Overview of Wireless LANs

- Use wireless transmission medium
- Until 10 years ago, wireless LANs were little used because of issues of high prices, low data rates, occupational safety concerns, & licensing requirements
- As those problems have been addressed, popularity of wireless LANs has grown rapidly
- Key application areas:
  - cross-building interconnect:
    - connects LANs in nearby buildings, connecting bridges or routers; point-to-point wireless link and no a LAN per se
  - LAN extension
  - nomadic access
  - ad hoc networking
Single Cell LAN Extension

Figure 17.1

Multi Cell LAN Extension

Figure 17.2
Nomadic and Stationary Stations

Ad Hoc Networking

- temporary peer-to-peer network
**Wireless LAN Requirements**

- Throughput: MAC should provide efficient use of wireless medium
- Number of nodes: support for hundreds of nodes across multiple cells
- Connection to backbone LAN
- Service area: 100 to 300 m
- Low power consumption for long battery life on mobiles
- Transmission robustness and security
- Collocated network operation: likely that two or more wireless LANs operate in same areas with possible interference
- License-free operation
- Handoff/roaming: enable mobile stations to move from one cell to another.
- Dynamic configuration: addition, deletion, and relocation of end systems without disruption to users

---

**Transmission Technology**

- Infrared (IR) LANs
  - individual cell of IR LAN limited to single room
  - IR light does not penetrate opaque walls
- Spread spectrum LANs
  - operate in ISM (industrial, scientific, and medical) 2.4-GHz microwave bands
  - no FCC licensing is required in USA
  - the most popular type of wireless LANs
- Orthogonal Frequency Division Multiplexing (OFDM) LANs
  - operate in either 2.4 GHz or 5 GHz band
  - superior to spread spectrum
  - product with this technology are getting common
Transmission Issues

- Licensing regulations differ between countries
- In USA FCC, three microwave bands have been set aside for unlicensed spread spectrum use:
  - 902 - 928 MHz (915-MHz band)
  - 2.4 - 2.4835 GHz (2.4-GHz band)
  - 5.725 - 5.825 GHz (5.8-GHz band)
- 2.4 GHz also in Europe and Japan
- Interference
  - many devices around 900 MHz: cordless telephones, wireless microphones, and amateur radio
  - fewer devices at 2.4 GHz; microwave oven
  - little competition at 5.8 GHz

Wireless Stations

- All components that can connect into a wireless medium are referred to as stations and stations are equipped with wireless network interface controllers (WNICs).
- **Wireless stations** fall into one of two categories: access points, and clients.
- **Access points (APs)**, earlier we have referred to them as control modules (CMs), are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.
- **Wireless clients** can be mobile devices such as laptops, personal digital assistants, IP phones, and other smartphones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.
IEEE 802.11 Specification

- IEEE has defined 802.11 specification for a wireless LAN, which covers the physical and data link layers.
- Public uses term WiFi (for wireless fidelity) as a synonym for wireless LAN.
- WiFi, however, is a wireless LAN that is certified by the WiFi Alliance, an industry association of more than 300 member companies devoted to promoting the growth of wireless LANs.
- IEEE 802.11 defines two kind of services:
  - the basic service set (BSS)
  - the extended service set (ESS)

IEEE 802.11 Services

- The basic service set (BSS) is a set of all stations that can communicate with each other and every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.
- An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they can not connect to any other basic service set.
- An extended service set (ESS) is a set of connected BSSs with access points.
- A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells. DS can be wired or wireless.
- Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.
Extended Service Set (ESS)

• 2 BSSs can overlap; a station may participate in more than one BSS
• ESS appears as a single logical LAN to the upper layer.

Basic Functioning

• AP can function as a bridge and a relay point.
• If one station in the BSS wants communicate with another station outside of its range (reach), the MAC frame is first sent to AP and then from AP to destination station if in the same BSS.
• If the destination is in another BSS, the MAC frame is relayed over DS.
• The idea is similar to communication in cellular (wireless telephone) network, if we consider each BSS to be a cell and each AP to be a base station.
Types of Stations Based on Mobility

- There are three types of stations, based on their mobility:
  - no-transition mobility: a station is either stationary or moving only inside a BSS
  - BSS-transition mobility: a station can move from one BSS to another, but the movement is confined inside one ESS.
  - ESS-transition mobility: a station can move from one ECC to another, but IEEE 802.11 doesn't guarantee that communication is continued during the move.

IEEE 802.11 Protocol Architecture

![IEEE 802.11 Protocol Architecture](image)

Figure 17.5
Data Rate (Mbps) vs. Distance (meters)

Table 17.5

<table>
<thead>
<tr>
<th>Data Rate (Mbps)</th>
<th>802.11b</th>
<th>802.11a</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>90+</td>
<td>–</td>
<td>90+</td>
</tr>
<tr>
<td>2</td>
<td>75</td>
<td>–</td>
<td>75</td>
</tr>
<tr>
<td>5.5 (b) / 6 (a/ g)</td>
<td>60</td>
<td>60+</td>
<td>65</td>
</tr>
<tr>
<td>9</td>
<td>–</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td>11 (b) / 12 (a/ g)</td>
<td>50</td>
<td>45</td>
<td>50</td>
</tr>
<tr>
<td>18</td>
<td>–</td>
<td>40</td>
<td>50</td>
</tr>
<tr>
<td>24</td>
<td>–</td>
<td>30</td>
<td>45</td>
</tr>
<tr>
<td>36</td>
<td>–</td>
<td>25</td>
<td>35</td>
</tr>
<tr>
<td>48</td>
<td>–</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>54</td>
<td>–</td>
<td>10</td>
<td>20</td>
</tr>
</tbody>
</table>

- IEEE 802.11 standards don’t specify speed versus distance objectives.
- Different vendors will give different values, depending on environment.
- This table gives estimated values for a typical office environment.

IEEE 802.11 MAC Layer

MAC layer covers three functional areas

- reliable data delivery
- access control
- security
Reliability of Data Transfer

• A wireless LAN is subject to considerable unreliability, such as noise, interference, and other effects result in corrupted frames; even error correction codes could not help loss of many frames.

• Using reliability mechanisms at a higher layer, such as TCP, is not appropriate since timers used for retransmission are typically on the order of seconds; It is therefore more efficient to deal with errors at the MAC level.

Basic Data Transfer Mechanism

• For this purpose, IEEE 802.11 includes a frame exchange protocol.

• When a station receives a data frame from another station, it returns an acknowledgment (ACK) frame to the source station. This exchange is treated as an atomic unit, not to be interrupted by a transmission from any other station.

• If the source does not receive an ACK within a short period of time, either because its data frame was damaged or because the returning ACK was damaged, the source retransmits the data frame.
Medium Access

• Wireless LANs cannot implement CSMA/CD since:
  — for collision detection a station must be able to send data and receive collision signals at the same time; this full duplex can mean costly stations and increased bandwidth requirements
  — collision may not be detected because of the hidden station problem
  — The distances between stations can be great and signal fading could prevent a station at one end from hearing a collision at the other end.

CSMA with Collision Avoidance

• To avoid collisions on wireless networks IEEE 802.11 defines Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) procedure.
• Wireless LAN MAC’s sublayer called Distributed Coordination Function (DCF) performs basic CSMA/CA.
• Point Coordination (PCF) sublayer is implemented on the top of DCF. Its operations consists of polling by centralized polling master (point coordinator).
• PCF is implemented only in very few hardware devices as it is not part of the WiFi Alliance’s interoperability standard.
• CSMA/CA uses two strategies:
  — interframe space – IFS,
  — contention window.
CSMA/CA Access Logic

- A station with a data frame to transmit senses the medium. If the medium is idle, it waits to see if the medium remains idle for a time equal to IFS. If so, the station may transmit immediately.
- If the medium is busy (either because the station initially finds the medium busy or because the medium becomes busy during the IFS idle time), the station defers transmission and continues to monitor the medium until the current transmission is over.
- Once the current transmission is over, the station delays another IFS. If the medium remains idle for this period, then the station starts a backoff procedure. Otherwise it waits for this new transmission is over and repeats this step.
CSMA/CA Access (continued)

- The station backs off a random amount of time while contiguously sensing the medium. 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, which is determined by the absence of an acknowledgement, then it is assumed that a collision has occurred, and the data frame will be retransmitted.
- To ensure that backoff maintains stability, the binary exponential backoff, described in the context of CSMA/CD, is also used here.

Backoff Procedure Details

- To begin the backoff procedure, the station chooses a random number $W$ (according to the exponential backoff) and defines the contention window as an amount of time equal to $W$ time slots, and sets its timer to that amount.
- The station senses the channel after each time slot and it decrease the timer each time it finds channel idle. If the channel is busy, the station just holds the timer (doesn't resets it) and resumes the timer when the channel is senses idle.
- Transmission of the data frame shall commence when the timer reaches zero. Note that the timer reaches zero and transmission starts when the channel is idle.
Priority IFS

- DCF includes different IFSs to act as a priority scheme
- DIFS (DCF IFS) used for most traffic contending for access; it is longest of three delays; IFS used so far has been DIFS.
- SIFS (Short IFS) for all immediate response actions; it is shortest and gives highest priority and it used when a sender has one of following frames to send:
  - ACK frame: a station is responding with an ACK frame, when a data frame addressed only to itself (not a broadcast) is received
  - CTS frame: a station can ensure that its data frame will get through by first issuing a small RTS frame, and the receiver should immediately respond with a CTS frame
- PIFS (PCF IFS) is used by polling coordinator; not to be discussed.

Timing Diagram of DCF CSMA/CA Access

DIFS in this figure is ISF we used earlier

Figure 17.7a
Data Frame Retransmission

- A station that receives the data frame should return an ACK.
- ACK frame is a special frame that is transmitted following the end of SIFS period starting when the data transmission ended.
- If the data transmission is unsuccessful, which is determined by the absence of an acknowledgement by the end of ACK time-out interval, then the station will make retransmission attempt.
- For each retransmission attempt, the number of slots in the contention window changes according to binary exponential back-off strategy.
- Binary exponential backoff provides a means of handling even a heavy load, since repeated failed attempts to transmit result in longer and longer times, which helps to smooth out the load.
- It is important to recognize the need for statistical independence among the random number generators among the stations.

IEEE802.11 RTS/CTS Exchange

- CSMA/CA can optionally be supplemented by the exchange of a Request to Send (RTS) frame sent by the sender, and a Clear to Send (CTS) frame sent by the intended receiver, alerting all nodes within range of the sender, the receiver, or both, to keep quiet for the duration of the main packet. This is known as the IEEE 802.11 RTS/CTS exchange.
- A node wishing to send data initiates the process by sending RTS frame. The destination node replies with a CTS. Any other node receiving the RTS or CTS frame should refrain from sending data for a given time.
- This mechanism used by the 802.11 wireless networking protocol provides for efficient transmission of large amount of data frames between two devices, as well as reduces frame collisions introduced by the hidden terminal problem.
More than one Data/ACK exchange can occur before NAV period expires, thus providing transfer of larger amounts of data. Note that data frames and ACK are send after SIFS, and without contention for the channel.

Network Allocation Vector - NAV

How do other stations defer sending their data if one station acquires access? In other words, how is the collision avoidance aspect of this protocol accomplished?

The key is a feature called NAV.

When a station sends an RTS (or CTS) frame, it includes the duration of time that it needs to occupy the channel. The stations that are affected by this transmission create a timer called a network allocation vector (NAV), that shows how much time must pass before these stations are allowed to check the channel for idleness.

Each time a station accesses the system and sends an RTS (or CTS) frame, other stations start their NAV. In other words, each station, before sensing the physical medium to see if it is idle, first checks its NAV to see if it has expired.
Virtual Carrier Sensing

- RTS/CTS is a method to implement *virtual carrier sensing* in CSMA/CA. By default, 802.11 relies on *physical carrier sensing*, which is known to suffer from the hidden terminal problem.
- The low RTS/CTS frame size threshold is 2347 bytes. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold.
- If the frame size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. Otherwise, the data frame gets sent instead of the RTS.

Collision During Handshake

- Sending RTS frame follows the same rules as for data frame.
- What happens if there is collision during the time when RTS or CTS control frames are in transition, often called the handshaking period?
- Two or more stations may try to send RTS frames at the same time. These control frames may collide. However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.
- The back-off strategy is employed, and the sender tries again.
Hidden Station Problem

- Station B has a transmission range shown by the left oval and every station in this range can hear any signal transmitted by B; station C is outside the transmission range of B;
- Station C has a transmission range shown by the right oval and every station in this range can hear any signal transmitted by station C; station B is outside the transmission range of C.
- Station A is in the area covered by both B and C and it detects collision when B and C are simultaneously transmitting.

Hidden Station Problem (continued)

- Assume that station B is sending data to station A.
- In the middle of this transmission, station C also has data to send to station A. However, station C is out of B’s range and transmissions from station B cannot reach station C.
- Therefore station C thinks the medium is free and it starts sending data to station A, which results in a collision at station A, because station A is receiving data from both B and C.
- In this case, we say that stations B and C are hidden from each other with respect to station A.
- Hidden stations can reduce the capacity of the network because of the possibility of collision.
- Note that if station C is sending to a station not in station B range, its receiving station will not be affected, but station A will still have collision if station B is sending to station A at the same time.
Preventing Hidden Station Problem

- RTS frame from station B reaches station A, but not station C.
- However, because both station B and station C are within the range of station A, CTS frame, which also contains the duration of data transmission from B to A reaches stations B and C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

Exposed Station Problem

- Station refrains from using a channel even when it is available.

- Station A is transmitting to station B, while station C has some data to send to station D, which can be sent without interfering with the transmission from station A to station B.
- However, station C is exposed to transmission from station A; it hears what station A is sending and thus refrains from sending. In other words, station C is too conservative and wastes the capacity of the channel.
IEEE 802.11 RTS/CTS mechanism could help solve exposed station problem as well, only if the stations are synchronized and packet sizes and data rates are the same for both the transmitting stations.

- When a station hears an RTS from a neighboring station, but not the corresponding CTS, then this station can deduce that it is an exposed station and is permitted to transmit to other neighboring stations.

- If the stations are not synchronized (or if the packet sizes are different or the data rates are different) the problem may occur that the sender will not hear the CTS or the ACK during the transmission of data of the second sender.
• RTS/CTS mechanism eliminates a hidden station problem, and helps solving one type of the exposed station problem, but it may also introduce another form of the exposed station problem.
• Assume that station A wants to transmit to station B and station A sends an RTS and waits for station B to send a CTS.
• Suppose that station D wants to transmit data to station C, and D transmits an RTS to C just before A sends the RTS to B.
• After receiving the RTS from D, C transmits a CTS. This CTS is heard by B upon which B is prevented from sending the CTS to A.
• Therefore, any transmission from a node within the area Y to a node within area X will prevent A from transmitting data to B, although simultaneous transmissions from area Y to area X would not have interfered with transmission from A to B.
• Stations in the region Y are the exposed stations for the station pair A/B.

---

**Hidden Station vs. Exposed Station**

• Hidden station: an unsuccessful transmission results from collision between a transmission originated by a station A which cannot hear on-going transmissions to its corresponding station B. The probability of such a collision is proportional to the total number of stations hidden from station A.
• Exposed station: an unsuccessful transmission results from station A being prevented from transmitting, because its corresponding station B is unable to send a CTS. The probability of this is proportional to the number of exposed stations to pair A/B.
• Both lead to degradation of a node's throughput.
IEEE 802.11 MAC Frame Format

- **FC** – Frame Control indicates the frame type and subtype (e.g. control, management, data), flags *To DS* and *From DS*, etc.
- **D/I** – Duration/Connection indicates the time (in µsec) the channel will be allocated for successful transmission.
- **Four addresses** are the source address and the destination address, the transmitter address and the receiver address; not all are always used.
- **SC** – Sequence Control defines the sequence number to be used in flow control and to facilitates fragmentation/reassembly.
- **Frame Body** contains between 0 and 2312 bytes of information depending on type and subtype.

![IEEE 802.11 MAC Frame Format](image)

IEEE 802.11 Addressing Mechanisms

- The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, *To DS* and *From DS*.
- Each flag can be either 0 or 1, resulting in four different situations. The interpretation of the four addresses (address 1 to address 4) in the MAC frame depends on the value of these flags.

<table>
<thead>
<tr>
<th>To DS</th>
<th>From DS</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Destination</td>
<td>Source</td>
<td>BSS ID</td>
<td>N/A</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Destination</td>
<td>Send AP</td>
<td>Source</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Receive AP</td>
<td>Source</td>
<td>Destination</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Receive AP</td>
<td>Send AP</td>
<td>Destination</td>
<td>Source</td>
</tr>
</tbody>
</table>
• **Case 1:** In this case, $To \ DS = 0$ and $From \ DS = 0$. This means that the frame is not going to a distribution system ($To \ DS = 0$) and is not coming from a distribution system ($From \ DS = 0$). Thus, the frame is going from one station in the BSS to another without passing through the distribution system. Note that this BSS’s AP could be involved in the transmission as a relay and its address will be in Address 3 field. The ACK frame should be sent to the original sender.

• **Case 2:** In this case, $To \ DS = 0$ and $From \ DS = 1$. This means that the frame is coming from a distribution system ($From \ DS = 1$). Thus, the frame is coming from AP and going to a station. Note that Address 3 field contains the address of the original sender of the frame (in another BSS). The ACK should be sent to the AP.
**IEEE 802.11 Addressing Mechanisms (cont.)**

- **Case 3:** In this case, $To\ DS = 1$ and $From\ DS = 0$. This means that the frame is going to a distribution system ($To\ DS = 1$). Thus, the frame is going from a station to AP. Note that Address 3 field contains the final destination of the frame (in another BSS). The ACK should be sent to the original station.

- **Case 4:** In this case, $To\ DS = 1$ and $From\ DS = 1$. This is the case in which the distribution system is also wireless. The frame is going from one AP to another AP in a wireless distribution system. We do not need to define addresses if the distribution system is a wired LAN because the frame in these cases has the format of a wired LAN frame (Ethernet, for example). Here, we need four addresses to define the original sender, the final destination, and two intermediate APs.

---

**Authentication, Deauthentication and Privacy**

- Authentication is used to establish the station identity.
- Wired LANs assume physical connection gives authority to use LAN, but that is not a valid assumption for wireless LANs.
- 802.11 supports several authentication schemes:
  - from relatively insecure handshaking to public-key encryption.
  - Deauthentication invoked whenever an existing authentication is to be terminated.
- Privacy is used to prevent messages being read by others
  - 802.11 allows optional use of encryption
- Original WEP (Wired Equivalent Privacy) security features were weak.
- Subsequently 802.11i and WPA (WiFi Protected Access) alternatives evolved giving better security.
Wireless LANs: Summary

- Wireless LAN alternatives
- IEEE 802.11 architecture and services
- 802.11 Media Access Control
- 802.11 Physical Layers
  - 802.11, 802.11a, 802.11b, 802.11g, 802.11n
- Security considerations

Bluetooth

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, desktop computers, laptops, cameras, printers, coffee makers, etc.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, called gadgets, find each other and make a network called a piconet.
- A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability.
- A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.
# Bluetooth Applications

Bluetooth technology has many applications, such as:

- peripheral devices such as a wireless mouse or keyboard can communicate with the computer
- home security devices can use this technology to connect different sensors to the main security controller
- monitoring devices can communicate with sensor devices in a small health care center
- conference attendees can synchronize their laptop computers at a conference.

Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard; it defines a wireless personal-area network operable in an area the size of a room or a hall.

# Bluetooth Band

A Bluetooth device has a built-in short-range radio transmitter; the current data rate is 1 Mbps with a 2.4-GHz bandwidth.

- This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth LANs.
- Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.
- Bluetooth FHSS hops 1600 times per second.
- Thus, each device changes its modulation frequency 1600 times per second and a device uses a frequency for only 625 μs (1/1600 s) before it hops to another frequency.
- To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering)
**Piconet**

- A Bluetooth network is called a **piconet**, or a small net.
- A piconet can have up to eight stations, one of which is called the **primary**; the rest are called **secondaries**.
- All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

![Diagram of Piconet](image)

**Scatternet**

- Piconets can be combined to form what is called a **scatternet**.
- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.

![Diagram of Scatternet](image)
**Cellular Wireless Networks**

- These are WAN wireless networks (not LANs)
- Cellular wireless is a key technology for mobiles, wireless nets developed to increase mobile phone capacity
- It is based on multiple low power transmitters and each area divided into cells
  - each with own antenna
  - each with own range of frequencies
  - served by base station (BS)
  - adjacent cells use different frequencies to avoid crosstalk
- Two types of cellular channels
  - control channels used to set up, maintain calls and establish relationship between mobile unit and nearest BS
  - traffic channels carry voice and data

**Overview of Cellular System**

![Figure 14.15](image)

Figure 14.15
Generations of Cellular Wireless Networks

- **First generation** (original cellular telephone networks)
  - analog voice channels, using circuit switching
  - early 1980s in North America, but replaced by new systems

- **Second generation** provide higher quality signals and overall greater capacity
  - digital traffic channels, still using circuit switching
  - Encryption & error detection and correction
  - channel access
    - time division multiple access (TDMA)
    - code division multiple access (CDMA)

- **Third generation (3G)** supports, in addition to voice channels using circuit switching (as the second generation), also multimedia, data, and video using packet switching.

- **Fourth generation (4G)** further improvements in packet switching.