King Fahd University of Petroleum & Minerals Computer Engineering Dept

COE 543 – Mobile and Wireless Networks

Term 082

Dr. Ashraf S. Hasan Mahmoud

Rm 22-148-3

Ext. 1724

Email: ashraf@kfupm.edu.sa

Lecture Contents

1.

Introduction to WLANs

- **Read** Chapter 10 – background material
  - Historical Overview of LAN industry
  - Evolution of WLAN industry
  - Wireless Home Networking Concepts

Evolution of The WLAN Industry

- Late 1970s - Gfleller, IBM Ruschlikson Laboratories in Switzerland – 1 Mb/s diffused IR – project abandoned
- Late 1970s - Ferrert, HP Palo Alto Research Laboratories – 100 kb/s DSS WLAN @ 900 MHz – experimental license agreement from FCC
- 1980s - Altair: Motorolla – 18-19 GHz
- 1985 - FCC releases ISM bands – played major role in the development of WLAN technologies
  - Conformance to band etiquette

Evolution of The WLAN Industry – cont'd

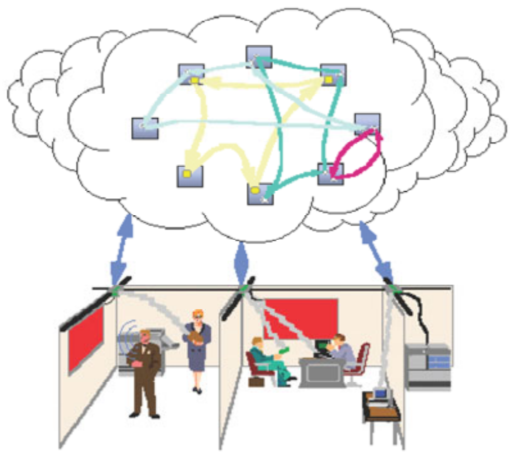
- Late 1980s – three technologies:
  - 18-19 GHz technology
  - 900 MHz technology
  - IR technology
- Late 1980 – IEEE 802.4L (later became IEEE 802.11)
  - Completed in 1997
- 1992 – WINForum initiated by Apple
  - Unlicensed bands PCS (Data-PCS activities)
- Mid 1990s – DARPA sponsored projects
  - InfoPAD – University of California, Berkeley
  - BodyLAN – BNN, Cambridge, Massachusetts
  - SUO/SAS – integration of telecom and geolocation network for modern fighting scenarios

Evolution of The WLAN Industry – cont'd

- Late 1990s – several developments
  - PCMCIA WLAN and Wireless Laptops
  - LMDS/LMCS
  - Low power PAN and Ad-Hoc networks
  - Bluetooth
  - Etc.

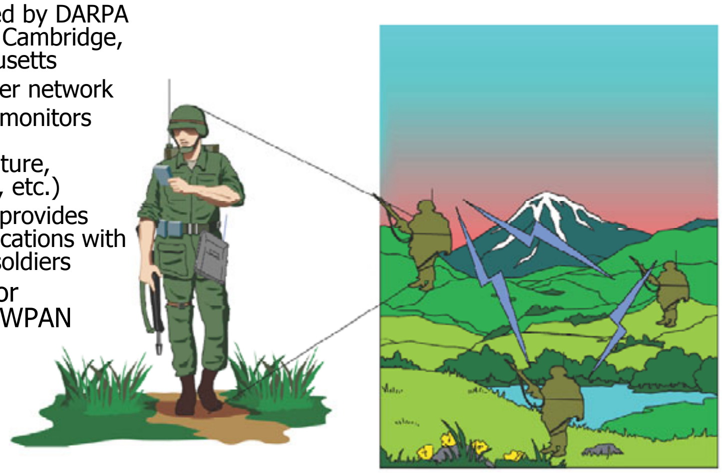
InfoPAD Project

- Figure 10.7 – Fusion of computers and communications in the InfoPAD project at the University of California, Berkeley.

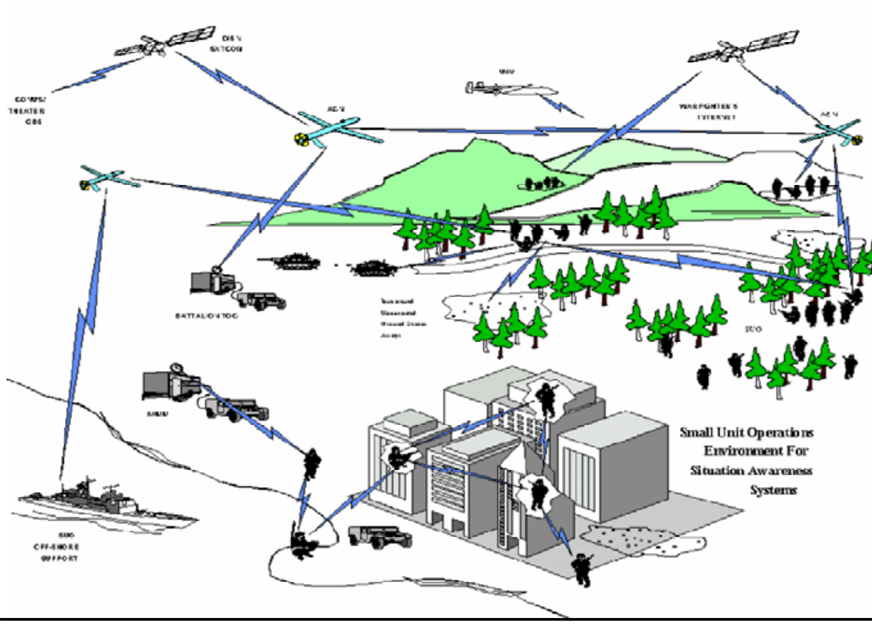


BodyLAN Project

- Figure 10.8 – BodyLAN or wearable LAN
  - Sponsored by DARPA – BBN in Cambridge, Massachusetts
  - Low-power network
  - Network monitors vital info (temperature, hearbeat, etc.)
  - Network provides communications with near by soldiers
- Motivation for IEEE802.15 WPAN



SUO/SAS Project

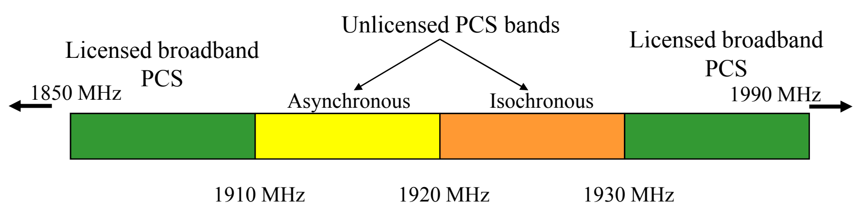


Bands of Operation

- ISM: 902-928 MHz, 2.4-2.4835 GHz, 5.725-5.875 GHz
- Unlicensed PCS: 1910-1930 MHz
- U-NII: 5.15-5.25 GHz, 5.25-5.35 GHz, 5.725-5.825 GHz

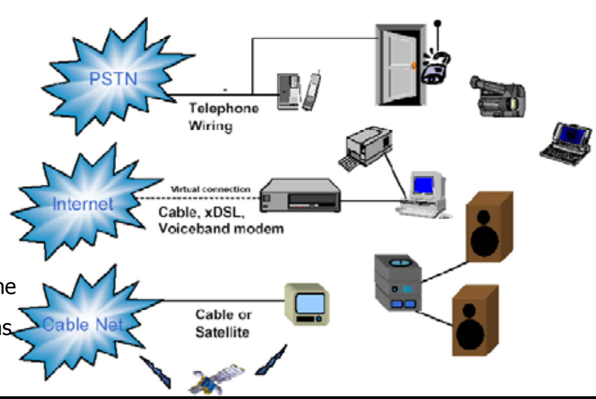
Unlicensed PCS bands

- Band Etiquettes:
    - Listen before talk (LBT protocols)
    - Low Transmitter power
    - Restricted duration of transmission



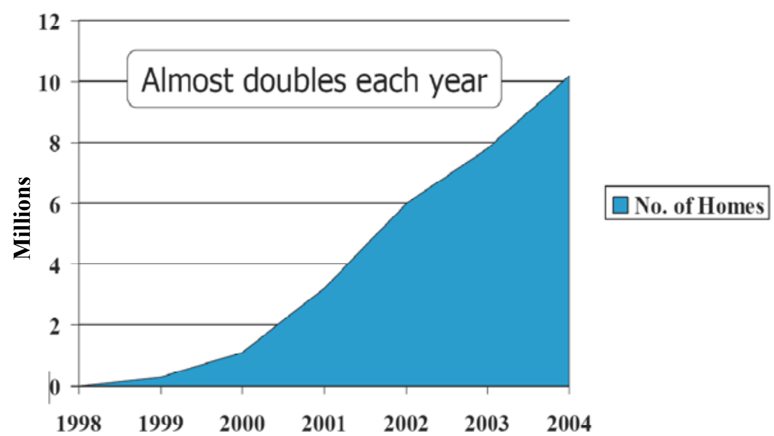
Home Networking (HAN)

- Expanding market
    - Doubling every year
- What is a HAN?
    - Infrastructure to interconnect a variety of home appliances and enable them to be accessible using the internet
- Why do we need a HAN?
    - User-friendly
    - Performance – multimedia
    - Flexible and scalable
    - Etc.
- HAN Enablers:
    1. broadband access at houses
    2. Information/Smart appliances
    3. PAN/WLAN hardware
- HAN technologies:
    - Use existing wiring
        - HPNA (Home phone network Alliance)
        - Power line modems
    - Wireless solutions



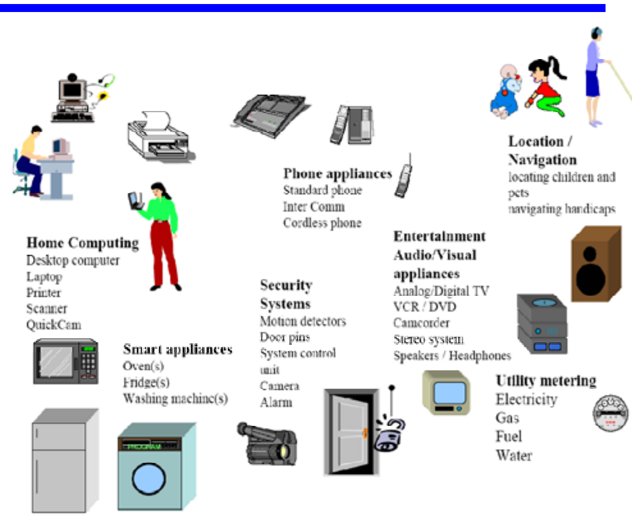
HAN Growth

- Expanding market
  - Doubling every year



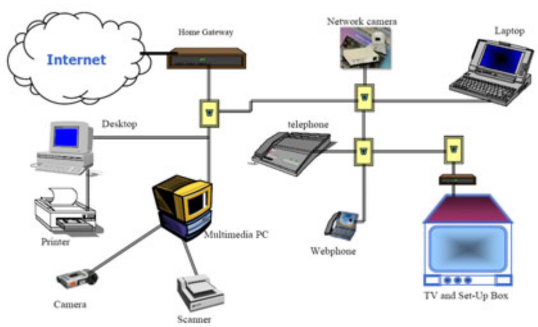
What is a HAN?

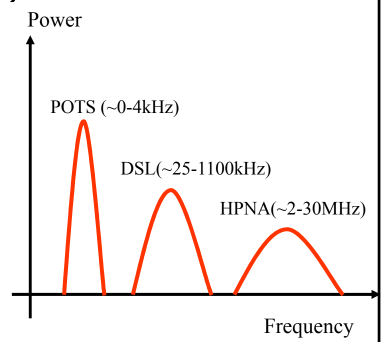
- Home computing equipment – computing and internet connectivity
- Phone appliances
- Security systems
- Entertainment appliances
- Location/Navigation
- Utility metering



HAN Technologies - HPNA

- Home Phone Network Alliance (HPNA)
  - Capitalize on existing TP wiring into/in your house
  - Ethernet-compatible LAN
  - Outlet in every room (almost)



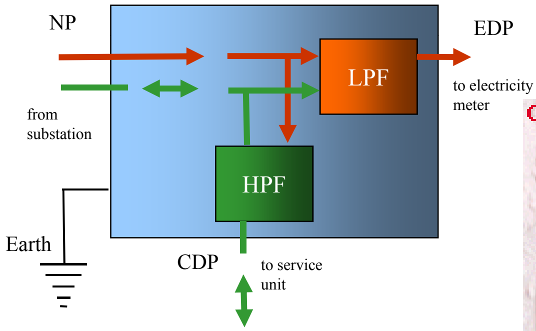


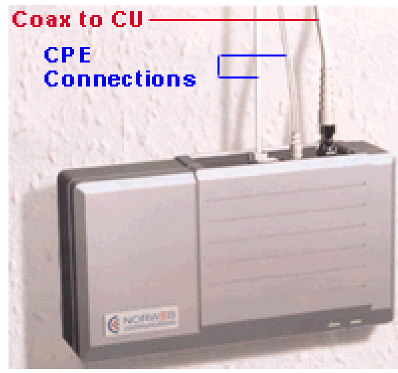
HAN Technologies – Power Lines

- Power Lines Modems
  - Wiring/outlets more available than TP
  - Outlet in every room
- Digital Power Line
  - High Frequency Conditioned Power Network (HFCPN),
  - Conditioning Unit (CU): sends electricity to the outlets in the home and data signals to a communication module or "service unit".
  - Service Unit: provides multiple channels for data, voice, etc.

Digital Power Line

- Conditioning Unit (CU)



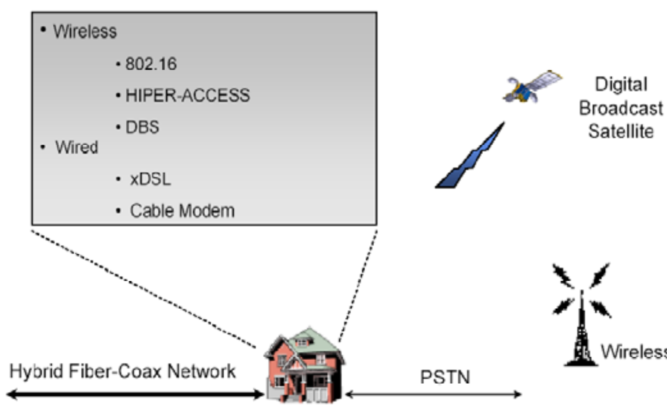


CU: conditioning unit
CDP: Communications Distribution Port
NP: Network Port
EDP: Electricity Distribution Port

 http://www.powerlineworld.com/powerlineintro.html

Home-Access Networking

- How to connect the home to the outside world?
- IEEE802.16 – WMAN for US
- HIPER-ACCESS – WMAN for EU
- LMDS (local multipoint distributed services) – also known as LMCS
- Refer to the other wired solutions



IEEE802.15

- Chapter 11

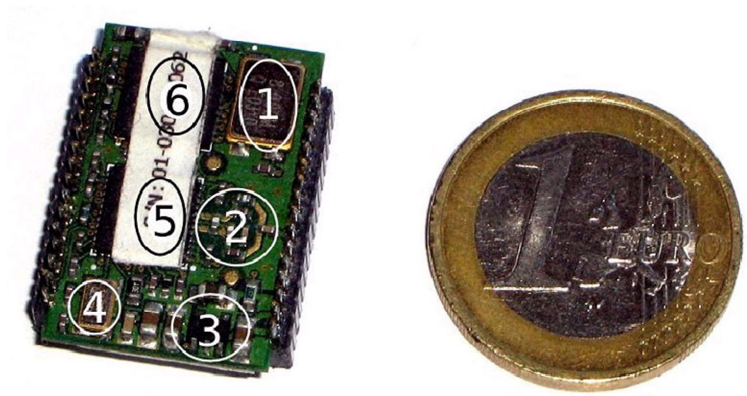
Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Technology

- Def: low-cost, low-power, wireless mesh networking standard
- The ZigBee Alliance – standard body defining ZigBee
  - For interoperable products
  - (IEEE802.15.4-2003, ZigBee) ←→ (IEEE802.11, WiFi)
- Applications: Wireless control and monitoring applications – Defined application profiles:
  - Home automation,
  - ZigBee Smart Energy,
  - Telecommunication Applications,
  - Personal Home and Hospital Care
- Timeline:
  - ZigBee 1.0 – ratified on Dec 14^{th}, 2004
  - ZigBee 2007 – posted Oct 30, 2007
  - 1^{st} ZigBee Application Profile (Home Automation) – announced Nov 2^{nd}, 2007.

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Technology



Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Technology – cont'd

- Operating Frequency: ISM bands
  - 915 MHz in USA
  - 868 MHz in Europe
  - 2.4 GHz in other countries
- Should be simpler and cheaper than other WPANs such as Bluetooth
- Chip vendors typically sell integrated radios and microcontollers with flash memory
  - Freescale MC13213, Ember EM250, TI CC2430
- Price (as of 2006):
  - ZigBee compliant transceiver ~ $1
  - ZigBee radio + processor + memory ~ $3
  - Compare to Bluetooth chip ~ $3

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Technology – cont'd

- ZigBee 2007 – current (most recent) stack release; contains two profiles:
  - Stack profile 1 (called ZigBee) – for home and light commercial use
  - Stack profile 2 (called ZigBee Pro) – more features: multi-casting, many-to-one routing and high security with Symmetric-Key Key Exchange (SKKE)
  - Both profiles offer full mesh functionality
  - Different routing functionality – same application
- Designed for embedded application – requiring low bit rate and low power
- Focus: "to define a general-purpose, inexpensive, self-organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc."

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Devices

- ZigBee Coordinator (ZC)
  - Most capable device
  - Forms root of network tree – may bridge to other network
  - One ZC per network
  - Can store info about the network and act as Trust Center & repository for security keys
- ZigBee Router (ZR)
  - Run applications
  - Act as an intermediate router (passing data from other devices)
- ZigBee End Device (ZED)
  - Limited functionality – least amount of memory
  - Talks to parent node (ZC or ZR) only
  - Much less expensive than ZC and ZR

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Protocols

- Core routing protocols – AODV and neuRFon
- Network – a mesh or single cluster or (for large networks) a cluster of clusters
- Non-Beacon Enabled:
  - Unslotted CDMA/CA channel access
  - ZigBee routers are mostly continuously active
  - Some devices are always on and some are not
- Beacon Enabled:
  - ZigBee routers transmit periodic beacons to confirm presence
  - Nodes may sleep between beacons – lower duty cycle
  - Beacon interval: 15.36 msec ~ 251 sec at 250 kb/s, or from 24 msec to 393 sec at 40 kb/s, or from 48 msec to 786 sec at 20 kb/s
- ZigBee devices conform to IEEE 802.15.4-2003 Low-Rate Wireless Personal Area Network (WPAN) standard.

Reference: http://en.wikipedia.org/wiki/Zigbee

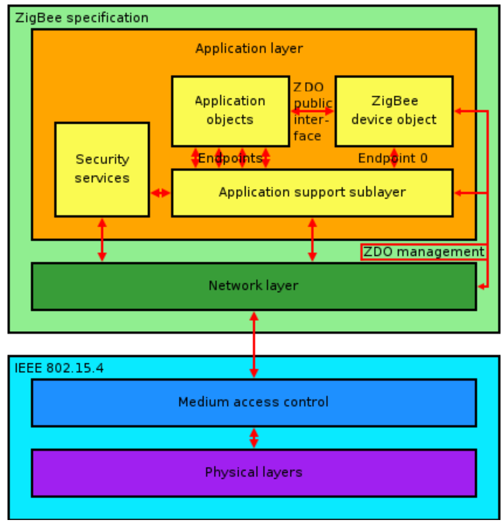
Zigbee Protocols – cont'd

- PHY – operation in unlicensed 2.4 GHz, 915 MHz, and 868 MHz.
  - In 2.4 GHz option – 16 5MHz-wide channels
  - Radio – direct-sequence spread spectrum
  - BPSK in the 868 MHz and 915 MHz
  - QPSK in the 2.4 GHz
  - Raw bit rate = 250 kb/s per channel for 2.4 GHz, 40 kb/s per channel in the 915 MHz, and 20 kb/s per channel in the 868 MHz
  - Range is between 10 and 75 meters
  - Maximum output power is 0 dBm or 1 mW
- MAC – IEEE802.15.4 - CDMA/CA
  - Exceptions - Beacons and message ACKs
  - Guaranteed Time Slots (GTS) an access mode for Beacon Oriented network providing low latency

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Protocol Stack

- PHY and MAC – defined by IEEE802.15.4 (Low-Rate WPANs)
- Additional Layers:
  - Network layer
  - Application layer
  - ZigBee Device Object (ZDO)
  - Manufacturer application-objects
- ZDO's – responsible for keeping dvice roles, management of requests to join, device discovery and security



Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Network Layer

- Mesh architecture – supporting three topologies:
  - Star
  - Tree
  - Generic mesh
- Every network MUST have one coordinator node
  - Tasks of ZC - creation, control of parameters, maintenance, etc.
  - In star – it must be the central node
- Tree and Mesh – allow ZR to extend the communication at network level
- For Trees:
  - Communication within trees are hierarchical
  - May use frame beacons
- For Mesh:
  - Generic communication structure but no router beaconing
- Routing Protocol - AODV

Reference: http://en.wikipedia.org/wiki/Zigbee

Zigbee Application Layer

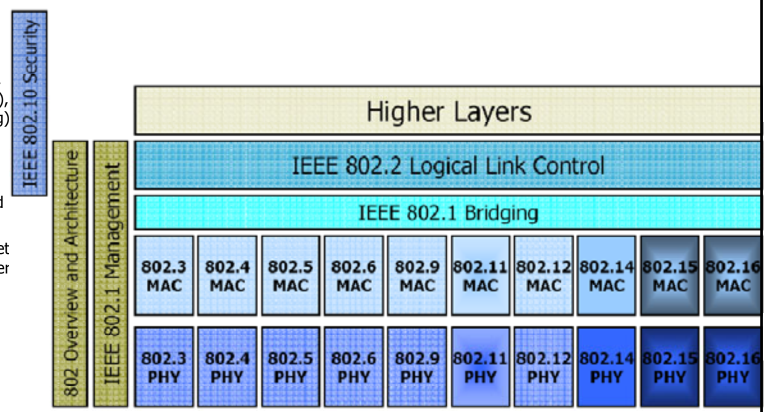
- Includes – ZDO, management procedure, application objects defined by manufacturer
- ZDO tasks:
  - Defines the role of the device as ZC, or end device
  - Discovery of new (one-hop) away devices and identification of their offered services
  - Establishing secure links with external devices
  - Reply to binding request
- Application Support Sublayer (APS) – well defined interface and control services
  - It keeps binding tables (database)
- Manufacturer application-objects – allows manufacturer to build customized applications

IEEE802.11 and its Derivatives

- Chapter 11

Overview of IEEE802 Protocols

- 802.1 and 802.2 are common
- 802.10 - security
- 802.3 (CSMA/CD), 802.4 (Token Bus), 802.5 (Token Ring) – all wired LANs
- 802.6 DQDB – MLAN
- 802.7 - broadband
- 802.8 - FDDI
- 802.9 ISO-Ethernet – voice & data over Ethernet
- 802.11,15, &16 WLAN
- 802.12 – 100BaseVG; priority
- 802.14 cable network
- 802.16 - WMAN



Overview of IEEE802.11

- History:
  - 1997: completion of first IEEE802.11 standards (1 and 2 Mb/s) – PHY: DSSS, FHSS, and DFIR
  - Afterwards: IEEE802.11b – 11 Mb/s using CCK and IEEE802.11a – 54 Mb/s using OFDM
- Same MAC layer for all three
  - CSMA/CA-based for contention data
  - Support RTS/CTS mechanism to solve hidden terminal problem
  - Point coordination function (PCF) – optional; for real-time traffic
- Topology
  - Centralized – through AP
  - Ad-hoc – supporting peer-to-peer communication between terminals

WLAN Protocol Concerns

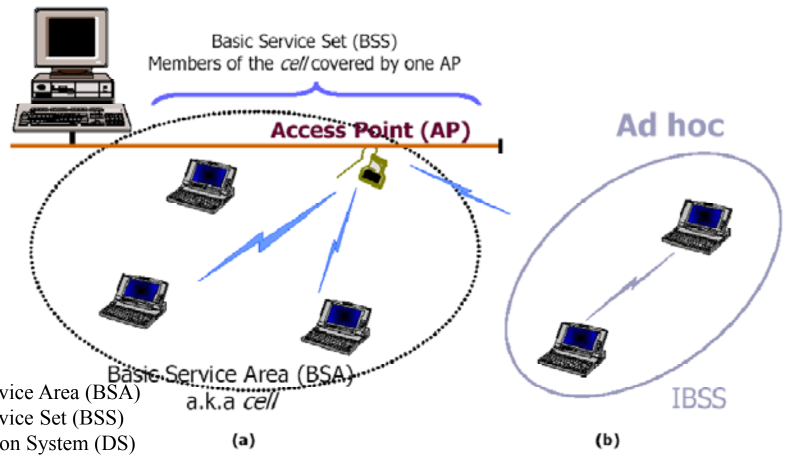
- Mobility
- Connection management: reliability and power
- Security

IEEE802.11 Requirements

- Single MAC supporting multiple PHYs
- Mechanism to allow multiple overlapping networks in the same area
- Provisions to handle the interference from other ISM band radios and microwave ovens
- Mechanism to handle "hidden" and "exposed" terminal problems
- Options to support time-bounded services
- Provisions to handle privacy and access security

Reference Architecture

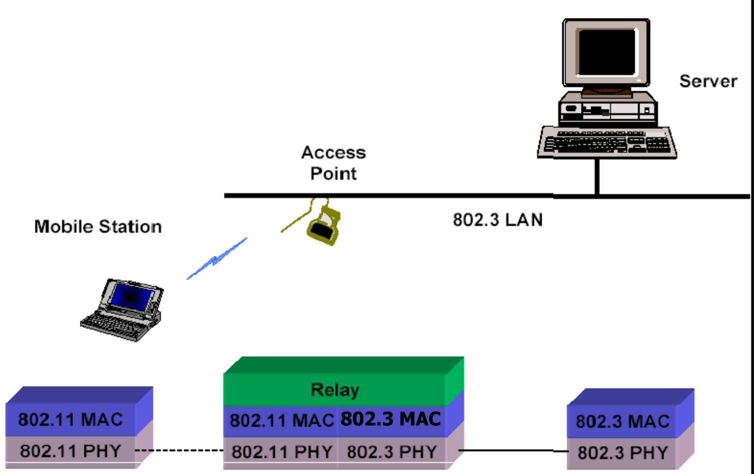
(a) Infrastructure Network (b) Ad-Hoc Network



Basic Service Area (BSA)
Basic Service Set (BSS)
Distribution System (DS)
Extended Service Set (ESS)

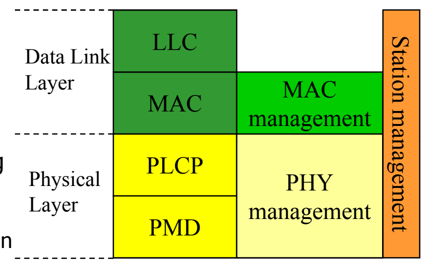
Typical Deployment

- Extended Service Set (ESS)



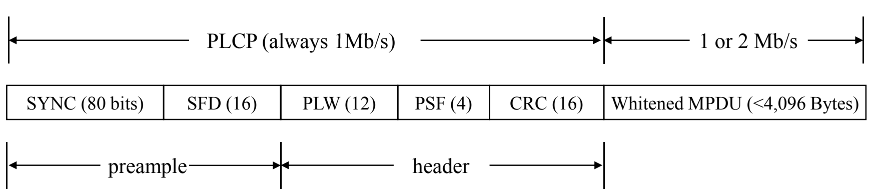
Protocol Architecture

- MAC sublayer responsibilities:
  - Access mechanism
  - Fragmentation and reassembly of packets
- MAC management sublayer responsibilities:
  - Roaming within ESS
  - Power management
  - Registration: Association, disassociation, and re-association
- PLCP responsibilities:
  - Carrier sensing
  - Forming packets for different PHYs
- PMD responsibilities:
  - Modulation, Coding
- PHY layer management: channel tuning to different options within PHY
- Station management sublayer:
  - Coordination and interaction between MAC and PHY



PMD: Physical Medium dependent
PLCP: Physical layer convergence protocol

IEEE802.11 PHY Layer - FHSS



SYNC: Alternating 0s and 1s
SFD: Start of frame delimiter – 0000110010111101
PLW: Packet length width – max of 4 kB
PSF: Packet signaling field – data rate in 500 kb/s step
CRC: PLCP header coding

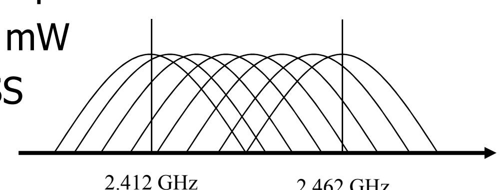
Example:
PSF = 0000 → R = 1Mb/s
= 0010 → R = 2 Mb/s
Maximum rate:
PSF = 1111 → 1 + 15X0.5 = 8.5 Mb/s

IEEE802.11 FHSS

- FHSS PMD hops over 78 channels of 1 MHz each in the centre of the 2.44 GH ISM band
- Modulation is (2 or 4-level) GFSK: 1 bit/symbol → 1 Mb/s or 2 bit/symbol → 2 Mb/s
- BSS selects (PHY management sublayer) one of three hopping patterns:
  - (0,3,6,9,…,75),
  - (1,4,7,10,…,76), or
  - (2,5,8,11,…,77)
- Hopping rate: 2.5 hops per second
- Therefore up to three APs can coexist in the same area ➔ maximum throughput of 6 Mb/s
- Maximum transmit power = 100 mW
- Scrambling (whitening) of MPDU – randomization and elimination of DC component

IEEE802.11 DSSS

- DSSS PMD uses 26 MHz chunks to transmit 11 Mc/s – refer to figure
- Modulation: DBPSK for 1 Mb/s and DQPSK for 2 Mb/s
- ISM band at 2.4 GHz ➔ 11 overlapping channels with 5 MHz spacing
- Coexisting – 5 choices per BSS
- Max tx power = 100 mW
- Wider range the FHSS



IEEE802.11 PHY Layer - DSSS

- PLCP frame for the DSSS of the IEEE802.11

PLCP (always 1Mb/s)

SYNC (128 bits)	SFD (16)	Signal(8)	Service (8)	Length (16)	FCS (8)	MPDU

preample — header

SYNC: Alternating 0s and 1s
SFD: Start of frame delimiter – 1111001110100000
Signal: Data rate in 100 kb/s steps
Service: reserved for future use
Length: length of MPDU in microseconds
FCS: PLCP header coding

Example:
Signal = 00001010 → R = 1 Mb/s
= 00010100 → R = 2 Mb/s
For IEEE802.b:
Signal = 001101110 → 5.5 Mb/s
= 01101110 → 11 Mb/s
Maximum:
Signal = 11111111 → 255X0.1 = 25.5 Mb/s

IEEE802.11 DFIR

- DFIR PMD utilizes 250 ns pulses
- Pulse Position Modulation (PPM)
  - 16-PPM for the 1 Mb/s option
  - 4-PPM for the 2 Mb/s option

PLCP (250 ns pulses)

SYNC (57-73 bits)	SFD (4)	Data Rate (3)	DCLA (32)	Length (16)	FCS (16)	MPDU (<2,500 Bytes)

preample — header

SYNC: Alternating 0, 1 pulses
SFD: Start of frame delimiter – 1001
Data rate: 000 and 001
DCLA: DC level adjustment sequence
Length: length of MPDU in microseconds
FCS: PLCP header coding

IEEE802.11a, b PHY

- IEEE802.11a:
  - OFDM @ 5 GHz U-NII bands – same as HIPERLAN-2
  - Rates up to 54 Mb/s
- IEEE802.11b:
  - CCK @ 2.4GHz
  - Rates up to 5.5 and 11 Mb/s
  - Same PLCP as IEEE802.11 DSSS

Wireless LAN Standards (3)

Standard	Modulation Method	Frequencies	Data Rates Supported (Mbit/s)
802.11 legacy	FHSS, DSSS, infrared	2.4 GHz, IR	1, 2
802.11b	DSSS, HR-DSSS	2.4 GHz	1, 2, 5.5, 11
"802.11b+" non-standard	DSSS, HR-DSSS (PBCC)	2.4 GHz	1, 2, 5.5, 11, 22, 33, 44
802.11a	OFDM	5.2, 5.8 GHz	6, 9, 12, 18, 24, 36, 48, 54
802.11g	DSSS, HR-DSSS, OFDM	2.4 GHz	1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54
802.11n*	advanced techniques: e.g. MIMO, etc.		> 100 Mb/s

*Release – April 2008 (drafts exist)
Source: http://en.wikipedia.org/wiki/IEEE_802.11
Very nice summary of all 802.11 technologies

IEEE802.11 family and Carrier Sensing

- PHY Sensing - Clear Channel Assessment (CCA) signal
  - Generate by the PLCP
  - Sensing: Detected data sensing vs Carrier Sensing
    - Any detected bits?, or – slow but reliable
    - RSS of carrier against threshold – fast but many false alarms
- Virtual carrier sensing:
    - Network Allocation Vector (NAV) signal supported by the RTS/CTS and PCF mechanisms at MAC – indicates the medium is occupied for a given (length field) time duration
    - Used for RTS/CTS and PCF based schemes only

IEEE802.11 MAC

- MAC Layer:
  - MAC sublayer
  - MAC layer management sublayer
- Major responsibilities of MAC sublayer:
  - Define access scheme
  - Define packet formats
- Major responsibilities of management sublayer:
  - Support ESS
  - Power management
  - Security

MAC Sublayer

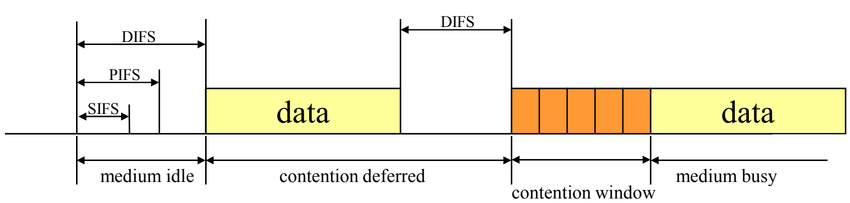
- Supported access schemes
  - CSMA/CA – contention data
  - RTS/CTS – contention-free
  - PCF – contention-free - for time-bounded traffic

These two modes are referred to as DCF

- Inter-frame spacing (IFS) – can be used to prioritize users
  - Short – SIFS - highest priority terminal
  - Point – PIFS – used in conjunction with PCF function
  - Distributed – DIFS – lowest priority terminal – used with DCF
- Refer to CSMA/CA slides

Primary Operation of CSMA/CA

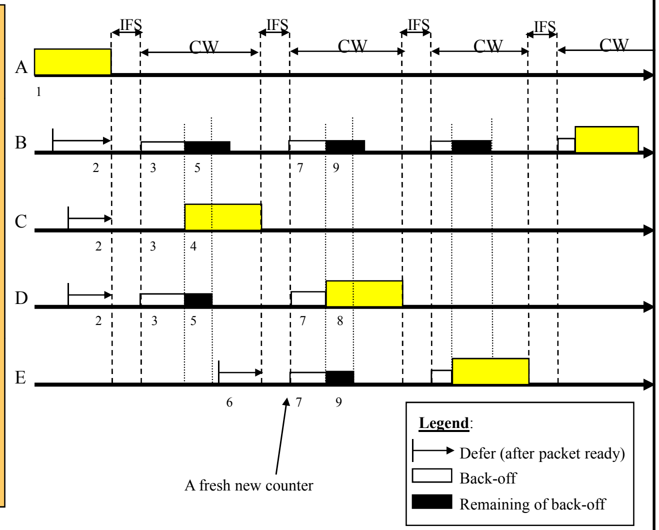
- Primary operation of CSMA/CA as shown in figure
- After the completion of a transmission all terminals having data to transmit must wait S/DIFS – depending on their priority before they start their back-off timers
- Binary exponential back-off scheme is used to minimize probability of collision



Note that this example DOES NOT show the ACKs

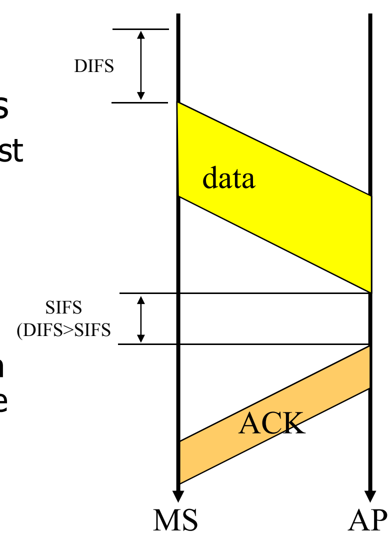
Operation of CSMA/CA in IEEE802.11 – Example 4.18

1. A is transmitting
2. B, C, & D persist on sensing the channel and defer their transmission until A is done
3. B,C, & D wait for IFS and then start their back-off counters
4. C finishes back-off first – it starts transmission
5. B & D freeze their back-off timers
6. During C's transmission, E senses the channel and finds it busy – it defers transmission
7. After the completion of C's transmission and the passing of IFS, B & D restart their frozen back-off counters, while E starts its back-off counter
8. D finishes its back-off counter first – it starts transmission
9. B & D freeze their counters
10. Etc.



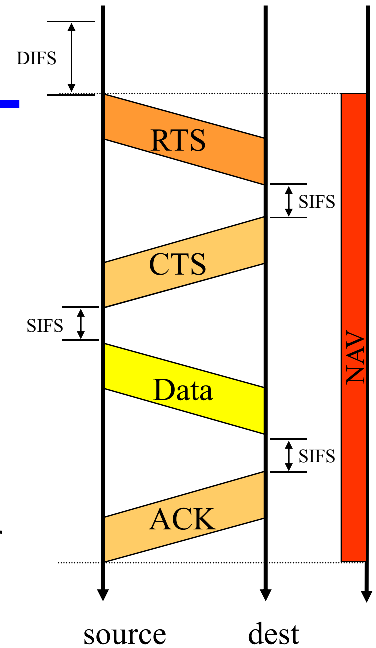
Operation of CSMA/CA with ACK for MAC Recovery

- Note that IEEE802.3 does not support ACK on the MAC level – connectionless
  - For IEEE802.11 there must be an ACK – why?
- AP waits for SIFS before ACK
  - Since SIFS is shorter than DIFS, all stations hear the ACK before they attempt transmission



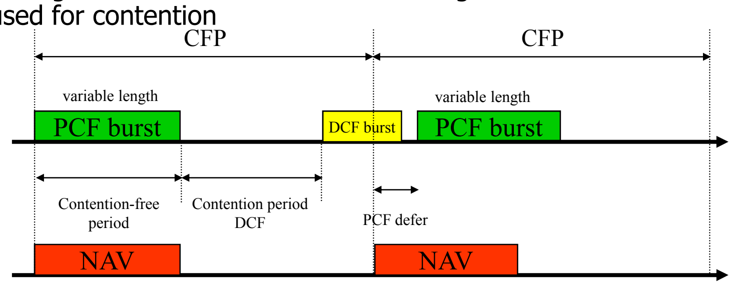
RTS/CTS Operation

- When source is ready – RTS (20 bytes) is sent
- Destination responds with CTS (16 bytes) after SIFS
- Source terminal received CTS and after SIFS sends data
- Destination terminal sends ACK after SIFS
- Other terminal listening to RTS/CTS will turn their NAV signal on – used for virtual carrier sensing
- NAV signal turned off when after the transmission and reception of the ACK frame



PCF for Contention-Free Access

- Optional MAC service – Not implemented by all manufacturers
- Available only for infrastructure networks – not Ad-hoc
- AP – point coordinator organizes periodical contention-free periods (CFP) for delay-sensitive services
- PCF operation
- During PCF operation (part of CFP) NAV signal is on –
- During the remainder of the CFP NAV signal is off and that can be used for contention



Reference: Giuseppe Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function,” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 18, NO. 3, MARCH 2000

Performance of DCF

- Define – slot time: time needed by any station to detect the transmission of any other station
  - Defined by standard – depends on the physical layer and account for the maximum propagation delay
- DCF adopts exponential backoff procedure – refer to the CSMA/CD slides
- At each packet transmission, the backoff is selected uniformly from [0,W]
  - W – called the contention window – increases with collisions
  - Doubled every collision until equal to CWmax = 2^mCWmin

TABLE I
SLOT TIME, MINIMUM, AND MAXIMUM CONTENTION WINDOW VALUES FOR THE THREE PHY SPECIFIED BY THE 802.11 STANDARD: FREQUENCY HOPPING SPREAD SPECTRUM (FHSS), DIRECT SEQUENCE SPREAD SPECTRUM (DSSS), AND INFRARED (IR)

PHY	Slot Time (σ)	CW_{min}	CW_{max}
FHSS	50 μs	16	1024
DSSS	20 μs	32	1024
IR	8 μs	64	1024

Reference: Giuseppe Bianchi, “Performance Analysis of the IEEE 802.11 Distributed Coordination Function,” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 18, NO. 3, MARCH 2000

Performance of DCF – cont’d

- For DCF and RTS/CTS
- Notes:
  - RTS/CTS have almost constant throughput – not function of number of terminals on the ground
  - Throughput of DCF decreases as number of terminals increase
- The analysis (results) assume saturation traffic – i.e. there is always traffic to send

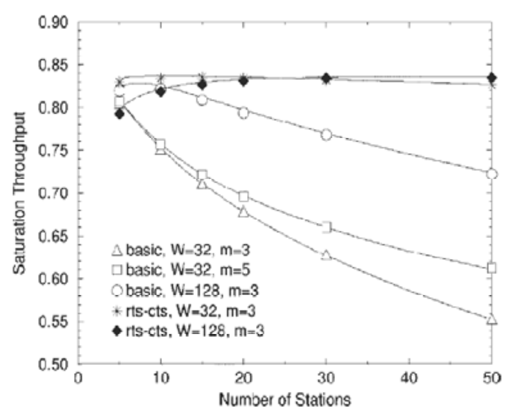


Fig. 6. Saturation Throughput: analysis versus simulation.

MAC Frames Formats

- Frame Control (2 bytes): determines type of frame (data, control and management) – see format of field
- Duration (2 bytes): length of the fragmented packet to follow
- Address fields (6 bytes each): up to 4 MAC address fields – source, destination, and APs the terminal is connected to
- Sequence Control (2 bytes): fragment numbering and sequencing
- Frame Body (0-2312 bytes): user data
- CRC (4 bytes): for protection of MAC frame

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

General MAC frame format for IEEE802.11

MAC Frame – Frame Control Field

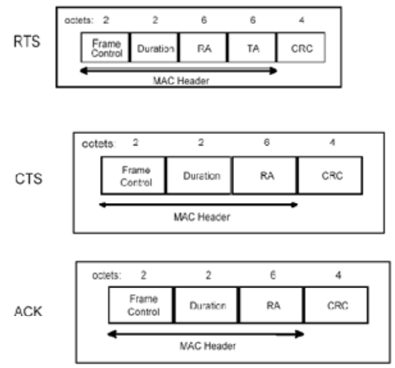
Protocol (2 bits)	Type (2)	Subtype (4)	To DS (1)	From DS (1)	More Frag (1)	Retry (1)	Pw Mgt (1)	More Data (1)	WEP (1)	Order (1)

Protocol Version:	currently 00, other options reserved for future use
Type:	Data (10), control (01), or management frame (00)
Subtype:	RTC, CTS, ACK frame
To DS/from DS:	"1" for communication between two APs
More Fragmentation:	"1" if another section of a fragment follows
Retry:	"1" if packet is retransmitted
Power Management:	"1" if station is in sleep mode
More data:	"1" more packet to the terminal in power-save mode
Wired equivalent privacy:	"1" data bits are encrypted

MAC Frame – Frame Control Field – cont'd

- Need to handle: registration, mobility management, power management and security

Three examples of short MAC frames: RTS, CTS, and ACK
Note: Not all the fields are included in all frames



MAC Management Sublayer – Beacon Message

- Management frame transmitted quasi-periodically by the AP to establish the time synchronization function (TSF) – typically every 100 msec
- Contains: BSS-ID, time-stamp, traffic indication map (TIM for sleep mode), power management, and roaming info.
- RSS measurements are made on the beacon message
- Used to identify the AP and the network

MAC management frame format

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	CRC

MAC Management Sublayer – Registration

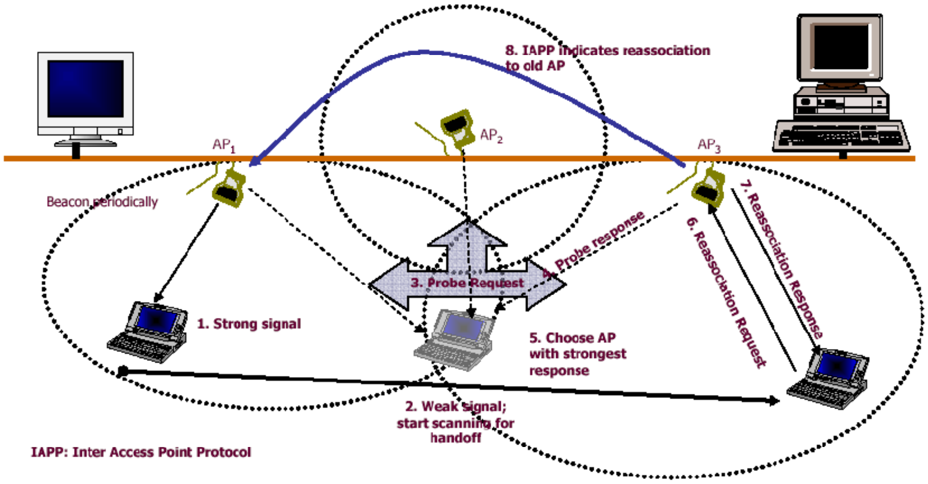
- Association: procedure by which an MS "registers" with an AP
  - After association, the MS can send/receive from AP
  - MS sends an "association request" frame to AP
  - AP grants permission

MAC Management Sublayer – Handoff

- Definitions:
  - No transition: MS is static or moves within BSA
  - BSS transition: MS moves from one BSS to another within the same ESS
  - ESS transition: MS moves from one ESS to another – upper layer connections may break unless a protocol like mobile IP is operating!
- Re-association service is used when an MS moves from BSS to another within the same ESS
  - MS initiates this service
- Dissociation service is used to terminate an association
  - MS or AP can initiate this service
  - Notification – not a request

MAC Management Sublay Handoff (2)

- Passive vs. active scanning:
  - probe request ←→ probe response (similar to beacon)
- Re-association request ←→ re-association response
- Re-association request contains info about the MS and old AP



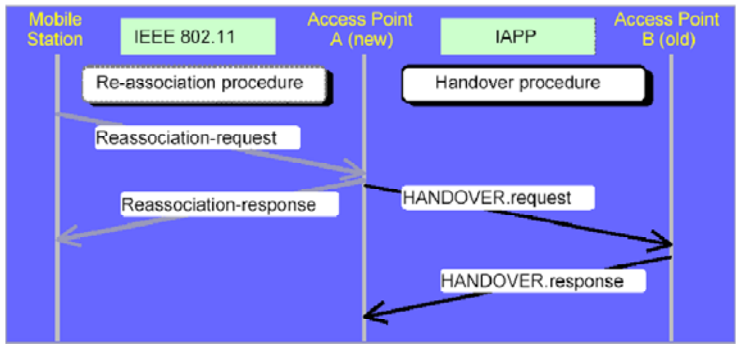
IAPP: Inter Access Point Protocol

MAC Management Sublayer – Handoff - IAPP

- IAPP: Inter-Access Point Protocol
  - Completed 2003 (IEEE 802.11f - recommendation)
  - Proprietary procedures may exist between APs
- PDUs exchanged between old AP and new AP – using UDP-IP over the wired infrastrucutre
- IAPP is used to announce the existence of APs and the creation of APs database within each AP
- If AP does not have an IP address, alternatively, the subnetwork access protocol (SNAP) may be used.
- Used to enforce a unique association throughput one ESS and to securely move the "security context" from old access point to the new access point
- RADIUS is used to distribution the communication keys between the APs
  - RADIUS - Remote Authentication Dial In User Service (RADIUS) is a networking protocol that uses access servers to provide centralized management of access to large networks
  - RADIUS - commonly used by ISPs and corporations managing access to the internet or internal networks employing a variety of networking technologies, including modems, DSL, wireless and VPNs.

MAC Management Sublayer – Handoff – IAPP (2)

- IAPP: Inter-Access Point Protocol

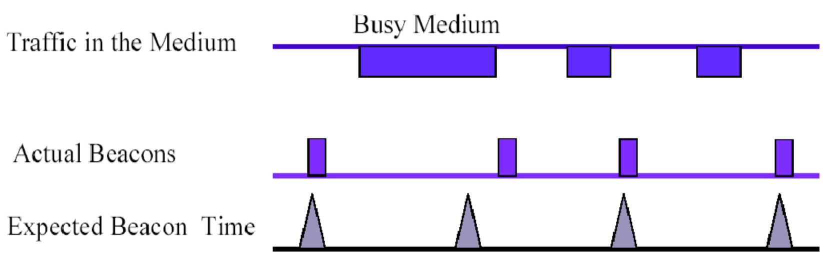


MAC Management Sublayer – Power Management

- The main power consuming state is the idle receive mode – not existent for cellular telephony
  - MS does not know when traffic will be sent to it – remains ready and powered on ➔ huge waste of power
- How to conserve power?
  - MS goes to "sleep"
  - Data buffered at AP and sent to MS only when it is "awake"
  - MS uses the power management bit in the frame control field to announce its sleep strategy
  - MS wakes up at beacon times (STF)
  - TIM field within beacon informs MS whether there is data buffered at AP or not
  - MS with data buffered at AP sends a *power-save poll* to AP – AP responds with data when MS is in active mode.

MAC Management Sublayer – Power Management – cont'd

Listening to the beacon for power management



MAC Management Sublayer – Security

- Very active area of research
- Two types of authentication
  - Open system authentication - default
  - Shared key authentication
    - Involves a challenge-response identification protocol

MAC Management Sublayer – Privacy

- Wired-Equivalent Privacy (WEP) specification
- A pseudorandom generator is used along with the 40-bit secret key to create a key sequence that is simply XOR-ed with the plaintext message
    - Very susceptible to planned attacks