IEEE 802.11 (WLAN)

Other WGs and WLAN Implementation issues

Luciano Bononi (bononi@cs.unibo.it)

IEEE 802.11 WGs

<table>
<thead>
<tr>
<th>Gruppi di standardizzazione IEEE 802.11</th>
<th>Descrizione</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.11</td>
<td>lo standard originale: bitrate da 1 a 2 Mbps, spettro 2.4 Ghz, livello fisico sia radio che infrarosso</td>
</tr>
<tr>
<td>IEEE 802.11a</td>
<td>54 Mbit/s, 5 GHz, lanciato nel 2001</td>
</tr>
<tr>
<td>IEEE 802.11b</td>
<td>sviluppo di IEEE 802.11 (1999), da 5.5 a 11 Mbps</td>
</tr>
<tr>
<td>IEEE 802.11d</td>
<td>estensioni per roaming internazionale</td>
</tr>
<tr>
<td>IEEE 802.11e</td>
<td>estensioni per qualità del servizio</td>
</tr>
<tr>
<td>IEEE 802.11f</td>
<td>standard per Inter Access Point Protocol (IAPP)</td>
</tr>
<tr>
<td>IEEE 802.11g</td>
<td>54 Mbit/s, 2.4 GHz, retrocompatibile con IEEE 802.11b</td>
</tr>
<tr>
<td>IEEE 802.11h</td>
<td>selezione dinamica dei canali e controllo della potenza trasmissiva (compatibile con direttive europee)</td>
</tr>
<tr>
<td>IEEE 802.11i</td>
<td>integrazioni e estensioni per la sicurezza (2004)</td>
</tr>
<tr>
<td>IEEE 802.11j</td>
<td>estensioni per direttive giapponesi</td>
</tr>
<tr>
<td>IEEE 802.11k</td>
<td>estensioni per misurazione dei parametri radio</td>
</tr>
<tr>
<td>IEEE 802.11m</td>
<td>estensioni per throughput elevati (oltre 200 Mbps) mediante tecnologia MIMO (trasmettitori e ricevitori multipli)</td>
</tr>
<tr>
<td>IEEE 802.11p</td>
<td>accesso wireless per sistemi televisivi (WA VE)</td>
</tr>
<tr>
<td>IEEE 802.11r</td>
<td>estensioni per roaming veloce</td>
</tr>
<tr>
<td>IEEE 802.11s</td>
<td>estensioni per reti wireless mesh</td>
</tr>
<tr>
<td>IEEE 802.11t</td>
<td>metodi e metriche per misurazione e previsione delle prestazioni</td>
</tr>
<tr>
<td>IEEE 802.11u</td>
<td>internetworking con reti non 802.11 (cellulari)</td>
</tr>
<tr>
<td>IEEE 802.11v</td>
<td>gestione e amministrazione delle reti wireless</td>
</tr>
</tbody>
</table>
WLAN and WMAN Wireless Standards and technologies

<table>
<thead>
<tr>
<th>Standard</th>
<th>UWB</th>
<th>Bluetooth</th>
<th>Wi-fi</th>
<th>Wi-fi</th>
<th>WiMAX</th>
<th>WiMAX</th>
<th>WiMAX</th>
<th>EDGE</th>
<th>CDMA</th>
<th>UMTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15.3a</td>
<td>802.15.1</td>
<td>802.11a</td>
<td>802.11b</td>
<td>802.11g</td>
<td>802.16d</td>
<td>802.16e</td>
<td>2.5G</td>
<td>3G</td>
<td>3G</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>contexto</th>
<th>WPAN</th>
<th>WPAN</th>
<th>WLAN</th>
<th>WLAN</th>
<th>WMAN (fisso)</th>
<th>WMAN (mobile)</th>
<th>WWAN</th>
<th>WWAN</th>
<th>WWAN</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>MAX bitrate</th>
<th>110-480 Mbps</th>
<th>720 Kbps</th>
<th>54 Mbps</th>
<th>11-22 Mbps</th>
<th>54-108 Mbps</th>
<th>75 Mbps (20 MHz)</th>
<th>30 Mbps (10 MHz)</th>
<th>384 Kbps</th>
<th>2,4 Mbps</th>
<th>10 Mbps</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>distanza</th>
<th>10 m</th>
<th>10 m</th>
<th>100 m</th>
<th>100 m</th>
<th>10 km</th>
<th>5 km</th>
<th>5 km</th>
<th>5 km</th>
<th>5 km</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>spettro</th>
<th>7.5 Ghz</th>
<th>2.4 Ghz (ISM)</th>
<th>5 Ghz</th>
<th>2.4 Ghz (ISM)</th>
<th>2.4 Ghz (ISM)</th>
<th>11 Ghz</th>
<th>2-6 Ghz</th>
<th>1800 Mhz</th>
<th>multi</th>
<th>multi</th>
</tr>
</thead>
</table>

Service Sets

### Basic Service Set
- Access Point
- Client nodes
- Service Set Identifier (SSID): 32 char ID (network name?)
  - not a password: can be sniffed (in clear in packet headers)
  - Used for association of clients to APs (sharing the same SSID)

### Extended service set
- two or more BSS connected by distribution system
  - Wireless routers (different SSID)
  - Wireless repeaters (same SSID)?

### Independent Basic Service Set (IBSS)
- Ad hoc network (peer to peer nodes, no AP authentication)
Range Extension between BSS cells and DS

IEEE 802.11: Distribution System (DS)

AP: Access Point
BSS: Basic Service Set
ESS: Extended Service Set
DS: Network to transmit packets between BSSs to realize ESSs.

SSID

- **Service Set Identifier (SSID):**
  - not a password! can be sniffed
    - AirMagnet, Netstumbler, AiroPeek NX...
    - Windows Xp sniffs SSID to configure NIC devices for access
      - ...potential for attacks?
  - Admin: useless to delete SSID info from Beacon frames...
    - ...Because SSID is used for association of clients to APs
  - Many SSID are factory-defined and never changed
    - E.g. CISCO “tsunami”, Proxim “Proxim”, Symbol “Symbol”
BSS attacks

- **BSS Attacks:**
  - (Phy/MAC) layer interference (bla bla bla bla...)
  - (MAC) CTS flooding

- **Rogue access points**
  - Un-authorized access point with no security alignment
  - Man in the middle + rogue access point to re-associate the client
    - Sniff area with NetStumbler, AirMagnet WLAN analyzer
    - Use centralized applications: AirWave, CiscoWorks
    - Use TCP port scanner (SuperScan 3.0) to monitor all 80 ports (rogue AP Web server responds?)

BSS security assessment (1)

- **Review existing security policies, and monitor for rogue access points**
  - Activate WEP at the very least
    - WEP key is static and crackable with AirSnort, WEPcrack
  - Utilize pre-shared key, or dynamic key exchange mechanisms, and static IP (no DHCP)
    - IEEE 802.11i, Advanced Encryption Standard (AES) and dynamic key exchange (Wireless Protected Access, Wi-Fi Protected Access, WPA)
    - DHCP gives local IP and enable crackers for IP access to the whole network

- Ensure NIC and access point firmware is up-to-date

- Ensure only authorized people can reset the access points
  - Disable reset buttons and console programming port
BSS security assessment (2)

- Assign "strong" passwords to access points, locate in good places and and disable them when not used
- Disable SSID broadcast in Beacons (but still present in association frames)
- Adopt Access Controller over Open Network (not authenticated access)
  Access Points
  - Implement mutual authentication mechanisms
  - Authentication of clients performed with RADIUS servers, IEEE 802.1X
- Use firewalls and IPSec VPNs technologies over client devices

IEEE 802.11 AP configuration (1)

- Configuring the AP...
  - Direct cable connection (console)
  - Wireless Web server access to URL "http://192.168.0.x"
    - do it before installation of multiple APs
  - Set the IP address (static?)
  - Set the radio channel
    - 1, 6, 11 preferable for IEEE 802.11b
IEEE 802.11 AP configuration (2)

- Configuring the AP
  - Set transmission power (max 100 mw)
  - Set SSID identifier (network name?)
  - Set allowed data rates
  - Set beacon repetition interval (typical 10 ms)
  - Set RTS/CTS activation and payload threshold
  - Set fragmentation threshold
  - Set WEP encryption (>128 bit = 26 HEX char)
  - Set mutual devices authentication (no open system):
    - Pre-shared keys, 802.1x + RADIUS authentication server, WPA
  - Set admin AP interface passwords

IEEE 802.11 WLAN deployment

- Radio planning
  - Map areas and channels with coverage analysis (AirMagnet, Yellow Jacket)
  - Check pre-existing radio channels assigned (neighbor network?)
    - 75% are channel 6 (device default) (use NetStumbler)
  - Put AP high on the ceiling, with antennas vertical towards the floor (better propagation and coverage area)
    - Beware of metallic grids within walls (Faraday’s grids)
  - Use Power over Ethernet (PoE) if the plug is unpractical

- Configuring the wireless repeater (increase AP radio range)
  - Switch the AP to repeater mode (see next slides)
  - Set the SSID of the same root AP
  - Set the preferred AP and secondary AP to forward frames to
  - Clients associates with the strongest signal with the same SSID
IEEE 802.11 WLAN deployment

- Configuring the wireless bridge (connects two or more wireless networks by considering MAC addresses only)
  - AP are similar to bridges, but connect many wireless users devices (NICs) to one network (e.g. Ethernet) and forward all frames received (no filtering)
  - Workgroup Bridges. Workgroup bridges connect wireless networks to larger, wired Ethernet networks

- Configuring the wireless router (connects wireless clients to more than one network, and always consider IP addresses)
  - Setup IP address and domain name server (DNS) address, or DHCP server
  - Setup SSID, RTS/CTS, WEP, frequency channel, fragmentation, power, etc.
  - Allow wireless clients to connect to more than one wireless network in the area
  - Implement Network Address Translation (NAT) for IP address sharing
  - Improve network management options and network performance (selective forwarding, no broadcast)
  - Improve security with built-in firewalls (IP filtering), IPSec and VPN support

Cohexistence Problems: mixed mode clients b/g

- IEEE 802.11b and IEEE 802.11g technologies
  - 802.11b is DSSS (11 Mb/s) in 2.4 Ghz
    - Mbps depend on the distance from AP
  - 802.11g is OFDM (54 Mb/s) in 2.4 Ghz (extra speed)
    - New technology to deploy over 802.11b systems?
    - Mixed mode Wireless router with b/g access support?
    - Performance drawbacks
    - Low throughput (waiting the slowest technology for channel access)... Similar to the “slow car on the tunnel” problem
  - Solution: separate b and g communication with different APs connected to the network router
  - Non-overlapping channels 1, 6, 11
  - Use mixed mode protection (RTS/CTS or CTS-to-self)

- 802.11b AP (b only AP)
- 802.11g AP (g only AP)
Cohexistence Problems: mixed mode clients b/g

- E.g. homogeneous IEEE 802.11b (or IEEE 802.11g) technology
  - BSS Scenario 1: 802.11 AP streaming large files to two clients
    - Clients near to AP (both at 11 Mbps download speed)
    - One client moves far from AP (1 Mbps)
  - Results in low speed for both clients!!! (-77% = avg 7.2 to 1.6 Mbps)

- E.g. mixed IEEE 802.11g IEEE 802.11b technology
  - BSS Scenario 2: 802.11b/g AP streaming large files to two clients
    - A) two IEEE 802.11g clients (both at 54 Mbps download speed, 30 Mbps avg MAC through.)
    - B) one client IEEE 802.11g and one client IEEE 802.11b (802.11b cannot detect OFDM transmissions, and need CTS with IEEE 802.11b modulation scheme)
      - = - 64% , avg 11.2 Mbps
    - Partial solution: initial contention window size: TXOP every 16 slots (g) and every 32 slots (b)
Configuration of a Wireless Network

**Access Point mode (target config)**

- IP: 130.136.22.55
- 802.11 MAC addr.
  - 000b abcd 1234
- 802.11 MAC addr.
  - 000e dcba 5678
- IP: 130.136.22.56
- 802.11 MAC addr.
  - 000e dcba 5678
- 802.11 MAC addr.
  - 000c ba2e 3c4d

**Operating Mode**: Access Point
- IP: 130.136.22.50
- Netmask: 255.255.255.0
- SSID: "my_wlan1"
- wireless channel: 6
- WEP/WPA encryption: 256 bit mode HEX
- WEP Key: 23d43fa00be...

**Ethernet MAC addr.**
- 000f 6a3c bcde

**802.11 MAC addr.**
- 000f 33dd abcd

**SSID**: "my_wlan1"

**Via console**: attach serial cable, run client software

Configuration of a Wireless Network

**Access Point mode**: step 0
- connect AP and set config PC

**Operating Mode**: ?
- IP: 192.168.0.50 (default)
- Netmask: 255.255.255.0 (default)
- SSID: ?
- wireless channel: ?
- WEP encryption: ?
- WEP Key: ?

**Ethernet MAC addr.**
- 000f 33dd abcd

**802.11 MAC addr.**
- 000f 6a3c bcde

**PC for AP config** (step 0: install software, run client)
- Via LAN Network: IP: 192.168.0.51, netmask: 255.255.255.0
- Via console: attach serial cable, run client software
Configuration of a Wireless Network

- **Access Point mode: step 1**
  - set LAN IP and config. parameters
    - 802.11 MAC addr.: 000f 6a3c bcde
    - Netmask: 255.255.255.0
    - SSID: "my_wlan1"
    - wireless channel: 6
    - WEP/WPA encryption: 256 bit mode HEX
    - Ethernet MAC addr.: 000f 3364 abcd

---

PC for AP config (step 0: install software, run client)
Via LAN Network: IP: 130.136.22.50, netmask: 255.255.255.0
Via console: attach serial cable to AP

---

**Access Point mode: step 2**
- set WLAN client parameters
  - IP: 130.136.22.50
  - 802.11 MAC addr.: 000f 6a3c bcde
  - Netmask: 255.255.255.0
  - SSID: "my_wlan1"
  - wireless channel: 6
  - WEP encryption: 256 bit mode HEX
  - WEP Key: 23cd4f3a00be...
  - Ethernet MAC addr.: 000f 3364 abcd

---

IP: 130.136.22.50
- 802.11 MAC addr.: 000f 012a bd3c4d

---

IP: 130.136.22.50
- 802.11 MAC addr.: 020f 3364 abcd
**Configuration of a Wireless Network**

- **Access Point mode (target config)**
  - Operating Mode: Access Point
  - IP: 130.136.22.50
  - Netmask: 255.255.255.0
  - SSID: "my_wlan1"
  - wireless channel: 6
  - WEP encryption: 256 bit mode HEX
  - WEP Key: 23cd4f3a00be...

- **SSID**: "my_wlan1"
- **wireless channel**: 6
- **000f 6a3c bcde**

---

**Configuration of a Wireless Network**

- **Other AP operating modes: Wireless client**
  - Operating Mode: Access Point
  - IP: 130.136.22.50
  - Netmask: 255.255.255.0
  - SSID: "my_wlan1"
  - wireless channel: 6
  - WEP encryption: 256 bit mode HEX
  - WEP Key: 23cd4f3a00be...

- **SSID**: "my_wlan1"
- **wireless channel**: 6
- **000f 6a3c bcde**

---

© 2005 Luciano Bononi Sistemi e Reti Wireless
Configuration of a Wireless Network

- **Other AP operating modes: Wireless client**

  Operating Mode: **Wireless Client**
  
  IP: 130.136.22.49
  
  Netmask: 255.255.255.0
  
  Ethernet Gateway: 130.136.22.50
  
  SSID: "my_wlan1"
  
  Wireless channel: 6
  
  WEP encryption: 256 bit mode HEX
  
  WEP Key: 23cd4f3a00be...

  802.11 MAC addr: 000f 33dd abcd

Configuration of a Wireless Network

- **Other AP operating modes: Wireless Bridge Mode**

  Only two APs can wirelessly connect each other!

  SSID: "my_two_bridged_LANs"
  
  Wireless channel: 6
  
  WEP encryption: 256 bit mode HEX
  
  WEP Key: 23cd4f3a00be...

  802.11 MAC: 000f 6a3c bcde

  130.136.22.host/24

© 2005 Luciano Bononi  Sistemi e Reti Wireless
Configuration of a Wireless Network

- Other AP operating modes: Multi-point Wireless Bridge Mode
  - Many APs can wirelessly connect multiple LANs each other
  - SSID: "my_bridged_LANs"
  - WEP encryption: 256 bit mode HEX
  - WEP Key: 23cd4f3a00be...

Configuration of a Wireless Network

- Other AP operating modes: Repeater Mode
  - Extends wireless range of the AP
  - Operating Mode: Access Point
    - 802.11 MAC addr: 000f 6a3c bcde
    - IP: 130.136.22.50
    - Netmask: 255.255.255.0
    - SSID: "my_wlan1"
    - Wireless channel: 6
    - WEP encryption: 256 bit mode HEX
    - WEP Key: 23cd4f3a00be...
Configuration of a Wireless Network

- Typical AP config. Mask: general configuration parameters

![AP Configuration Interface](image1)

Typical AP config. Mask: LAN IP address

![AP Configuration Interface](image2)
Configuration of a Wireless Network

- Typical AP config. Mask: (example, wireless client)

![Image](image1.png)

Configuration of a Wireless Network

- Typical AP config. Mask: set AP operating mode

![Image](image2.png)
**Configuration of a Wireless Network**

- Typical AP config. Mask: check MAC layer connection

![Typical AP configuration interface](image1)

**Configuration of a Wireless Network**

- Typical AP config. Mask: log connection status of AP

![Typical AP configuration interface](image2)
Configuration of a Wireless Network

- Typical AP config. Mask: MAC filtering