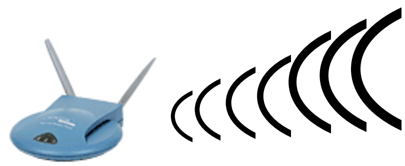
Wireless Local Area Networks

David Tipper
Associate Professor
Graduate Telecommunications and Networking Program
University of Pittsburgh



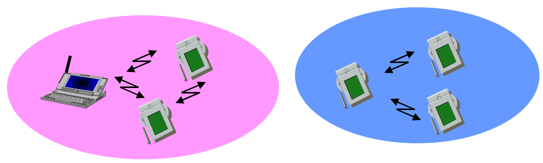
Wireless LANs

- **Wireless Local Area Networks**
  - Support communication to mobile ***data*** users via wireless channel
  - Types of WLAN

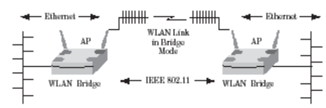
1. Infrastructure based (most popular)
   Connect users to a wired infrastructure network
   Wireless access network like cellular phone system
   IEEE 802.11, a, b, g , n, etc.
2. Ad-Hoc based networks
   - Provide peer to peer communication – mobiles communicate between each other directly
   - Rapid Deployment (conference room)
   - Bluetooth, IEEE 802.11, a, b, g, n Proprietary
3. Point – to –Point (cable replacement)

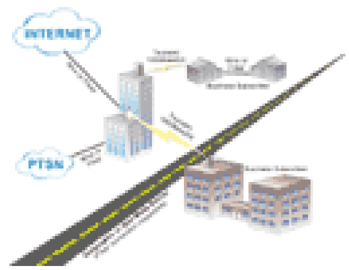
WLAN Topologies

ad-hoc based architecture

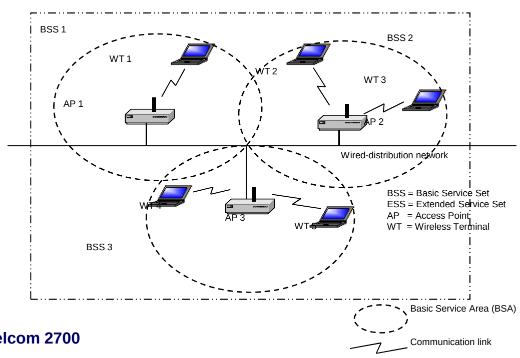


Point-to-point





Infrastructure based architecture



Wireless LANs

- Wireless LAN market
  - Medical: hospitals doctors and nurses have PDA's
  - Education: universities/colleges have campus wide network
  - Manufacturing – factories, storage, etc
  - Retail/Small Business – Superstores, grocery stores, Walmart, etc. used for inventory management
  - Public Access (Hotels, airports, coffee shops)
  - Wireless ISPs in many cities and housing developments
  - Homes – mobility in and around house
  - Market over $3 billion in 2010

Spectrum for Wireless LANS

Figure 6-5 CF Card wireless NIC

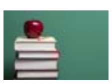
- Licensed Vs. Unlicensed
  - Private yard Vs. Public park
- Industrial Scientific and Medical bands
  - 902-928 MHz
  - 2.4 – 2.4835 GHz
  - 5.725 – 5.875 GHz
- (Unlicensed - National Information Infrastructure Bands) U-NII bands (5-6 GHz) region
  - Three bands of 100 MHz each
    - Band 1: 5.15 - 5.25 GHz
    - Band 2: 5.25 - 5.35 GHz
    - Band 3: 5.725 - 5.825 GHz
- 18-19 GHz licensed available in U.S.
- 17 GHz, 40 GHz and 60 GHz under study

Summary of (U-NII) Bands

Band of operation	Maximum Tx Power	Max. Power with antenna gain of 6 dBi	Maximum PSD	Applications: suggested and/or mandated	Other Remarks
5.15 - 5.25 GHz	50 mW	200 mW	2.5 mW/MHz	Restricted to indoor applications	Antenna must be an integral part of the device
5.25 - 5.35 GHz	250 mW	1000 mW	12.5 mW/MHz	Campus LANs	Compatible with HyperLAN II
5.725-5.825 GHz	1000 mW	4000 mW	50 mW/MHz	Community networks	Longer range in low-interference (rural) environs.

IEEE 802.11 Standard

- The project was initiated in 1990
- The first complete standard was released in 1997
- Supports two topologies: Infrastructure and Ad hoc
- Suite of standards for MAC layer and below
- Main sub-standards IEEE 802.11, a, b, g, n
- Common MAC layer for all sub-standards
- Supports different physical layers at various data rates and frequencies
  - Diffused infrared (802.11)
  - Frequency hopping spread spectrum (802.11)
  - Direct sequence spread spectrum (802.11b)
  - Orthogonal Frequency Division Multiplexing (OFDM) (802.11a, g)
  - Multiple Input Multiple Output OFDM (802.11n)
  - Is TDD for each physical layer
- Many additional sub-standards studying various aspects



IEEE 802.11 Standards

Standard	Scope
802.11	Original 1, 2 Mbps standard in 2.4 Ghz and IR frequency band
802.11a	54Mbps physical layer in 5GHz band
802.11b	11Mbps physical layer in 2.4GHz band
802.11d	Operation in additional regulatory domains
802.11e	Enhanced 802.11 Mac to support QoS in other standards (a,b,g,n)
802.11f	Inter-access point protocol (IAPP) to support roaming
802.11g	54Mbps physical layer in 2.4GHz band
802.11i	Enhanced security
802.11n	> 100Mbps physical layer using MIMO techniques
802.11s	Mesh networking
802.11u	Interworking with other networks (e.g., cellular)
802.11v	Wireless network managment

IEEE 802.11 Terminology

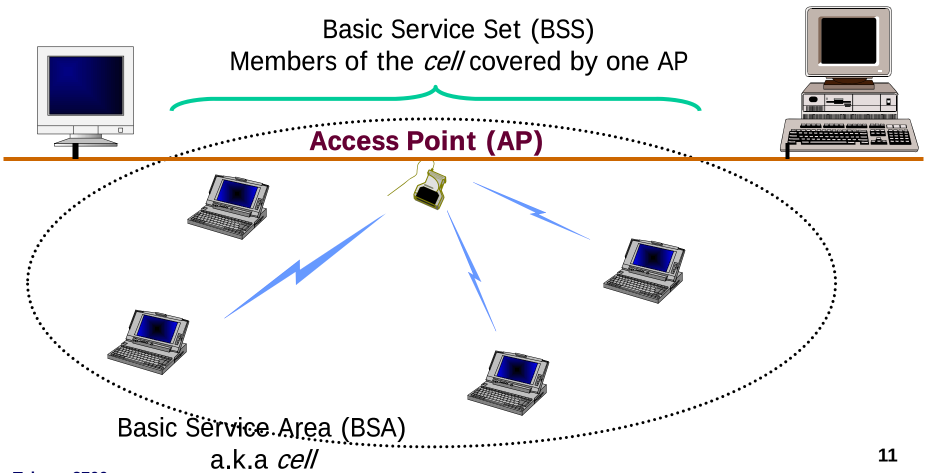
- Access Point (AP)
  - Acts as a base station for the wireless LAN and is a bridge between the wirless and wired network
- Basic Service Area (BSA)
  - The coverage area of one access point
- Basic Service Set (BSS)
  - A set of stations controlled by one access point
- Distribution system
  - The fixed (wired) infrastructure used to connect a set of BSS to create an **extended service set (ESS)**
- Portal(s)
  - The logical point(s) at which non-802.11 packets enter an ESS

Infrastructure Network Topology

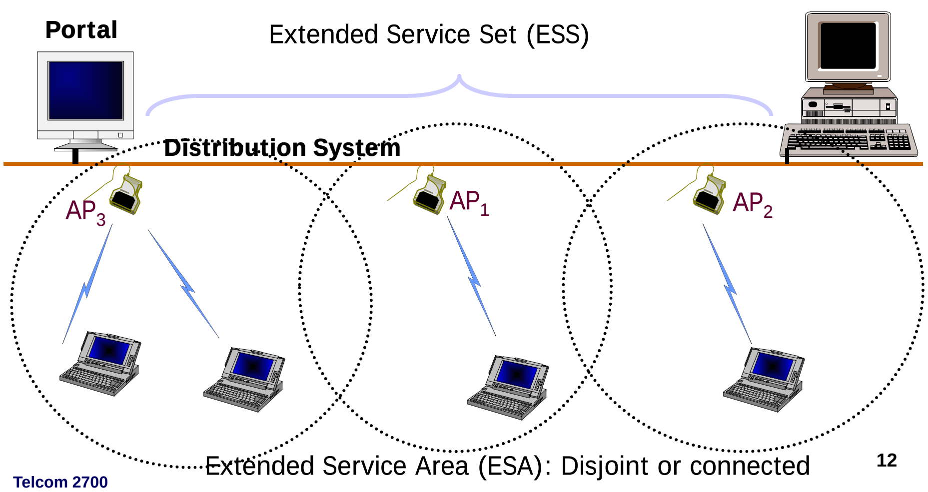
- A wired infrastructure supports communications between mobile hosts (MHs) and between MHs and fixed hosts
- Star topology

  - The BS or AP is the hub
  - Any communication from a MH to another has to be sent through the BS or AP
  - The AP manages user access to the network
  - APs typically mounted on wall or ceiling
  - AC power maybe a problem, power over Ethernet option delivers AC power over UTP Ethernet cable
- Designed for multiple APs interconnected to cover larger areas to form ESS

Infrastructure based Architecture

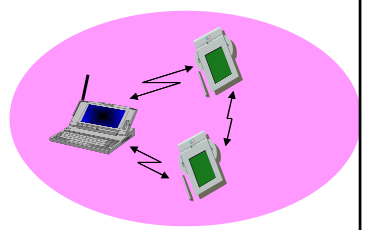


Infrastructure-based Architecture

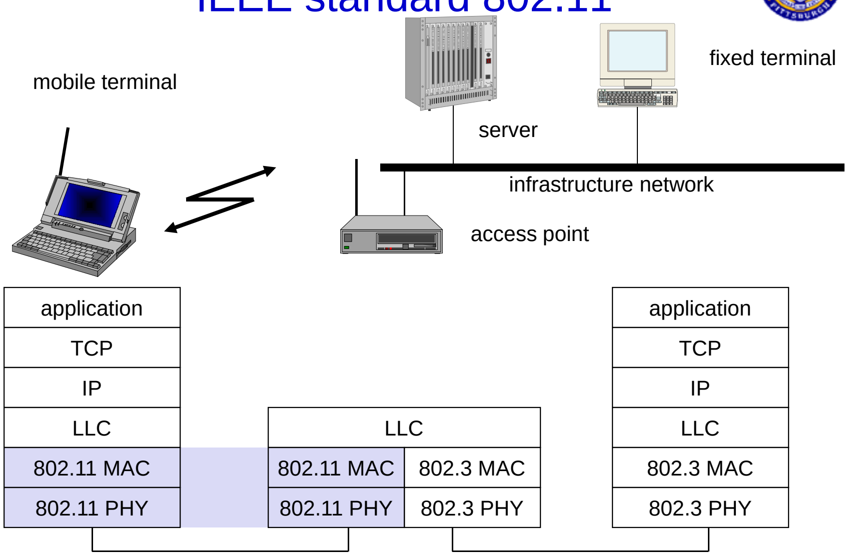


Ad hoc network topology

- Independent Basic Service Set (IBSS)
- Distributed topology
- MHs communicate between each other directly (like walkie-talkies)
- No need for a wired infrastructure
- Suitable for rapid deployment
- Use in conference rooms
- No support for multi-hop ad hoc networking - non standard freeware and proprietary systems available that support multi-hop

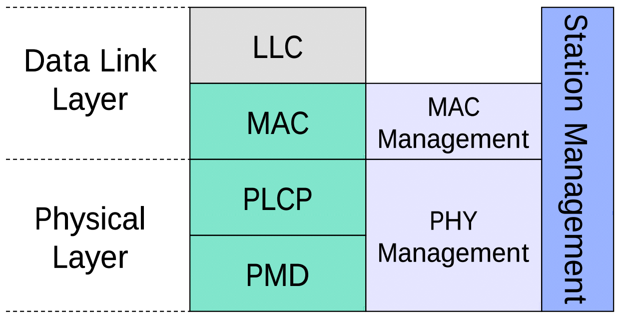


IEEE standard 802.11



IEEE 802.11 Protocol Architecture

MAC layer independent of Physical Layer
Physical varies with standard (802.11, 802.11a, etc.)
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent



The MAC Layer

- IEEE 802.11 data link layer has two sublayers
  - Logical Link Layer
    - determined by wired network interface
  - Media Access Control (MAC) layer :
    - security, reliable data delivery, access control
    - provides coordination among MHs sharing radio channel
- MAC Layer has two coordination techniques
  - Distributed Coordination Function (DCF)
    - based on CSMA/CA with randomized backoff
    - Asynchronous, best effort service
    - DCF with RTS/CTS (optional) avoids hidden terminal problem
  - Point Coordination Function (PCF)
    - Optional access mechanism
    - Provides "time bounded" service based on polling of MSs

802.11 Protocol Architecture

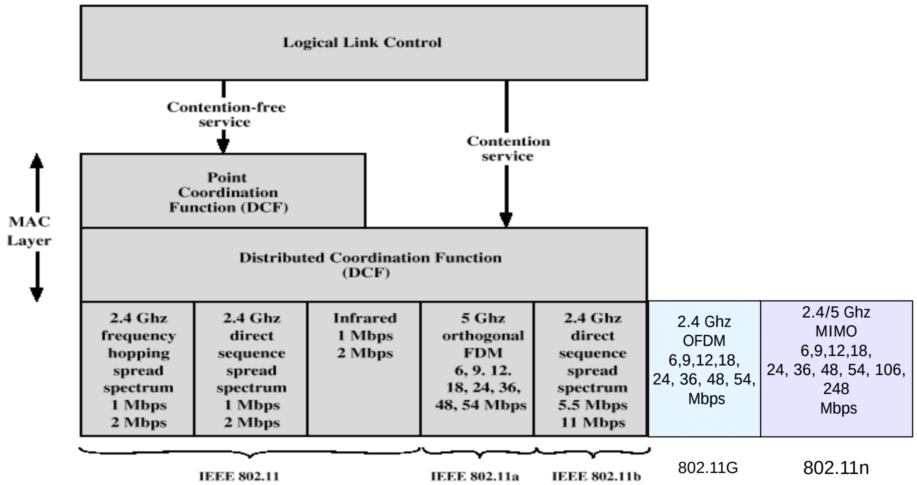


Figure 14.5 IEEE 802.11 Protocol Architecture

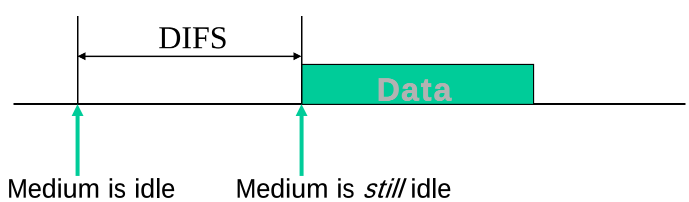
Distributed Coordination Function (DCF)

- Distributed Coordination Function (DCF)
- CSMA/CD can't be used – because can't always detect collisions
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - MSs listens to channel to see if busy
    - if busy will backoff random time before checking again
    - If idle channel for duration of interframe spacing will trasmit
  - If a collision occurs, clients wait random amount of slot time after medium is clear before retransmitting
- CSMA/CA also reduces collisions by using explicit packet acknowledgement (ACK)
  - Receiving client must send back to sending client an acknowledgement packet showing that packet arrived intact
  - If ACK frame is not received by sending client, data packet is transmitted again after random waiting time

Physical and Virtual Carrier Sensing

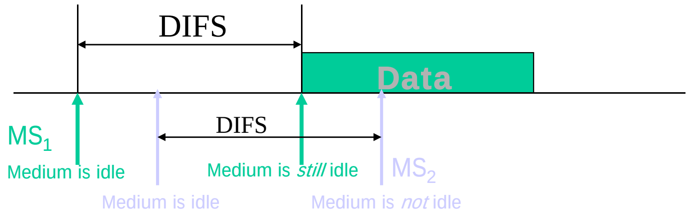
- The physical layer performs a “real” sensing of the air interface to determine if the channel is busy or idle
  - Detects carrier by RSS
- The MAC layer performs a “virtual” carrier sensing
  - Analyzes detected packets
  - The “length” in DURATOIN field in MAC control frame is used to set a network allocation vector (NAV)
  - The NAV indicates a prediction of future traffic based on duration information. In effect the amount of time that must elapse before the medium can be expected to be free again.
  - The channel will be sampled only after the NAV time elapses
- The channel is marked busy if either of the physical or virtual carrier sensing mechanisms indicate that the medium is busy

Idle Channel



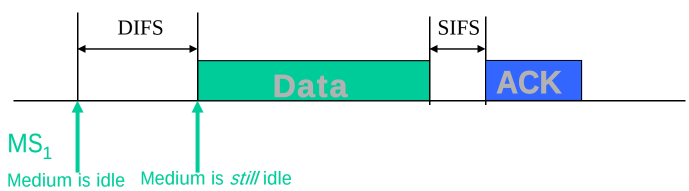
- If the medium is idle, every MS **has** to wait for a period DIFS (DCF inter-frame spacing) to send **DATA**
- After waiting for DIFS, if the medium is still idle, the MS can transmit its data frame

How does it help?



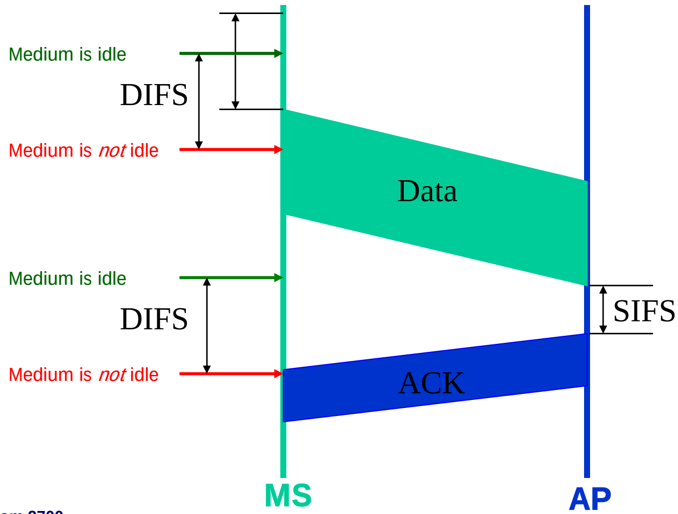
- If a second MS senses the medium to be idle after the first MS, it will find the medium to be busy after DIFS
- It will not transmit => collision is avoided

Acknowledgements

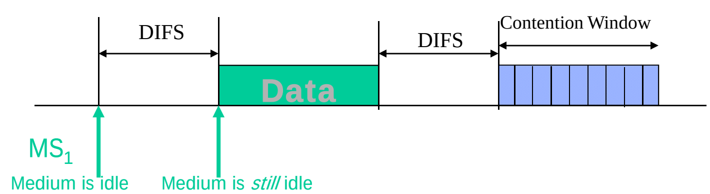


- A short inter-frame spacing (SIFS) is used
- SIFS is the ***absolute minimum*** duration that any MS should wait before transmitting anything
- It is used ONLY for acknowledgements (which will be sent by a receiving MS or AP alone)
- ACKs receive highest priority!
- ACKs will almost always be sent on time

Data Transmission And ACKs



Busy Channel



- Each MS has to still wait for a period of DIFS
- Each MS chooses a random time of **back-off** within a *contention window*
- Each MS decrements the back-off. Once the back-off value becomes zero, if the medium is idle, the MS can transmit
- The MS with the smallest back-off time will get to transmit
- All other MSs freeze their back-off timers that are “decremented” and start decrementing the timer in the next contention window from that point

Interframe Space (IFS) Values

- Short IFS (SIFS)
  - Shortest IFS
  - Used for immediate response actions (ACKs)
- Point coordination function IFS (PIFS)
  - Midlength IFS
  - Used by centralized controller in PCF scheme when polling MHs
- Distributed coordination function IFS (DIFS)
  - Longest IFS
  - Used as minimum delay of asynchronous frames contending for access

Medium Access Control Logic

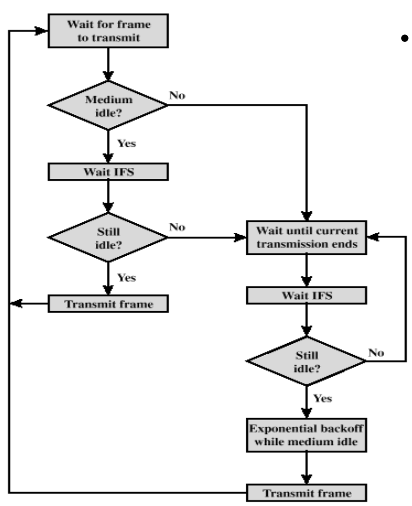
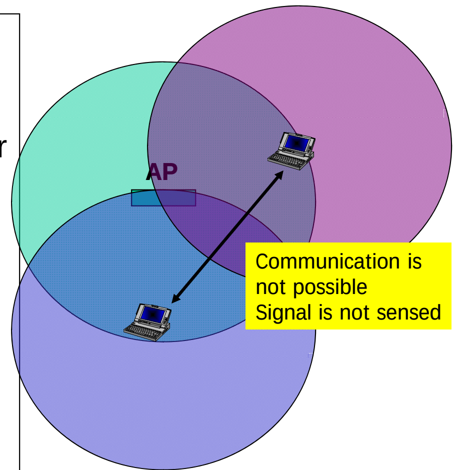


Figure 14.6 IEEE 802.11 Medium Access Control Logic

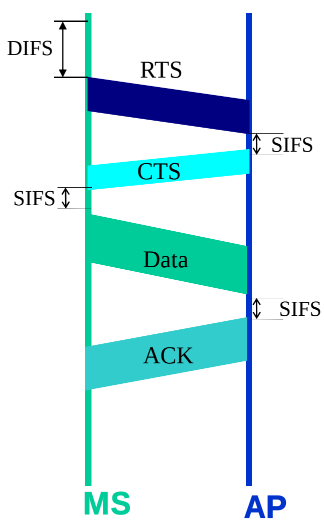
- DCF uses two Interframe space values
  1. Short IFS (SIFS)
     - Shortest IFS
     - Used for immediate response actions (ACKs)
  2. Distributed coordination function IFS (DIFS)
     - Longest IFS
     - Used as minimum delay of asynchronous frames contending for access

When do collisions occur?

- MSs have the same value of the back-off timer
- MSs are not able to hear each other because of the "hidden terminal" effect
  - MSs are not able to hear each other because of fading
- Solution: RTS/CTS
  - Also avoids excessive collision time due to long packets



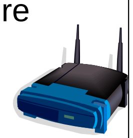
RTS/CTS Mechanism



- RTS-Request to Send (20 bytes)
- CTS-Clear to Send (14 bytes)
- They can be used only prior to transmitting data
- After successful contention for the channel, a MS can send an RTS to the AP
- It gets a CTS in reply after SIFS
- CTS is received by all MSs in the BSS
- They defer to the addressed MS while it transfers data
- If there is a collision, no CTS is received and there is contention again

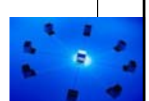
Large Frames

- Large frames that need fragmentation are transmitted sequentially without new contention
- The channel is automatically **reserved** till the entire frame is transmitted
- The sequence of events is:
  - Wait for DIFS & CW; Get access to channel
  - Send first fragment; include number of fragments in the field
  - All other MSs update their NAV based on the number of fragments
  - ACK is received after SIFS
  - The next fragment is transmitted after SIFS
  - If no ACK is received, a fresh contention period is started
  - If RTS/CTS is used it is need only for the first fragment

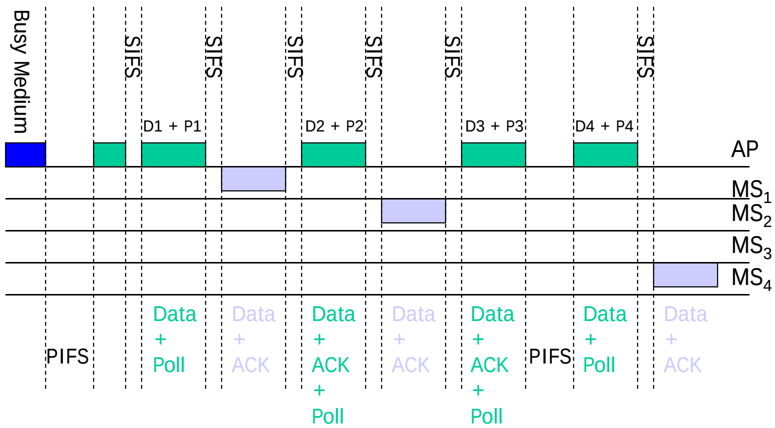


Point Coordination Function (PCF)

- Optional capability to provide “time-bounded” services
- It sits on top of DCF and needs DCF in order to successfully operate
- A point coordinator (the AP) polls each station and enables them to transmit without contention
  - Ad hoc networks cannot use this function
- Time (a super time slot) is divided into two parts
  - Contention Free Period (CFP)
  - Contention Period (CP)
- A MS must be CFP-aware to access the CFP
- Point coordination function IFS (PIFS)
  - Midlength IFS
  - Used by centralized controller in PCF scheme when polling MHs
- Replies to polling can occur after SIFS



PCF Continued



802.11 - Frame format

- Types of messages in 802.11
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

Special Frames: ACK, RTS, CTS

- Acknowledgement

ACK

bytes	2	2	6	4
ACK	Frame Control	Duration	Receiver Address	CRC

- Request To Send

RTS

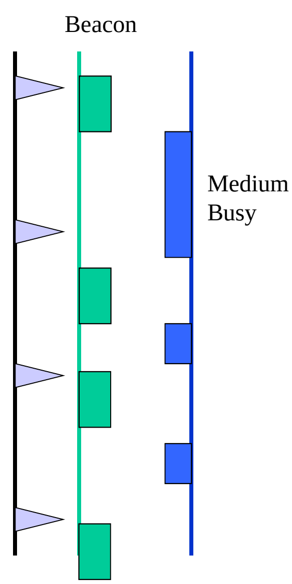
bytes	2	2	6	6	4
RTS	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

- Clear To Send

CTS

bytes	2	2	6	4
CTS	Frame Control	Duration	Receiver Address	CRC

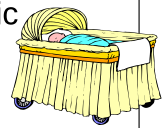
Beacon



- Beacon is a message that is transmitted quasi-periodically by the access point
- It contains information such as the ESS-ID, timestamp (for synchronization), beacon interval, traffic indication map (for sleep mode), power management, AP capabilities, roaming support, security
- Beacons are always transmitted at the expected beacon interval unless the medium is busy – in which they are the next transmission after an ACK
- RSS measurements are made on the beacon message

Power Management

- All MSs switch off the radio part and enters sleep mode when possible
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
  - Traffic is buffered at AP for sleeping MS
- At periodic intervals Beacon announces traffic indication maps
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
  - All sleeping clients change to active listening mode, check Beacon, if frames are waiting, request that frames be forward
- Typical values for TX ~400mA versus sleep mode of ~20mA



Power Management

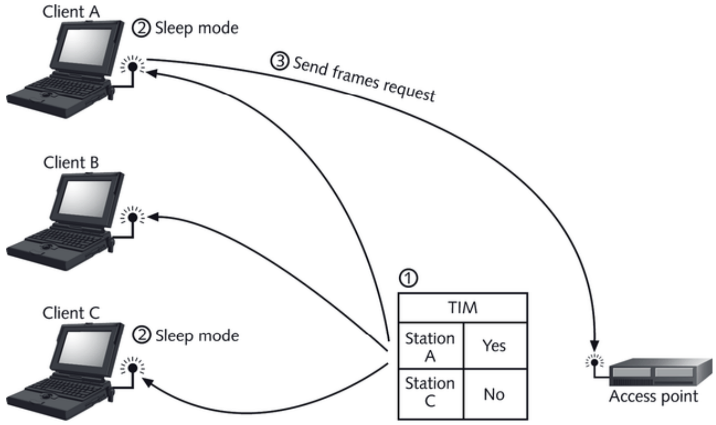


Figure 6-20 Power management

Association and Disassociation

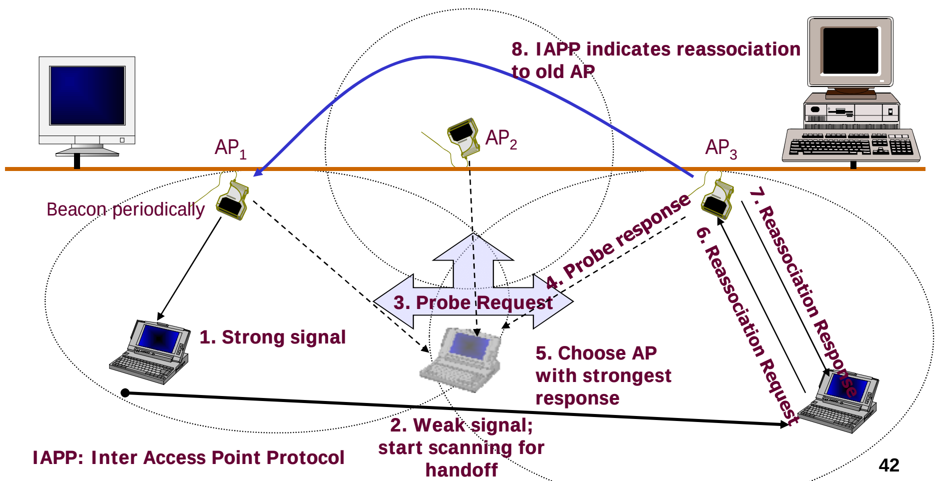
- ***Association*** is procedure by which a MS "registers" with an AP
- Only after association can a MS send packets through an AP
- After powering up a mobile listens for Beacons in a passive scanning mode and attempts to associate with appropriate AP
- A MS can be associated with only one AP
- How the association information is maintained in the distribution system is NOT specified by the standard

- The ***dissociation*** service is used to terminate an association
- It may be invoked by either party to an association (AP/MS)
- It is a notification and not a request. It cannot be refused
- MSs leaving a BSS will send a dissociation message to the AP
- ***Re-association*** – used for mobility

Mobility

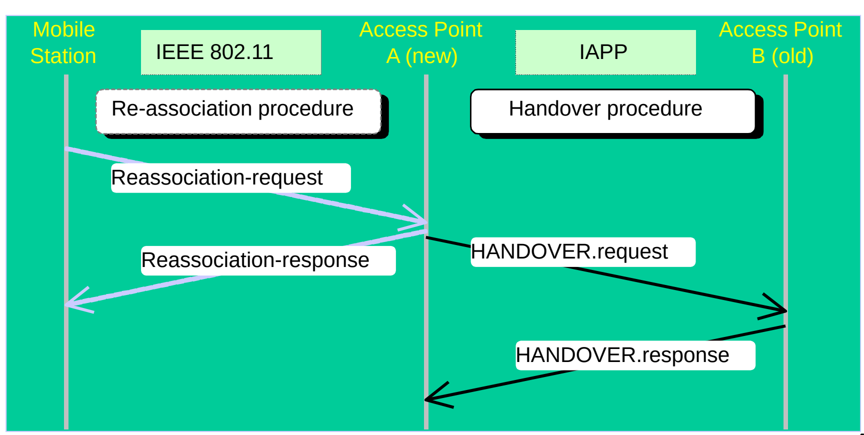
- Types
  - No Transition
    - MS is static or moving within a BSA
  - BSS Transition
    - The MS moves from one BSS to another within the same ESS (i.e., changes APs on the same network)
    - Re-association service is used when a MS moves from one BSS to another within the same ESS. It is always initiated by the MS with a Probe message
      - Probe: request from MS contains ESSID, Capabilities, Supported Rates
      - Probe Response: same as beacon except for TIM
      - After receiving probe response mobile picks new AP sends re-association request
      - Re-association Request: MS capability, listen interval, ESSID, supported rates, old AP address
      - Re-association Response: Capability, status code, station ID, supported rates
  - ESS Transition
    - The MS moves from one BSS to another BSS that is part of a new ESS
    - Upper layer connections may break (needs Mobile IP)

Handoff in 802.11



Handoff Procedure in IEEE 802.11 LANs

- 802.11f group standardized IAAP protocol for extended roaming
- APs register with a "Registration Service" in the distribution system
  - Use the IAPP-INITIATE and IAPP-TERMINATE to register and deregister
- 802.11r group fast handoff between APs – (cars, trains, etc.)



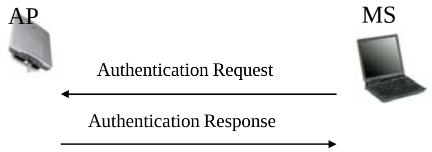
Inter-AP Protocol 802.11f

- APs register with a "Registration Service" in the distribution system
  - They use the IAPP-INITIATE and IAPP-TERMINATE to register and deregister
- An MS in 802.11 can be associated with only one AP
- When the MS sends a ***re-association*** request and obtains an association frame, the new AP sends an IAPP-MOVE-notify packet to the old AP
  - The old AP address is obtained from the registration service
  - If the registration service cannot be located, the AP will issue an IAPP-ADD-notify packet to the broadcast MAC address on the LAN
- The old AP sends an IAPP-MOVE-response packet with any context information it had for the MS and cached packets

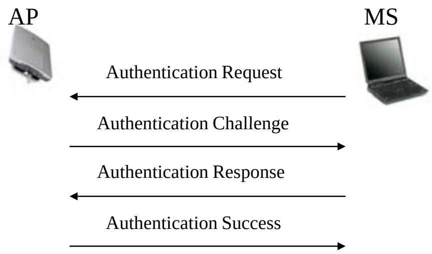
802.11 Security

- Authentication
  - Establishes identity of mobile stations to APS and vice a versa
  - Most 802.11 networks don't use any type of authentication!
    - APs accept connections from all MSs
  - Open system authentication
    - Exchange of identities using Service Set Identifier (SSID) of network
    - SSID can be advertised by AP or entered manually into mobiles
  - Shared Key authentication
    - Uses a version of challenge/response protocol
    - Either 40 or 104 bit shared key
    - Keys are static and manually configured
  - De-authentication
    - Invoked when existing authentication is terminated

WEP Authentication



Open Security Authentication



Shared Key Authentication

- Shared key authentication
  - Allow the AP to know that the MS possesses the right secret key
- Process
  - The AP sends a 128 byte arbitrary challenge text
  - The MS responds by encrypting the random message with the correct key
  - Algorithm used is RC-4 stream cypher
- The authentication is NOT mutual

802.11 Security

- Privacy
  - Prevents message contents from being read by unintended recipient
  - Uses Wired Equivalent Privacy (WEP) encryption
- WEP encryption
  - Each packet is encrypted separately
  - WEP based on RC4 stream cypher with 40 bit secret key
  - Secret key is combined with a 24 bit initialization vector (IV) that changes every packet to increase key size from 40 to 64
- Weakness
  - IV is transmitted in plaintext
  - IVs are reused too often (pseudorandom generator for IV repeats often (4-5 hours)
  - May start with same IV after shut down
- Many networks don’t even implement WEP are open!

Wired Equivalent Privacy

- WEP Encryption is fast but weak
- Publicly available tools to hack key – note keys are static
  - AIRsnort
  - WEPcrack
- Also tools to find a network
  - NetStumbler
- Tools to analyze traffic
- Can improve security using additional techniques
  - Access control list with approved MAC addresses
  - Centrailized server to authenticate users (RADIUS, EAP,etc.)

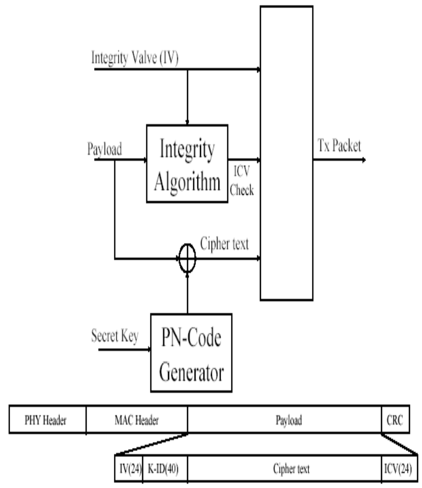
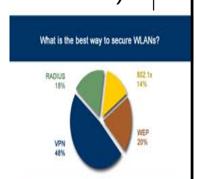


Figure 11.25: Privacy in IEEE 802.11

Improving 802.11 Security

- Wi-Fi Protected Access (WPA)
  Industry group developing techniques for existing networks
  - Use access control list with approved MAC addresses
  - Use 128 bit proprietary implementation of WEP key (doesn't scale well) with temporal key integrity protocol (prevents replay)
  - Use VPNs (IPSec or SSL)
  - Security architecture based on 802.1x and EAP (Extensible Authentication Protocol)
    - Allows many protocols within a common framework
  - Example
    - Use a RADIUS server
    - Authenticate the access point using a variation of SSL
    - Authenticate the MS using passwords (CHAP)



- IEEE 802.11i is the new security standard
  - Use AES instead of RC4 for better security
  - Push button security – easy configuration
  - WPA2 implements IEEE 802.11i – no longer backwards compatible

802.11 Physical Layers

Below MAC layer 802.11 has physical layer PHY
PHY has two sublayers
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent

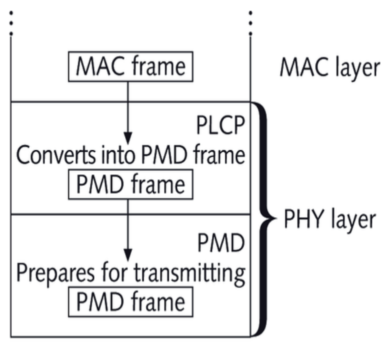


Figure 6-12 PLCP sublayer reformats MAC data

Physical Sub-Layers

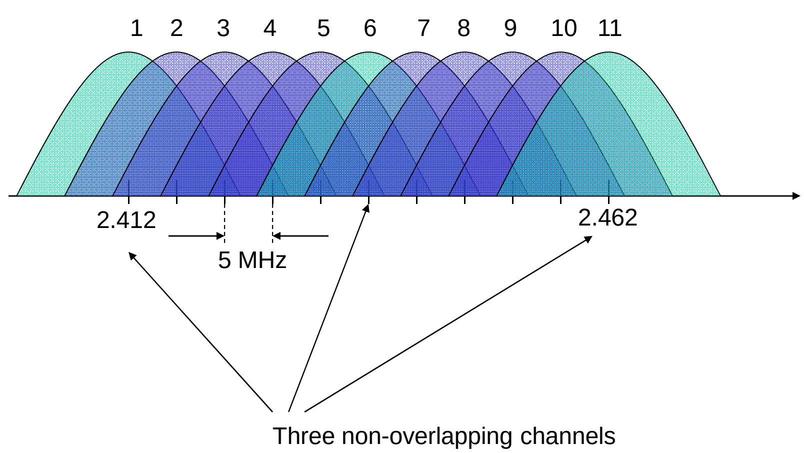
- PLCP maps the MAC frame into an appropriate PHY frame
  - Reduces MAC dependence on PMD
- PLCP frame includes information for synchronization, length of transmission, header error check, frame delimiters, etc.
- The PLCP forms the PMD frame which is different for different physical layers

- The PMD layer specifies the modulation, demodulation, and coding
- Together the two physical sub-layers provide the MAC layer a “clear channel assignment” signal to indicate the busy/idle nature of the channel
- The Physical Management layer fine tunes the channel, modulation, etc. and manages the physical layer MIBs

Physical Layer

- 802.11 Supports different physical layers at various data rates and frequencies
  - Diffused infrared (802.11)
    - PPM , 1, 2 Mbps, ARQ with CRC, 10m range, cheap
  - Frequency hopping spread spectrum (802.11)
    - Random 2.5 hops per second, GMSK modulation, ARQ with CRC, 1, 2 Mbps in 915MHz band
  - Direct sequence spread spectrum (802.11)
    - 11 bit spreading Barker code, DBPSK – 1Mbps, DQPSK – 2Mbps, ARQ with CRC, in 915MHz band
  - Direct sequence spread spectrum (802.11b)
    - Complementary Code Keying 1,2, 5.5, 11 Mbps
    - Spreading done in modulation channel symbols, error control ARQ with CRC in 20MHz band – 20MHz channels
    - Rate depends on RSS
  - Orthogonal Frequency Division Multiplexing (OFDM) (802.11a, g)
    - Parallel sub-channels with adaptive modulation based on SNR – higher data rates up to 54Mbps - 20MHz channels
  - OFDM and Multiple Input Multiple Output (802.11n)
    - Multiple antenna and receivers together with OFDM – higher data rates > 100Mbps

Channels in the 802.11b



Physical Layer 802.11a,g

- OFDM: Orthogonal Frequency Division Multiplexing

  Problem with increasing speed on WLANs is inter-symbol interference due to multipath propagation environment

- Transmits single high-rate data stream over multiple parallel low-rate data streams.

- Using several parallel sub-channels and reducing the data rate on each channel, the symbol duration in each channel is increased

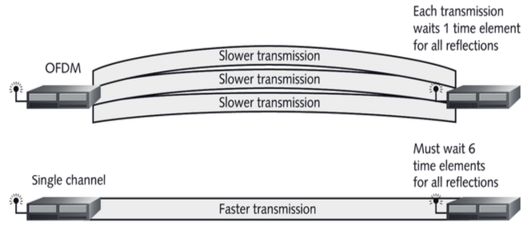


Figure 7-6 OFDM vs. single channel

802.11a Channels

- 802.11a

  specifies 8, 20 MHz channel frequencies

  each channel divided into 52 sub-channels 300KHz wide

  48 subchannels for data
  4 subchannels for error corrections

- 802.11g

  Ports 802.11a to 2GHz
  3 frequency channels

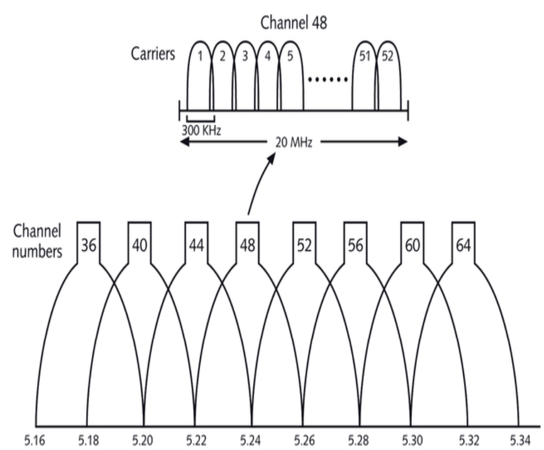


Figure 7-2 802.11a channels

Adaptive OFDM

- Modulation technique on each subcarrier is independent and depends on data rate and channel quality
- Basic idea is changing modulation scheme or allocating bits/power per subcarrier according to quality of each subchannel.
- 802.11 a, g use adaptive OFDM

AOFDM Components

Adaptive Loading/Allocation Algorithm

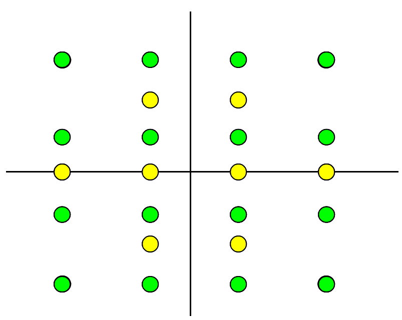
+

Set of Modulation Schemes

+

Channel Quality Estimator*

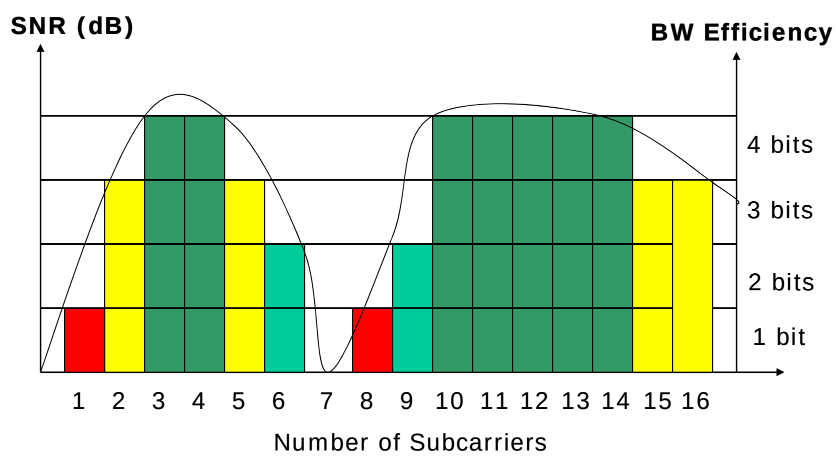
Adaptive Modulation



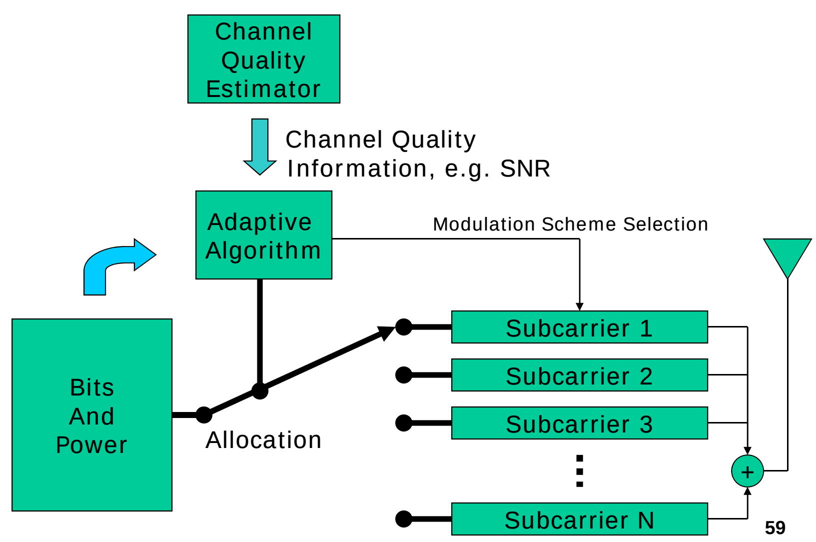
Set of Modulation Schemes:

- No transmission (0 bit)
- BPSK (1 bit/symbol)
- QAM (2 bits/symbol)
- 8-QAM (3 bits/symbol)
- 16-QAM (4 bits/symbol)

Adaptive Modulation on Parallel Channels



Adaptive OFDM Algorithm



802.11a,g

- Each subcarrier uses same modulation – adapts modulation and convolutional FEC as function of SIR to provide variety of data rates

Data rate	Modulation	FEC Coding Rate	Data bits per channel symbol
6Mbps	BPSK	1/2	24
9Mbps	BPSK	3/4	36
12Mbps	QPSK	1/2	48
18Mbps	QPSK	3/4	72
24Mbps	16QAM	1/2	96
36Mbps	16QAM	3/4	144
48Mbps	64QAM	2/3	192
54Mbps	64QAM	3/4	216

802.11n

- Approved Dec 2008
- Works in 2.4 and 5GHz bands 4x to 5x data rates of 802.11a,g ➔ 200-300Mbps
- Main Changes
  1. Physical layer uses Multiple Input Multiple Output (MIMO) OFDM
     - Has multiple antennas at each end of the channel – provides spatial diversity
     - OFDM part about the same as 802.11a,g – uses 64QAM with 5/6 FEC rate
  2. Channel Bonding
     - Combines 2 of the 20MHz 802.11a,g channels to achieve higher data rates
  3. Packet Aggregation
     - Reduce overhead by aggregating multiple packets from a single apr into a common frame.

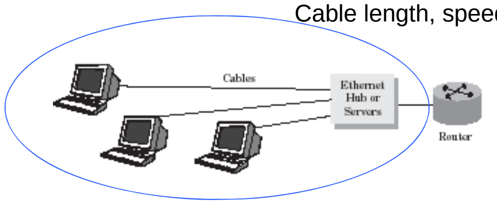
- Pre-n equipment available now based on Draft 2

Design Issues in WLAN

Compare WLAN with wired LAN

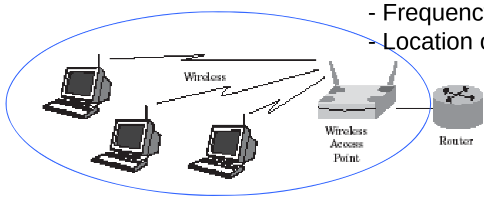
Cable length, speed

Conventional
Wired LAN



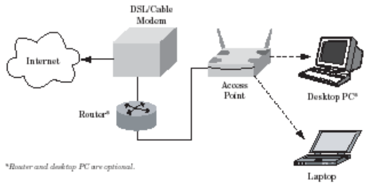
- Tx power level
- Frequency channel
- Location of access point

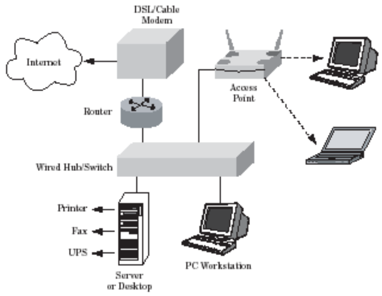
Typical
Wireless LAN



WLAN Deployment scenarios

1. Small network scenario
   Ex:
   - small office, home office (SOHO)
   - coffee shop ~17% of market in 05



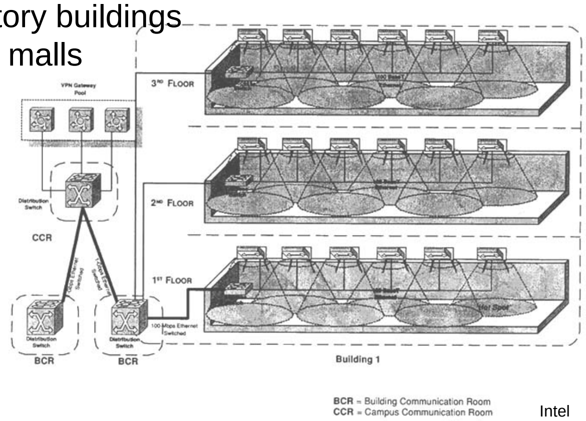


WLAN Deployment scenarios

2. Large network scenario

Ex:

- large office, warehouse
- university campus, dormitory
- corporate multistory buildings
- hotels, shopping malls



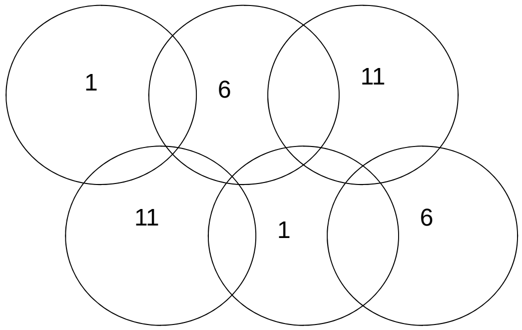
Intel

Design Issues in WLANs

- In the 2.4 GHz bands
    - For 802.11b there are 11 frequency bands that can be used
    - There are only three non-overlapping channels
    - For 802.11g there are 3 frequency bands (non-overlapping)
    - Coverage roughly 375 feet omni-directional
- In the 5 GHz bands,
    - For 802.11a there are eleven channels
    - There are 8 non-overlapping channels
    - Coverage roughly 250 feet omni-directional
- Network Planning of large networks requires
    - – Coverage Planning,
        - 3-D, depends on antenna pattern, building architecture, power level
    - – Frequency Planning
        - frequency reuse is possible and AP can support multiple channels

WLAN design approaches

- Simple rules of thumb
  - open 160m /semi-open 50m /closed 25m



  - Reuse the three no-overlapping frequencies and verify with field measurements

Coverage of AP

Radio level coverage determined by location/power level, etc.
Use *indoor* propagation models to predict coverage augment with measurements/prediction software
Max number of frequencies per AP shown in figure.

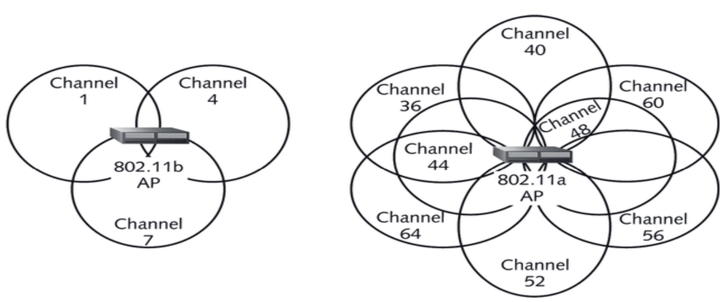


Figure 7-3 802.11b vs. 802.11a channel coverage

WLAN design issues

- Capacity considerations
- Depending on # users sharing the AP and the amount of data traffic at the time
  - Heavy vs light data transfer
- Intel suggests rules of thumb for 802.11b
  - 50 nominal users who are mostly idle and occasionally check email
  - 25 mainstream users who use a lot of email and download or upload moderately sized files
  - 10 to 20 power users who are constantly on the network and deal with large files
- 802.11a/g can support higher #users and/or traffic volume
- Design ➔ location of APs, frequency assignment and power levels.

WLAN standards

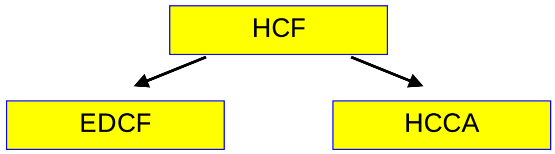
Note 802.11 has large overhead – throughput < channel rate

Table 1. IEEE 802.11 WLAN standards.

Standard	Spectrum	Maximum physical rate	Layer 3 data rate	Transmission	Compatible with	Major disadvantage	Major advantage(s)
802.11	2.4 GHz	2 Mbps	1.2 Mbps	FHSS/DSSS	None	Limited bit rate	Higher range
802.11a	5.0 GHz	54 Mbps	32 Mbps	OFDM	None	Smallest range of all 802.11 standards	Higher bit rate in less-crowded spectrum
802.11b	2.4 GHz	11 Mbps	6-7 Mbps	DSSS	802.11	Bit rate too low for many emerging applications	Widely deployed; higher range
802.11g	2.4 GHz	54 Mbps	32 Mbps	OFDM	802.11/ 802.11b	Limited number of colocated WLANs due to narrow spectrum	Higher bit rate in 2.4-GHz spectrum higher range than 802.11a
802.11n	2.4/5GHz	200-300Mbps	70-120Mbps	OFDM/MIMO			

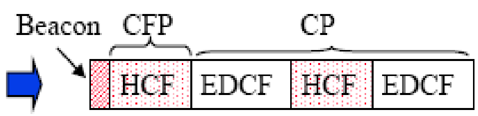
802.11e

- 802.11e standard provides a new MAC layer to provide QoS
- 802.11e defines a new Hybrid Coordination Function (HCF) that offers two modes of operation:



Enhanced DCF (EDCF) introduces different priority levels for different services.

HCF Controlled Channel Access (HCCA) is a CSMA/CA-compatible polling-based access method (improved PCF) - contention free period

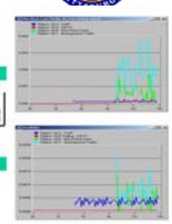


EDCF

EDCH supports four Access Categories (AC) for traffic

Channel access is controlled by four parameters:

1. Minimum contention window size (CWmin)
2. Maximum contention window size (CWmax)
3. Arbitration Interframe Space (AIFS) = variable DIFS
4. Transmission Opportunity (TXOP) - specifies the time (maximum duration) during which a wireless station can transmit a series of frames. Contention Free Bursts (CFB) allows stations to send several frames in a row without contention, if the allocated TXOP permits



AC	Application	CWmin	CWmax	AIFS
0	Best effort	CWmin	CWmax	2
1	Video probe	CWmin	CWmax	1
2	Video	(CWmin+1)/2 - 1	CWmin	1
3	Voice	(CWmin+1)/4 - 1	(CWmin+1)/2 - 1	1

HCCA

HCCA is based on a Contention-Free Period (CFP) during which the access point uses polling for controlling the traffic in the WLAN, like PCF.

The differences between HCCA and PCF are the following:

HCCA can poll stations also during the Contention Period (CP).

HCCA supports scheduling of packets based on the QoS requirements.

Stations can communicate their QoS requirements (data rate, delay, packet size…) to the access point.

New ACK rules. For instance in applications where retransmission cannot be used due to the strict delay requirements, the ACK frame need not be used.

WLANs Summary

- WLANs
  - Faster than 3G
    - 11 or 54 Mbps vs. 2 Mbps for 3G when stationary
  - Data experience matches the Internet
    - with the added convenience of mobile
  - Well established IEEE standards
  - Low cost, low barriers to entry.
  - Organizations can build own networks
  - Smaller range then cellular
- Many operators deploying WLAN as adjunct to 2.5G or 3G