Wireless LANs

Overview of Wireless LANs

- use wireless transmission medium
- issues of high prices, low data rates, occupational safety concerns, & licensing requirements now addressed
- key application areas:
  - LAN extension
  - cross-building interconnect
  - nomadic access
  - ad hoc networking
Single Cell LAN Extension

Multi Cell LAN Extension
Cross-Building Interconnect

- connect LANs in nearby buildings
- point-to-point wireless link
  - Not a LAN per se
- connect bridges or routers

Nomadic Access

- link LAN hub & mobile data terminal
  - laptop or notepad computer
  - enable employee to transfer data from portable computer to server
- also useful in extended environment such as campus or cluster of buildings
  - users move around with portable computers
  - may wish access to servers on wired LAN
Infrastructure Wireless LAN

(a) Infrastructure Wireless LAN

Ad Hoc Networking

- temporary peer-to-peer network
Wireless LAN Requirements

- throughput - efficient use wireless medium
- no of nodes - hundreds of nodes across multiple cells
- connection to backbone LAN - using control modules
- service area - 100 to 300 m
- low power consumption - for long battery life on mobiles
- transmission robustness and security
- collocated network operation
- license-free operation
- handoff/roaming
- dynamic configuration - addition, deletion, and relocation of end systems without disruption to users

Technology

- infrared (IR) LANs
  - individual cell of IR LAN limited to single room
  - IR light does not penetrate opaque walls
- spread spectrum LANs
  - mostly operate in ISM (industrial, scientific, and medical) bands
  - no Federal Communications Commission (FCC) licensing is required in USA
- narrowband microwave
  - microwave frequencies but not use spread spectrum
  - some require FCC licensing
Infrared LANs

- constructed using infrared portion of spectrum
- strengths
  - spectrum virtually unlimited hence high rates possible
  - unregulated spectrum
  - infrared shares some properties of visible light
    - reflection covers room, walls isolate networks
  - inexpensive and simple
- weaknesses
  - background radiation, e.g. sunlight, indoor lighting
  - power limited by concerns for eye safety and power consumption

Transmission Techniques

- directed-beam IR
  - point-to-point links
  - range depends on power and focusing
  - for indoor use can set up token ring LAN
  - IR transceivers positioned so data circulates in ring
- omnidirectional
  - single base station with line of sight to other stations
  - acts as a multiport repeater
  - other stations use directional beam to it
- diffused configuration
  - stations focused / aimed at diffusely reflecting ceiling
**Spread Spectrum LAN Configuration**

- usually use multiple-cell arrangement
- adjacent cells use different center frequencies
- configurations:
  - hub
    - connected to wired LAN
    - connect to stations on wired LAN and in other cells
    - may do automatic handoff
  - peer-to-peer
    - no hub
    - MAC algorithm such as CSMA used to control access
    - for ad hoc LANs

**Spread Spectrum LANs Transmission Issues**

- licensing regulations differ between countries
- USA FCC allows in ISM band:
  - spread spectrum (1W), very low power (0.5W)
    - 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
### IEEE 802 Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>Medium access control (MAC); for common MAC for WLAN applications</td>
</tr>
<tr>
<td></td>
<td>Physical layer: Infrared at 1 and 2 Mbps</td>
</tr>
<tr>
<td></td>
<td>Physical layer: 2.4-GHz IEEE 802 at 1 and 2 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11a</td>
<td>Physical layer: 5.8-GHz IEEE 802 at 5.5 and 11 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11b</td>
<td>Bridge operation on 802.11 MAC layer</td>
</tr>
<tr>
<td></td>
<td>Physical layer: Extended operation of 802.11b DSS to one regulatory domain (countries)</td>
</tr>
<tr>
<td>IEEE 802.11c</td>
<td>Bridge operation on 802.11b MAC layer</td>
</tr>
<tr>
<td></td>
<td>Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11d</td>
<td>Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11e MAC: Enhance to improve quality of service and enhance security mechanisms</td>
</tr>
<tr>
<td>IEEE 802.11f</td>
<td>Recommended practices for multireader access point</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11g MAC: Enhance to add indoor and outdoor channel selection to improve spectrum and transmit power management</td>
</tr>
<tr>
<td>IEEE 802.11h</td>
<td>Physical layer: Extend 802.11 to data rates greater than 2 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11i</td>
<td>Radio resource measurements enhancements to provide interfaces to higher layers for radio and network management services and to improve spectrum and transmit power management</td>
</tr>
<tr>
<td>IEEE 802.11j</td>
<td>Accessibility of 802.11-1999 standard with technical and editorial corrections</td>
</tr>
<tr>
<td>IEEE 802.11k</td>
<td>Physical layer: Enhancements to enable higher throughputs</td>
</tr>
<tr>
<td>IEEE 802.11l</td>
<td>Physical layer: Extend 802.11 to data rates greater than 2 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11m</td>
<td>MAC: Enhance security and authentication mechanisms</td>
</tr>
<tr>
<td>IEEE 802.11n</td>
<td>Recommended practices for the Evaluation of 802.11 wireless performance</td>
</tr>
<tr>
<td>IEEE 802.11o</td>
<td>Physical layer: Enhancing with external networks</td>
</tr>
</tbody>
</table>

### IEEE 802 Terminology

<table>
<thead>
<tr>
<th>Access point (AP)</th>
<th>Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic service set (BSS)</td>
<td>A set of stations controlled by a single coordination function</td>
</tr>
<tr>
<td>Coordination function</td>
<td>The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs</td>
</tr>
<tr>
<td>Distribution system (DS)</td>
<td>A system used to interconnect a set of BSSs and integrated LANs to create an ESS</td>
</tr>
<tr>
<td>Extended service set (ESS)</td>
<td>A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs</td>
</tr>
<tr>
<td>MAC protocol data unit (MPDU)</td>
<td>The unit of data exchanged between two peer MAC entities using the services of the physical layer</td>
</tr>
<tr>
<td>MAC service data unit (MSDU)</td>
<td>Information that is delivered as a unit between MAC users</td>
</tr>
<tr>
<td>Station</td>
<td>Any device that contains an IEEE 802.11 conformant MAC and physical layer</td>
</tr>
</tbody>
</table>
IEEE 802.11 - BSS

- basic service set (BSS) building block
- may be isolated
- may connect to backbone distribution system (DS) through access point (AP)
- BSS generally corresponds to cell
- DS can be switch, wired network, or wireless network
- have independent BSS (IBSS) with no AP
Extended Service Set (ESS)

- possible configurations:
  - simplest is each station belongs to single BSS
  - can have two BSSs overlap
  - a station can participate in more than one BSS
  - association between station and BSS dynamic
- ESS is two or more BSS interconnected by DS
- appears as single logical LAN to LLC

---

IEEE 802 Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Provider</th>
<th>Used to support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association</td>
<td>Distribution system</td>
<td>MSDU delivery</td>
</tr>
<tr>
<td>Authentication</td>
<td>Station</td>
<td>LAN access and security</td>
</tr>
<tr>
<td>Deauthentication</td>
<td>Station</td>
<td>LAN access and security</td>
</tr>
<tr>
<td>Dissassociation</td>
<td>Distribution system</td>
<td>MSDU delivery</td>
</tr>
<tr>
<td>Distribution</td>
<td>Distribution system</td>
<td>MSDU delivery</td>
</tr>
<tr>
<td>Integration</td>
<td>Distribution system</td>
<td>MSDU delivery</td>
</tr>
<tr>
<td>MSDU delivery</td>
<td>Station</td>
<td>MSDU delivery</td>
</tr>
<tr>
<td>Privacy</td>
<td>Station</td>
<td>LAN access and security</td>
</tr>
<tr>
<td>Reassociation</td>
<td>Distribution system</td>
<td>MSDU delivery</td>
</tr>
</tbody>
</table>
Services - Message Distribution

- distribution service
  - primary service used by stations to exchange MAC frames when frame must traverse DS
  - if stations in same BSS, distribution service logically goes through single AP of that BSS
- integration service
  - enables transfer of data between 802.11 LAN station and one on an integrated 802.x LAN

Association Related Services

- DS requires info about stations within ESS
- provided by association-related services
- station must associate before communicating
- 3 mobility transition types:
  - no transition - stationary or in single BSS
  - BSS transition - between BSS in same ESS
  - ESS transition: between BSS in different ESS
Association Related Services

- DS needs identity of destination station
  - stations must maintain association with AP within current BSS
- 3 services relate to this requirement:
  - Association - establishes initial association between station and AP
  - Reassociation - to transfer an association to another AP
  - Disassociation - by station or AP

Medium Access Control

- MAC layer covers three functional areas
  - reliable data delivery
  - access control
  - security
Reliable Data Delivery

- 802.11 physical / MAC layers unreliable
  - noise, interference, and other propagation effects result in loss of frames
  - even with error-correction codes, frames may not successfully be received
- can be dealt with at a higher layer, e.g. TCP
- more efficient to deal with errors at MAC level
- 802.11 includes frame exchange protocol
  - station receiving frame returns acknowledgment (ACK) frame
  - exchange treated as atomic unit
  - if no ACK within short period of time, retransmit

Four Frame Exchange

- can use four-frame exchange for better reliability
  - source issues a Request to Send (RTS) frame to dest
  - destination responds with Clear to Send (CTS)
  - after receiving CTS, source transmits data
  - destination responds with ACK
- RTS alerts all stations within range of source that exchange is under way
- CTS alerts all stations within range of destination
- other stations don’t transmit to avoid collision
- RTS/CTS exchange is required function of MAC but may be disabled
Media Access Control

Distributed Coordination Function

- DCF sublayer uses CSMA
  - if station has frame to send it listens to medium
  - if medium idle, station may transmit
  - else waits until current transmission complete
- no collision detection since on wireless network
- DCF includes delays that act as a priority scheme
Priority IFS Values

- **IFS (Inter Frame Space)**
- **SIFS** (short IFS)
  - for all immediate response actions (see later)
- **PIFS** (point coordination function IFS)
  - used by the centralized controller in PCF scheme when issuing polls
- **DIFS** (distributed coordination function IFS)
  - used as minimum delay for asynchronous frames contending for access
**SIFS Use**

- SIFS gives highest priority
  - over stations waiting PIFS or DIFS time
- SIFS used in following circumstances:
  - Acknowledgment (ACK)
    - station responds with ACK after waiting SIFS gap
    - for efficient collision detect & multi-frame transmission
  - Clear to Send (CTS)
    - station ensures data frame gets through by issuing RTS
    - and waits for CTS response from destination
  - Poll response
    - see Point coordination Function (PCF) discussion next

**PIFS and DIFS Use**

- PIFS used by centralized controller
  - for issuing polls
  - has precedence over normal contention traffic
  - but not SIFS
- DIFS used for all ordinary asynchronous traffic
IEEE 802.11 MAC Timing
Basic Access Method

Point Coordination Function (PCF)

- alternative access method implemented on top of DCF
- polling by centralized polling master (point coordinator)
- uses PIFS when issuing polls
- point coordinator polls in round-robin to stations configured for polling
- when poll issued, polled station may respond using SIFS
- if point coordinator receives response, it issues another poll using PIFS
- if no response during expected turnaround time, coordinator issues poll
- coordinator could lock out async traffic by issuing polls
- have a superframe interval defined
PCF Superframe Timing

IEEE 802.11 MAC Frame Format

<table>
<thead>
<tr>
<th>octets</th>
<th>FC</th>
<th>D/I</th>
<th>Address</th>
<th>Address</th>
<th>Address</th>
<th>SC</th>
<th>Address</th>
<th>Frame body</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>0 to 2312</td>
<td>4</td>
</tr>
</tbody>
</table>

FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control
Control Frames

- Power Save-Poll (PS-Poll)
  - request AP transmit buffered frame when in power-saving mode
- Request to Send (RTS)
  - first frame in four-way frame exchange
- Clear to Send (CTS)
  - second frame in four-way exchange
- Acknowledgment (ACK)
- Contention-Free (CF)-end
  - announces end of contention-free period part of PCF
- CF-End + CF-Ack:
  - acknowledges CF-end to end contention-free period and release stations from associated restrictions

Data Frames – Data Carrying

- eight data frame subtypes, in two groups
- first four carry upper-level data
- Data
  - simplest data frame, contention or contention-free use
- Data + CF-Ack
  - carries data and acknowledges previously received data during contention-free period
- Data + CF-Poll
  - used by point coordinator to deliver data & req send
- Data + CF-Ack + CF-Poll
  - combines Data + CF-Ack and Data + CF-Poll
**Data Frames – Not Data Carrying**

- other four data frames do not carry user data
- Null Function
  - carries no data, polls, or acknowledgments
  - carries power mgmt bit in frame control field to AP
  - indicates station is changing to low-power state
- other three frames (CF-Ack, CF-Poll, CF-Ack + CF-Poll) same as corresponding frame in preceding list but without data

**Management Frames**

- used to manage communications between stations and Ap's
- such as management of associations
  - requests, response, reassociation, dissociation, and authentication
### 802.11 Physical Layer

<table>
<thead>
<tr>
<th></th>
<th>802.11</th>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available bandwidth</td>
<td>83.5 MHz</td>
<td>300 MHz</td>
<td>83.5 MHz</td>
<td>83.5 MHz</td>
</tr>
<tr>
<td>Unlicensed frequency of operation</td>
<td>2.4 - 2.4835 GHz DSSS, FHSS</td>
<td>5.15 - 5.35 GHz OFDM 5.725 - 5.825 GHz OFDM</td>
<td>2.4 - 2.4835 GHz DSSS</td>
<td>2.4 - 2.4835 GHz DSSS, OFDM</td>
</tr>
<tr>
<td>Number of non-overlapping channels</td>
<td>3 (indoor/outdoor)</td>
<td>4 indoor, 4 (indoor/outdoor)</td>
<td>3 (indoor/outdoor)</td>
<td>3 (indoor/outdoor)</td>
</tr>
<tr>
<td>Data rate per channel</td>
<td>1, 2 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>1, 2, 5.5, 11 Mbps</td>
<td>1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps</td>
</tr>
<tr>
<td>Compatibility</td>
<td>802.11</td>
<td>Wi-Fi5</td>
<td>Wi-Fi</td>
<td>Wi-Fi at 11 Mbps and below</td>
</tr>
</tbody>
</table>

---

### Original 802.11 Physical Layer - DSSS

- Direct-sequence spread spectrum (DSSS)
- 2.4 GHz ISM band at 1 Mbps and 2 Mbps
- up to seven channels, each 1 Mbps or 2 Mbps, can be used
- depends on bandwidth allocated by various national regulations
  — 13 in most European countries
  — one in Japan
- each channel bandwidth 5 MHz
- encoding scheme DBPSK for 1-Mbps and DQPSK for 2-Mbps using an 11-chip Barker seq
Original 802.11 Physical Layer - FHSS

- Frequency-hopping spread spectrum
  - 2.4 GHz ISM band at 1 Mbps and 2 Mbps
  - 23 channels in Japan
  - 70 channels in USA
  - Signal hopping between multiple channels based on a pseudonoise sequence
  - 1-MHz channels are used
- Hopping scheme adjustable
- Two-level Gaussian FSK modulation for 1 Mbps
- Four-level GFSK modulation used for 2 Mbps

Original 802.11 Physical Layer – Infrared

- Omnidirectional
- Range up to 20 m
- 1 Mbps uses 16-PPM (pulse position modulation)
  - 4 data bit group mapped to one of 16-PPM symbols
  - Each symbol a string of 16 bits
  - Each 16-bit string has fifteen 0s and one binary 1
- 2-Mbps has each group of 2 data bits is mapped into one of four 4-bit sequences
  - Each sequence consists of three 0s and one binary 1
- Intensity modulation is used for transmission
802.11a

- uses 5-GHz band (different to other variants)
  - supports higher data rates, is less cluttered
- orthogonal frequency division multiplexing (OFDM)
  - multiple carrier signals at different frequencies
  - some bits on each channel
- up to 48 subcarriers modulated using BPSK, QPSK, 16-QAM, or 64-QAM
  - subcarrier frequency spacing 0.3125 MHz
  - convolutional code at rate of 1/2, 2/3, or 3/4 provides forward error correction
  - combination of modulation technique and coding rate determines data rate

802.11a Physical Frame
802.11b

- extension of 802.11 DS-SS scheme
  - with data rates of 5.5 and 11 Mbps
- chipping rate 11 MHz
  - same as original DS-SS scheme
  - Complementary Code Keying (CCK) modulation gives higher data rate with same bandwidth & chipping rate
  - also Packet Binary Convolutional Coding (PBCC) for future higher rate use

11-Mbps CCK Modulation Scheme
802.11g

- higher-speed extension to 802.11b
- operates in 2.4GHz band
- compatible with 802.11b devices
- combines physical layer encoding techniques used in 802.11 and 802.11b to provide service at a variety of data rates
  — ERP-OFDM for 6, 9, 12, 18, 24, 36, 48, 54Mbps rates
  — ERP-PBCC for 22 & 33Mbps rates
**Data Rate vs Distance (m)**

<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>

**Access and Privacy Services - Authentication**

- authentication used to establish station identity
- wired LANs assume physical connection gives authority to use LAN
- not a valid assumption for wireless LANs
- 802.11 supports several authentication schemes
- does not mandate any particular scheme
- from relatively insecure handshaking to public-key encryption
- 802.11 requires mutually acceptable, successful authentication before association
Access and Privacy Services
Deauthentication & Privacy

- Deauthentication
  - invoked whenever an existing authentication is to be terminated
- Privacy
  - used to prevent messages being read by others
  - 802.11 allows optional use of encryption
- Original WEP security features were weak
- Subsequently 802.11i and WPA alternatives evolved giving better security

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
- Security considerations