden from each other.

Hidden Station Problem



Collision Avoidance using the RTS and CTS Frames

- Stations use Request to Send (RTS) and Clear to Send (CTS) control frames to reserve access to the channel
- Network Allocation Vector (NAV)
  - Timer created by non-transmitting stations
  - Valid till the duration of time given in RTS frame
  - Checks NAV to determine if the physical medium to be sensed.

Wi-Fi: 802.11 Wireless LANs

• IEEE 802.11 Frame

- Payload: consists of IP datagram or ARP packet – maximum size 2312 bytes – typically of 1500 bytes
- CRC: 32-bit CRC – to detect bits errors in the received frames
- Address fields:
  - Address 2: sender's address (wireless station or AP)
  - Address 1: receiver's address (wireless station or AP)
  - Address 3: router's interface
  - Address 4: next AP's address (ad-hoc mode)
- Sequence number: allows the receiver to distinguish between a newly transmitted frame and the retransmission of a previous frame
- Duration: time for which the channel will be reserved for transmitting frame and acknowledgement
- Frame control: consists of multiple subfields
  - Type and Subtype: distinguishes between RTS, CTS, ACK, and data frames
  - To and From: indicates different address fields
  - WEP: encryption used or not

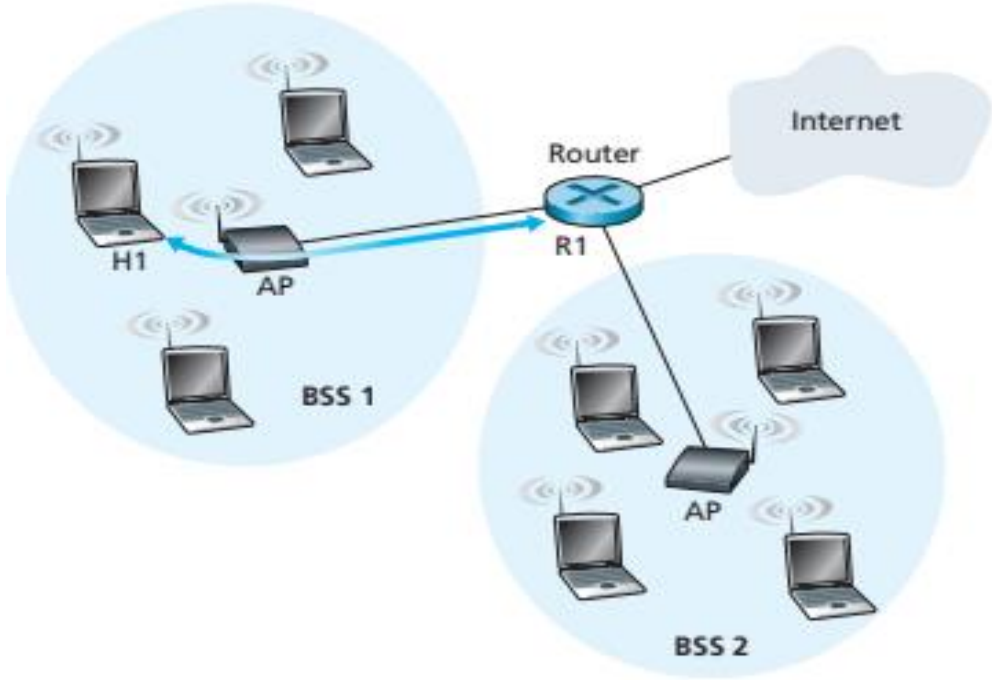
Frame (numbers indicate field length in bytes):

2	2	6	6	6	2	6	0-2312	4
Frame control	Duration	Address 1	Address 2	Address 3	Seq control	Address 4	Payload	CRC

Frame control field expanded (numbers indicate field length in bits):

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

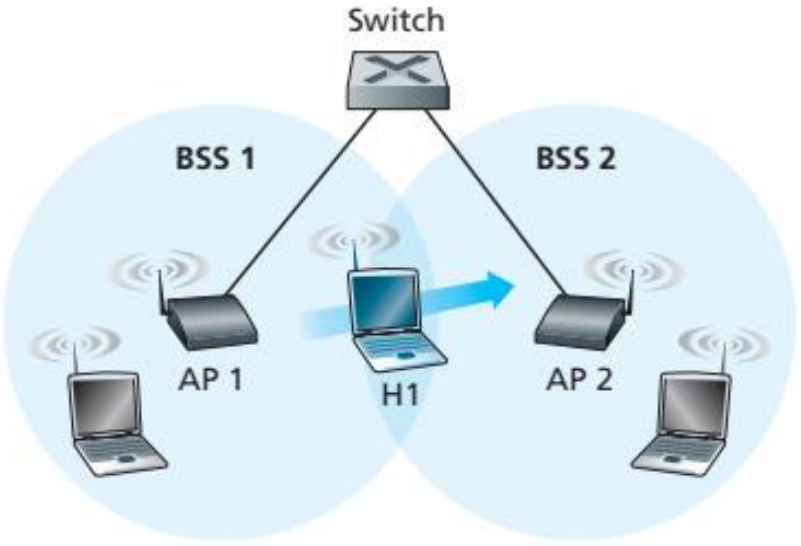
The IEEE 802.11 Frame



Use of Address Fields in 802.11 frames

Wi-Fi: 802.11 Wireless LANs

- Mobility in the Same IP Subnet
  - Interconnection device: switch
  - Wireless stations, APs: belong to the same IP subnet
  - *BSS1* →*BSS2*: IP address, TCP connection are retained
  - Scenario*: H1* moves from *BSS1* to *BSS2*
    - *AP1*'s signal weakens; *H1* scans for stronger signal
    - Receives beacon frames from *AP2*
    - Handoff process: disassociates from *AP1*, associates with *AP2* – same IP address, ongoing TCP session.
    - Switch updates forwarding table: pairing of *H1*'s MAC address with the outgoing interface
      - Self-learning
      - Broadcast message from *AP2* following association



Mobility in the Same Subnet

- Advanced Features in 802.11
  - Rate adaptation: select physical layer modulation technique based on current or recent characteristics
  - Power management:
    - Sensing, transmitting, receiving – consumes power
    - Alternates between sleep and wake states
    - Sleep state – set the power-management bit in IEEE 802.11 frame
    - AP refrains from sending data frames to stations with the power management bit set high – stores the frames in its buffer
    - Timer wakes up the station before AP sends beacon frame (typically after every 100 ms) in 250 µs
    - AP sends the list of stations whose frames are buffered in the beacon frame
    - Station go back to sleep if it has no buffered frames – otherwise requests for the frame by sending polling message