IEEE 802.11 WLAN

By
Orly Meir & Ilan Bar

Agenda

- The wireless revolution
- IEEE 802.11 vs. 802.3
- Architecture (introduction)
  - WLAN 802.11 requirements
  - Wireless Network Overview
  - IEEE 802.11 services
- MAC Layer
  - Reliability of data delivery service
  - Control of shared WL network
  - Frame Types
  - Management Frame Types
  - Privacy service
- Open Issues
- The IEEE task groups for 802.11
- 802.11 documentation

The wireless revolution

- NO WIRES
- Goals
  - One Wireless standard for at Home, in the Office, and on the Move.
  - Interoperability with wired networks
  - Security, QOS, Roaming users.
- Usage:
  - Entertainment (films, shows, gaming, music,..)
  - Information (Internet, ..)
  - E-commerce (secure home shopping,..)
  - Social contacts (email, voice, interest groups,..)
  - PC (documents, data, printing, scanner, server, ...)
  - Control (A/V devices, security, ..)

intel

IEEE 802.11 vs. 802.3

- Similarity
  - Same LLC (Logical Link Control). There in no differences for upper layer protocol
- Differences
  - WLAN is not private (not protected)
  - WLAN is exposed to more distractions (environment problems)
    - Reflectors
    - Changes in strength on the Rx signal in small position change
    - Moving object can change the wave signal
    - Other infrared devices overlap the Tx path.
    - Etc…
  - Mobility
    - The WLAN user can move from one place to another – big advantage. But it cause internal complexity. Roaming between access points and between different IP networks (Mobile IP or DHCP).
    - Servers and services need to be changed (Printer, Proxy server, file server, etc…)
  - IEEE 802.11 PHY has **NO collision detection**
    - IEEE 802.3 use collision detection algorithm.
    - IEEE 802.11 use collision avoidance algorithm.
- **Translation** of 802.11 ⇔ 802.3 is not on the scope of the IEEE 802.11 spec'

intel

Architecture

WLAN 802.11 requirements

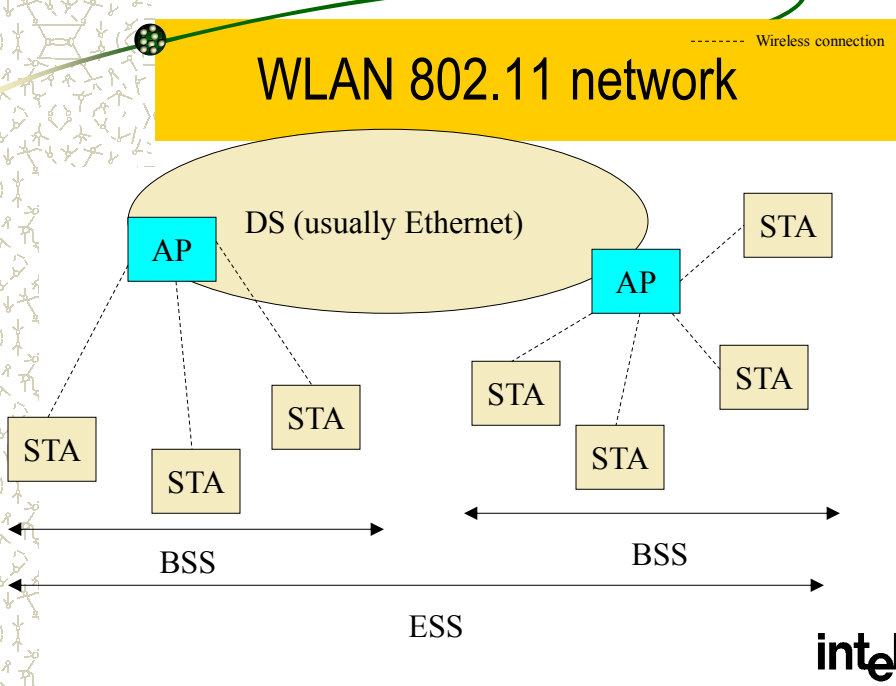
- Mobility
- Tolerant to faults
- Support:
  - Small and transient (temporary) Networks
  - Large [semi-]permanent Networks
- Power saving without losing network connectivity.
- Allow all network protocols to run over WLAN without any considerations.

Wireless Network Overview

- APs (access points) and stations
- BSS (Basic service set)
- DS (Distribution system) and ESS (Extended Service Set)
- Ad-hoc networks

intel

WLAN 802.11 network



intel

APs & stations

- Each node in the IEEE 802.11 network may be station (STA) or and access point
- In definition AP contains a station.

BSS

- Set of arbitrary stations, and **one** AP
- Station have to be associated with the AP in order to be part of the BSS
- Local relay function through the AP.
  - Advantage : When station is in power saving mode the AP will buffer traffic for the (sleeping) mobile station.
  - Disadvantage: Consume twice bandwidth

DS

- Logical communication between the APs
- The DS is the backbone of the WLAN and may be constructed over wired or wireless connection.
- The communication between the APs over the DS, is in the scope of TGf (IAPP – inter access point protocol).
- The connection of the several BSS networks

→ forms Extended Service Set (**ESS**)

ESS

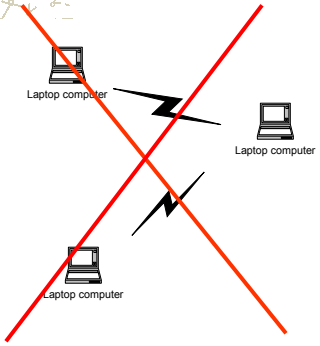
- Group more than one BSS networks
- The APs communicate among themselves to form relay between the BSS domains, through abstract distribution system (DS)

Ad-hoc networks (IBSS)

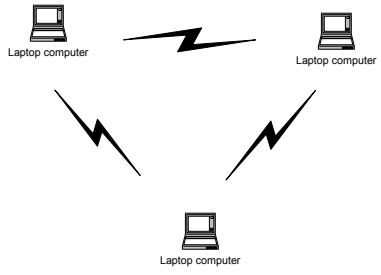
- Temporary set of stations
- Forming as ad-hoc network – an independent BSS (IBSS), means that there is no connection to wired network
- No AP
- No relay function (direct connection)
- Simple setup

intel

Ad-hoc networks



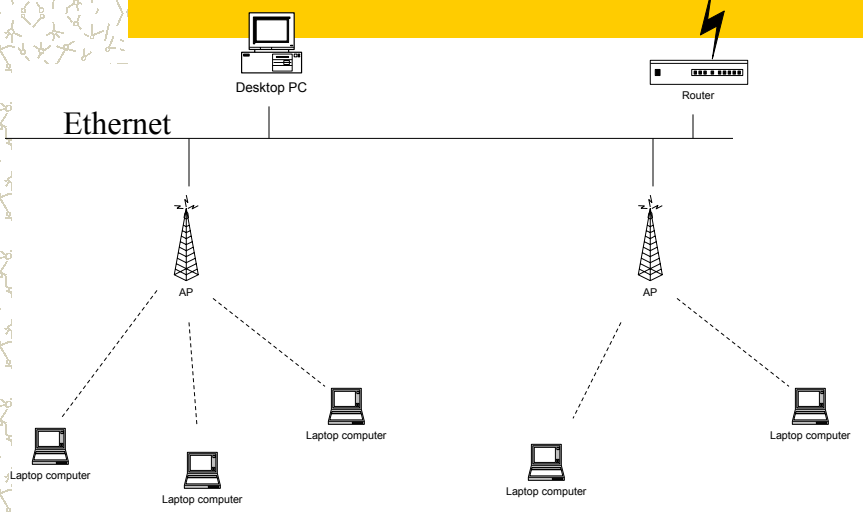
No Relay



Direct connection

intel

Hybrids



IEEE 802.11 overview

intel

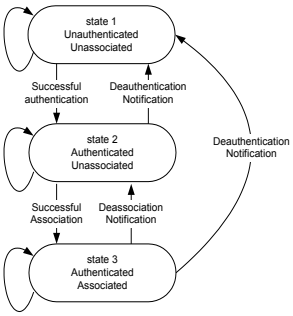
IEEE 802.11 services

- Station services (similar to wired network)
  - Authentication (login)
  - De-authentication (logout)
  - Privacy
  - Data delivery
- Distribution services
  - Association
    - Make logical connection between the AP to the station – the AP will not receive any data from a station before the association. assist the DS to know where to deliver the mobile data. (sets the AID)
  - Reassociation (Similar to the association)
    - Send repeatedly to the AP.
    - Help to AP to know if the station has moved from/to another BSS.
    - After Power Save
  - Disassociation
    - Manually disconnect (PC shutdown or adapter is ejected)
  - Distribution (AP forwarding using the DS)
    - Determine how to deliver
      - Internal in the BSS
      - It's own station
      - To another BSS or network

intel

Handshake protocol

BSS



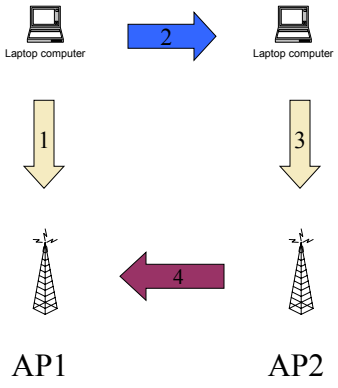
Data delivery state

IBSS

Authentication is not defined
Association before every connection

intel

Services example : Roaming



1- Authenticate and associate

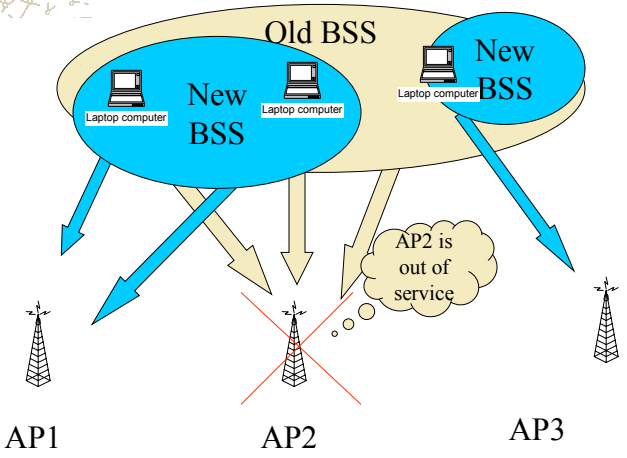
2 – Laptop roaming

3 – Authenticate (if needed) and (re)associate

4 – Notify the new location of the laptop (disassociation of AP1)

intel

Services example : “Out of service”



intel

Medium Access Control (MAC) Layer

intel

MAC functionalities

- Reliability of data delivery service
- Control of shared WL network
- Frame Types (informational section)
- Management
- Privacy service (Wired Equivalent Privacy - WEP)

Reliability of data delivery service

- Problems to solve
  - The air is noisy and unreliable media
  - The Hidden Node problem
- Solutions : Frame Exchange Protocol
  - Every frame is acknowledged (ACK)
  - CTS & RTS frames
  - Fragment long data frames (see Fragmentation)

Acknowledgments (ACK)

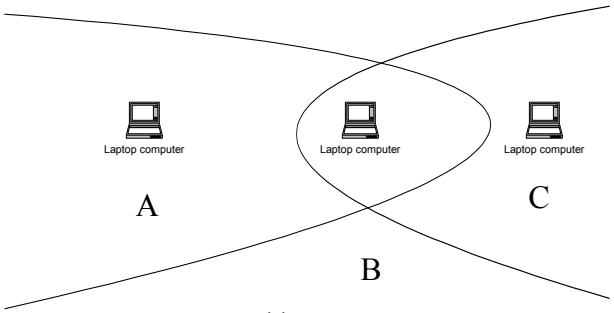
Note: as said before WL media has **no** PHY collision detection.

Traffic flow:

1. Data is being sent (Source → Destination)
2. If the data was received correctly in the destination, an ACK (Destination → Source) will be sent back. If ACK is returned than go to 6.
3. Else (data was not received or ACK didn't returned), increment the retry counter.
4. If retry counter < MAX_RETRY_COUNTER go to 1
5. Else (counter exceeded) ➔transmit failed (frame is lost)
6. Transmition succeeded, continue.

intel

The Hidden Node problem



Direct connections:
A ⇔ B
C ⇔ B

Problems
1. A Send data to B
2. C can disturb transmition A ⇔ B because C can't hear A

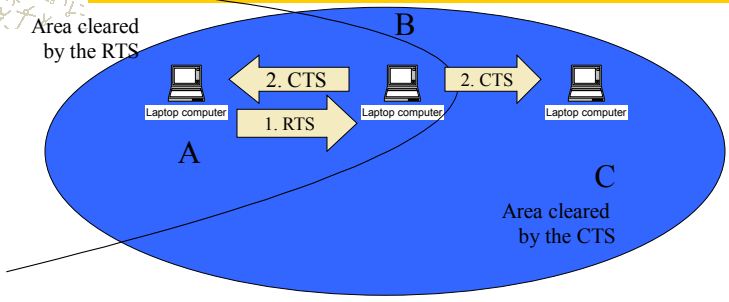
intel

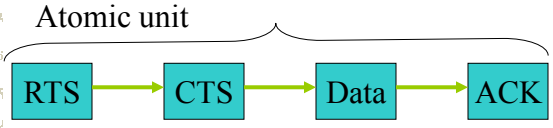
Solving the Hidden Node problem

- Request To Send (RTS):
  - Source announcing its transmition.
  - Will cause its neighborhood stop transmitting
- Clear To Send (CTS):
  - Destination received the RTS and announce the source to send the data.
  - Will cause its (the destination) neighborhood stop transmitting.

intel

Example





intel

Notes

- RTS and CTS can be avoided by threshold parameter. This is useful in 'all connected' topology. The RTS and CTS bandwidth will be saved this way (typical threshold is 128 bytes)
- RTS and CTS mechanism can be used in BSS and IBSS.
- AP is never a Hidden node.
- Retransmit counters are configurable
  - Short frames retry counter
  - Long frames retry counter

  } Short/Long Frame length is also configurable
- When data transmission fails (by retransmit counter), the MAC layer will notify it to the MAC user, through the service interface.

intel

Control of shared WL network

MAC access mechanism

- Distributed Coordination Function
  - Based on the IEEE 802.3 Ethernet access mechanism.
- Point Coordination Function
  - Token based mechanism (one Point Coordinator in the BSS at the AP, that gives the 'token' to speak)
  - **Not relevant** to WLAN implementations.

intel

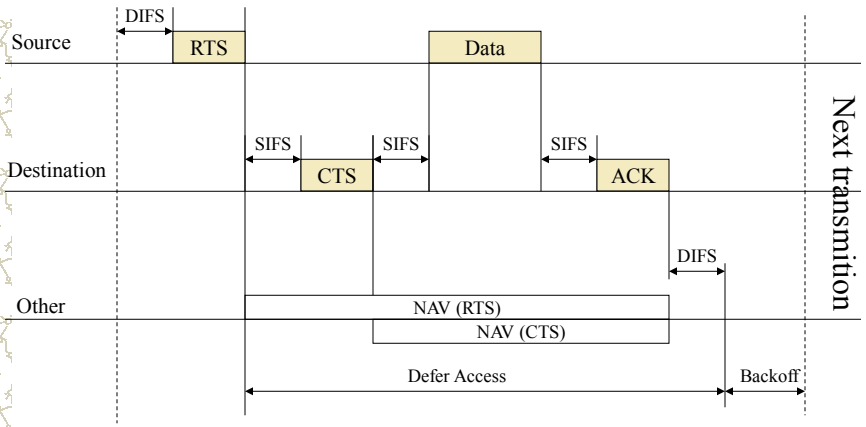
Distributed Coordination Function

- Carrier Sense Multiple Access Collision Avoidance (CSMA/CA), uses binary exponential backoff (Same as in IEEE 802.3)
  - IEEE 802.3 use collision detection algorithm.
  - IEEE 802.11 use collision avoidance (CA) algorithm
- Listen Before Talk – LBT (don't transmit while others transmit to avoid collision)
- Network Allocation Vector (NAV) – the time till the network will be cleared from any transmitting.
- The NAV with the LBT assist to avoid collisions (CA)

intel

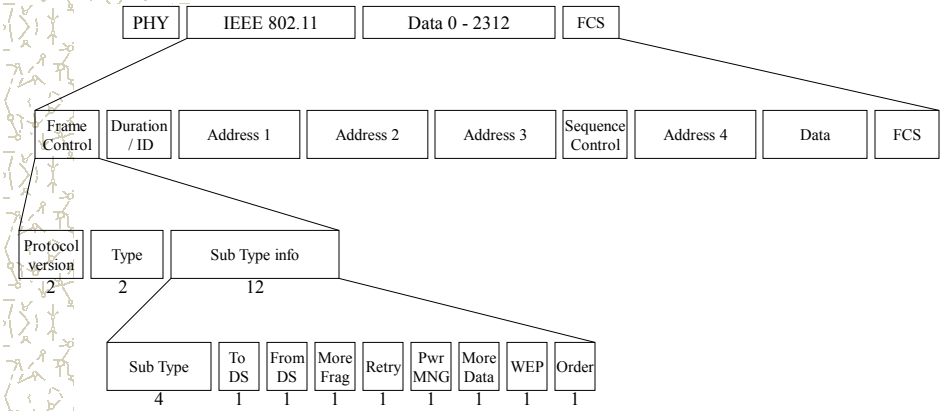
NAV setting

SIFS – Short Interframe Space
DIFS - Distributed Interframe Space



intel

Frame Formats

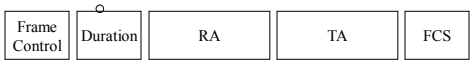


intel

Control Frame Types

Time in microseconds. Update the NAV time in the neighborhood

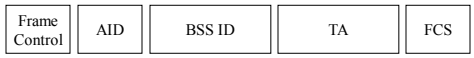
- RTS



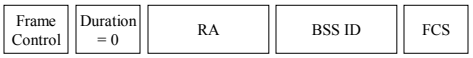
- CTS

- ACK

- Power Save poll

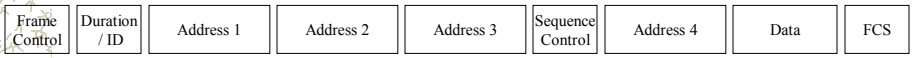


- Contention Free (CF) End & CF-End+ACK



intel

Data Frame Types



Function	To DS	From DS	Address 1 (Receiver)	Address 2 (Transmitter)	Address 3	Address 4
IBSS	0	0	RA = DA	SA	BSSID	N/A
From AP	0	1	RA = DA	BSSID	SA	N/A
To AP	1	0	RA = BSSID	SA	DA	N/A
Wireless DS	1	1	RA	TA	DA	SA

Note
Broadcast and multicast never leave the BSS

intel

Data Frame Fields

- **Duration**
  Time in microseconds from end of data frame (including the ACK frame to this data frame). Must be zero for multicast frame.
- **Address 1**
  Destination address (the receiver address)
- **Address 2**
  The source address (the transmitter address)
- **Address 3**
  DS information
- **Address 4**
  Used only in wireless DS

intel

Management Frame Types

- Same as data frames, but with different type field
- Restricted to 3 addresses
- Include beacons, association and authentication messages
- Management frame are generated and terminated within the MAC layer

Beacons

- Transmitted periodically by the AP to locate and identify its BSS
- The AP will send a Beacon to notify the station that it has buffered frames to that station.
- The station don't have to wakeup every Beacon (in the IBSS the station MUST wakeup in Beacon receive)
- When the station wakes up it sends power save poll frame to the AP. The AP than will send to the station its buffered frames.
- In IBSS Beacons are sent also. Every time it sent by another station, see "Synchronization"
- notes:
  - Timer Synchronization Function (TSF) timer Synchronize the clock.
  - Target Beacon Transmitting Timer control the Beacons periods
  - In IBSS, a station will not power down until it hears Beacon from another station

The Probe Frame

- Transmitted by a mobile station, attempting to quickly locate a WLAN.
- May be used to locate particular BSS (SSID) or any WLAN
- Used in active scanning, see "Combining Management Solutions"
- Probe Response looks like a Beacon frame, sent by AP in the BSS or by last transmitting Beacon station in the IBSS (see "Synchronization")

intel

(De)Authentication

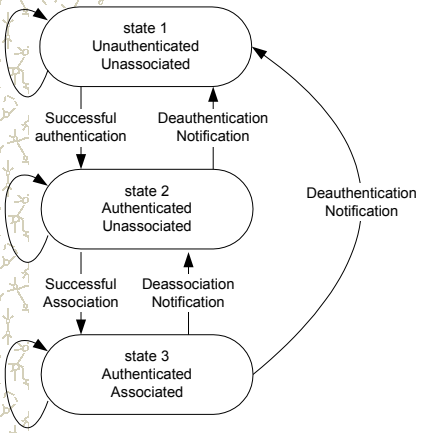
- Verify identification between station and its AP.
- A station can be authenticated with many APs simultaneously.
- De Authentication: the station notify of the termination of an authentication relation.

intel

(Re/De)Association

- Used to make a logical connection between the mobile station and its AP. See the "Handshake protocol"
- The logical connection useful for the AP to deliver frames to/from the mobile station, and to allocate resources to the mobile station.
  The output of the Association is the Association ID (AID). This AID+BSSID will be send in the power save poll (see Control Frame Types).
- Invoked once, when :
  - mobile station is entering the WLAN for the first time
  - After power saving state
  - After being out of touch
- Re-association is similar to the association but it contains information about the AP. This will assist the mobility function, see "Roaming example"
- The De-Association will terminate the association relation.

Relationship between station state and the services



state	Control	Management	Data
1	CTS,RTS,ACK, CF+ACK, CF	Probe,Beacon ,Auth,deAuth, ATIM	Only internal in the BSS
2		(Re,Dis)Assoc iation	
3	PS-Poll	DeAuth (goto state 1)	All data types are allowed

Fragmentation

- Needed to decrease the probability of the surrounding destruction (microwave ovens, etc…) by splitting frame to smaller parts
- It is possible to tune the size from which the frame will be fragmented by a MIB (management Information Base) parameter name - dot11FragmentationTreshold
- By default no fragmentation is being done.

intel

Privacy

1. Any one with antenna can hear you
2. Wired Equivalent Privacy (WEP)
3. Only the data is encrypted (the MAC layer is not changed after the encryption). WEP doesn't protect from traffic analysis.
4. RC4 – symmetric stream cipher algorithm with variable key length is used (same key and algorithm for encryption and decryption)

intel

WEP details

Two methods:

- Default keys (up to four) will be shared in the BSS or the whole ESS.
  - It is useful to learn some default keys **once**
  - The keys can be revealed more easily.
- One-To-One key mapping.

MAC Management

We need management environment in order to solve those problems:

1. Noisy media
   - Many users on air
   - Destructions from other WLANs
2. Every one can connect to the WLAN
   - Security issues
3. Mobility
4. Power management

MAC Management Solution

- Threshold and retransmit parameters
- Address filtering. 1

- Authentication
  Simple authentication (Open System Authentication)
  Authentication with both side verification (WEP)
  Notes
  The authentication connection is one-sided.
  Usually a station is authenticated to AP.
  If the AP is a "pretender" we can have security problem. 2
- Privacy (WEP)

- Association
- Synchronization (Beaconing + Scanning) 3

- Power mng mechanism. 4

intel

Synchronization

The process of Synchronize a station to its BSS (MAC/PHY) parameters. Includes Beaconing (announce the presents of the BSS :AP → STA) and Scanning (find a BSS: STA → AP)

Beaconing

- In the BSS
  - AP sends periodically Beacons.
  - This will update the Timer Synchronization Function (TSF) . This timer is used to sync' the station for the CA mechanism.
- In the IBSS
  - No AP the update the TSF.
  - First station will reset the TSF, and will adjust the Beacon periods.
  - The next Beacon transmitting is chosen like a back off algorithm (each station choose random number for delay. The first to transmit will stop the other stations. However if there is a Beacon collision which will cause several Beacons at once, the IEEE 802.11 support this case).

intel

Synchronization cont'

- Scanning
  - Passive scanning:
    - The station will scan all channels
    - It will listen to each channel for a period of time (not defined in the spec'), to find a BSS
    - Saves bandwidth and transmit power
  - Active scanning:
    - The station will scan all channels
    - It will send a Probe request to get details on the BSS, if exists in the current channel.
- In the end of the Synchronization process the station will have information on the BSSs and it will decide which BSS to join (not defined in the spec').

Power Management

- In BSS
  - The station that want to enter into power save mode send to the AP a power save bit in the frame control. This means that in the end of the traffic flow, it will enter into power save mode .
- In IBSS
  - The station will enter into power save mode only after it has finished its current connection with another station (No specification in IEEE 802.11 when to enter into power save mode).
  - A Beacon frame **always** cause the station to wakeup, because there is no AP to buffer the incoming traffic to the station.
  - After the Beacon was received the station MUST stay awake for Ad-Hoc Traffic Message Window
  - The spec' defines that every period of time one of the stations in the IBSS will send a Beacon. (see Beacons)

Combining Management Solutions

- Power Saving with Scanning
  - Mobile station notify the AP that it is in power saving mode. Than start to scan for a new BSS.
  - While the AP will buffer frames that destined to the “sleeping” mobile station, the station will associate with a new AP.
  - The buffered frames and the old station configuration will be transferred to new AP from the old AP to the station.
- Pre-Authentication with scanning
  - The station can Authenticate with the new AP that is scanned.
  - It will save authentication time when it will go to the new BSS.

intel

Open Issues

- Load balancing between APs
- IP roaming problems (In BSS & In IBSS)
- “Tower of Babel”
  - ~40 802.11 different vendors
  - No argument on:
    - QOS
    - Roaming
    - Etc…
  - PAN (connect from public area to remote ISP with security)

intel

The IEEE task groups for 802.11 and current status

- Terms
  - Task group: a committee that tasked by the working group as author of the standard
  - Working group: includes all the task groups
- MAC task group (last published in 1999)
- PHY task group (last published in 1999)
- TGa : define the PHY for 802.11a (last published in 1999)
- TGb : define the higher rate PHY for 802.11 (completed in 1999)
- TGb – Cor1 : define the MIB parameters for TGb, (status: ongoing)
- TGc : wireless LAN with bridge operations (completed)
- TGd: support by region (country) – (status – ongoing)
- TGe: QOS (status – ongoing)
- TGf: AP ⇔ AP compatibly protocol (ongoing)
- TGg: improvements in the 802.11b PHY (ongoing)
- TGh: improvements in the 802.11a PHY (ongoing)
- TGi: improvements in security (ongoing)

intel

802.11 documentation

- "IEEE 802.11 handbook, a designers companion", by Bob O'Hara & Al Petrick
- "IEEE official standard"

intel