

# IEEE 802.11 (WLAN)

## Other WGs and WLAN Implementation issues

Luciano Bononi (bononi@cs.unibo.it)

© 2005 Luciano Bononi      Sistemi e Reti Wireless

### IEEE 802.11 WGs

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

© 2005 Luciano Bononi      Sistemi e Reti Wireless

### WLAN and WMAN Wireless Standards and technologies

	UWB	Bluetooth	Wi-fi	Wi-fi	Wi-fi	WIMAX	WIMAX	EDGE	CDMA	UMTS
Standard	802.15.3a	802.15.1	802.11a	802.11b	802.11g	802.16d	802.16e	2.5G	3G	3G
contesto	WPAN	WPAN	WLAN	WLAN	WLAN	WMAN (fisso)	WMAN (mobile)	WWAN	WWAN	WWAN
MAX bitrate	110-480 Mbps	720 Kbps	54 Mbps	11-22 Mbps	54-108 Mbps	75 Mbps (20 MHz)	30 Mbps (10 MHz)	384 Kbps	2,4 Mbps	10 Mbps
distanza	10 m	10 m	100 m	100 m	100 m	10 km	5 km	5 km	5 km	5 km
spettro	7.5 Ghz	2.4 Ghz (ISM)	5 Ghz	2.4 Ghz (ISM)	2.4 Ghz (ISM)	11 Ghz	2-6 Ghz	1800 Mhz	multi	multi

© 2005 Luciano Bononi      Sistemi e Reti Wireless

- ### 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)
- © 2005 Luciano Bononi      Sistemi e Reti Wireless

### 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.

© 2005 Luciano Bononi      Sistemi e Reti Wireless      5

### 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"

© 2005 Luciano Bononi      Sistemi e Reti Wireless      6

### BSS attacks

---

▪ **BSS Attacks:**

- (Phy/MAC) layer interference (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?)

© 2005 Luciano Bononi      Sistemi e Reti Wireless      7

### 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

© 2005 Luciano Bononi      Sistemi e Reti Wireless      8

## BSS security assessment (2)

- Assign "strong" passwords to access points, locate in good places 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

© 2005 Luciano Bononi

Sistemi e Reti Wireless

9

## 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



© 2005 Luciano Bononi

Sistemi e Reti Wireless

10

## 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

© 2005 Luciano Bononi

Sistemi e Reti Wireless

11

## 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

© 2005 Luciano Bononi

Sistemi e Reti Wireless

12

## 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

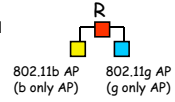
© 2005 Luciano Bononi

Sistemi e Reti Wireless

13

## 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 DSSS (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)



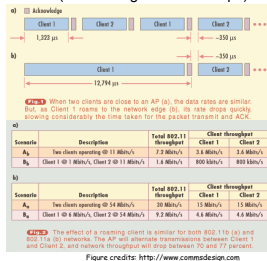
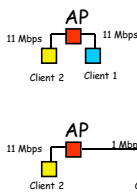
© 2005 Luciano Bononi

Sistemi e Reti Wireless

14

## 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)



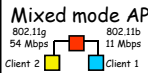
© 2005 Luciano Bononi

Sistemi e Reti Wireless

15

## Cohexistence Problems: mixed mode clients b/g

- E.g. mixed IEEE 802.11g IEEE 802.11b technology
  - BSS Scenario 2: 802.11b/g AP streaming large files to two clients
    - Two IEEE 802.11g clients (both at 54 Mbps download speed, 30 Mbps avg MAC through)
    - 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)



Client 1	Client 2	Client 1	Client 2	Client 1	Client 2	Client 1	Client 2	Client 1	Client 2
10	5.9	6.2	6.5	6.8	7.0	7.2	7.4	7.6	7.8
9	5.9	6.2	6.5	6.8	7.1	7.4	7.6	7.8	8.0
8	5.9	6.3	6.6	6.9	7.2	7.5	7.7	8.0	8.2
7	5.9	6.3	6.7	7.1	7.4	7.7	7.9	8.2	8.4
6	5.9	6.4	6.8	7.2	7.6	7.9	8.2	8.4	8.7
5	5.9	6.5	7.0	7.4	7.8	8.2	8.5	8.7	9.0
4	5.9	6.6	7.2	7.7	8.2	8.5	8.9	9.2	9.4
3	5.9	6.8	7.6	8.2	8.7	9.1	9.4	9.7	10.0
2	5.9	7.2	8.2	8.9	9.4	9.8	10.2	10.4	10.7
1	5.9	8.2	9.4	10.2	10.7	11.1	11.3	11.6	11.7
0	0.0	20.1	22.1	23.1	23.1	23.1	23.1	23.1	23.1

In a mixed 802.11g and 802.11b environment, the throughput (including TCP/IP overhead) depends on the number and type of clients associated with the AP. The figures represent total network throughput.

© 2005 Luciano Bononi

Sistemi e Reti Wireless

16

### 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...

802.11 MAC addr: 000f 6a3c bcde  
 Ethernet MAC addr: 000f 33dd abcd

IP: 130.136.22.55  
 802.11 MAC addr: 000b abcd 1234

IP: 130.136.22.56  
 802.11 MAC addr: 000e dcba 5678

IP: 130.136.22.57  
 802.11 MAC addr: 000c 1a2b 3c4d

Internet Router: 130.136.22.host/24 (Ethernet LAN)

© 2005 Luciano Bononi Sistemi e Reti Wireless 17

### 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: ?

802.11 MAC addr: 000f 6a3c bcde  
 Ethernet MAC addr: 000f 33dd abcd

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

© 2005 Luciano Bononi Sistemi e Reti Wireless 18

### Configuration of a Wireless Network

- Access Point mode: step 1 set LAN IP and config. parameters**

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...

802.11 MAC addr: 000f 6a3c bcde  
 Ethernet MAC addr: 000f 33dd abcd

PC for AP config (step 0: install software, run client)  
 Via LAN Network: IP: 130.136.22.host, netmask: 255.255.255.0  
 Via console: attach serial cable to AP

© 2005 Luciano Bononi Sistemi e Reti Wireless 19

### Configuration of a Wireless Network

- Access Point mode: step 2 set WLAN client parameters**

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...

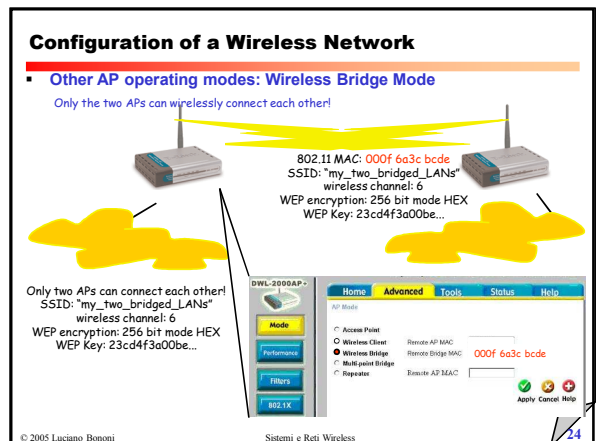
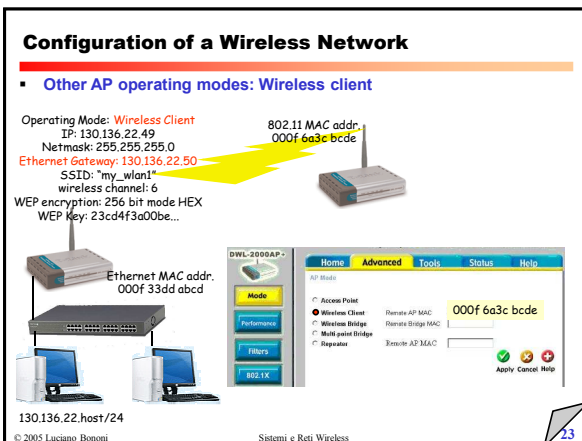
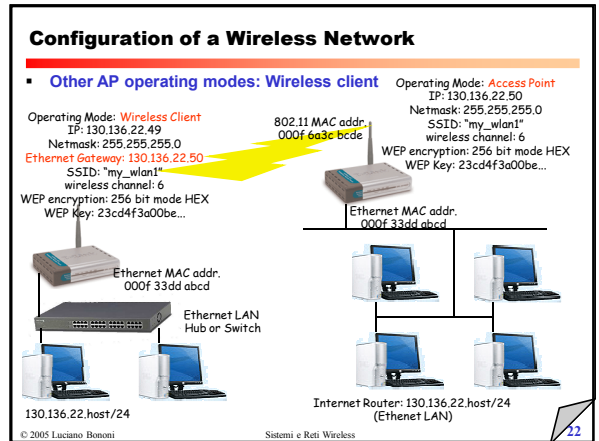
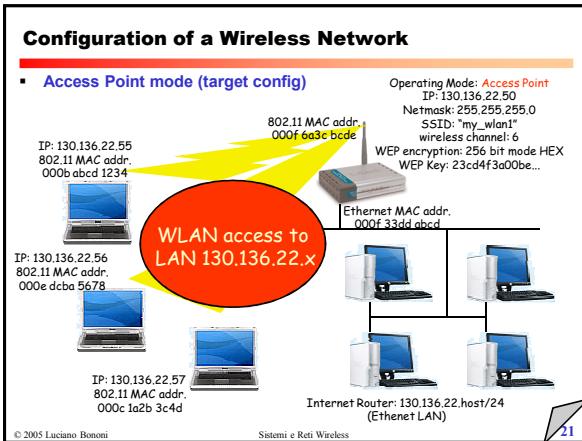
802.11 MAC addr: 000f 6a3c bcde  
 Ethernet MAC addr: 000f 33dd abcd

IP: 130.136.22.whost1  
 802.11 MAC addr: 000b abcd 1234  
 SSID: "my\_wlan1"  
 WEP encryption: 256 bit mode HEX  
 WEP Key: 23cd4f3a00be...

IP: 130.136.22.whost2  
 802.11 MAC addr: 000c 1a2b 3c4d  
 ...

IP: 130.136.22.host1, netmask: 255.255.255.0

© 2005 Luciano Bononi Sistemi e Reti Wireless 20



### Configuration of a Wireless Network

- Other AP operating modes: Multi-point Wireless Bridge Mode  
Many APs can wirelessly connect multiple LANs each other!

Only two APs can connect each other!  
SSID: "my\_bridged\_LANs"  
WEP encryption: 256 bit mode HEX  
WEP Key: 23cd4f3a00be...

© 2005 Luciano Bononi Sistemi e Reti Wireless 25

### 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 b0de  
IP: 190.136.22.50  
Netmask: 255.255.255.0  
SSID: "my\_wlan1"  
wireless channel: 6  
WEP encryption: 256 bit mode HEX  
WEP Key: 23cd4f3a00be...

© 2005 Luciano Bononi Sistemi e Reti Wireless 26

### Configuration of a Wireless Network

- Typical AP config. Mask: general configuration parameters

© 2005 Luciano Bononi Sistemi e Reti Wireless 27

### Configuration of a Wireless Network

- Typical AP config. Mask: LAN IP address

© 2005 Luciano Bononi Sistemi e Reti Wireless 28

## Configuration of a Wireless Network

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

**D-Link**  
Building Networks for Today

**AirPlus XtremeG+**  
High-Speed 2.4GHz Wireless Access Point

DWL-2000AP+  
Home Advanced Tools Status Help

Device Information  
Firmware Version 1.13, 18 Feb 2004

**Ethernet**

MAC Address	0009546c00
IP Address	192.168.0.52
Subnet Mask	255.255.255.0
Gateway	192.168.0.50

**Wireless**

MAC Address	0009546465
SSID	default
Encryption Function	64 bits
Channel	E

Help

## Configuration of a Wireless Network

- Typical AP config. Mask: set AP operating mode

**DWL-2000AP+**

Home Advanced Tools Status Help

AP Mode

Access Point  
 Wireless Client  
 Wireless Bridge  
 Multi-point Bridge  
 Repeater

Remote AP MAC: 00F3546c00  
 Remote Bridge MAC:  
 Remote AP MAC:

Apply Cancel Help

## Configuration of a Wireless Network

- Typical AP config. Mask: check MAC layer connection

**DWL-2000AP+**

Home Advanced Tools Status Help

Traffic Statistics  
Traffic Statistics display Receive and Transmit Packets Passing through the DWL-2000AP+

**Ethernet**

Send Good Packets	1240
Droped Packets	0
Recv Good Packets	1177
Droped Packets	0

**Wireless**

Send Good Packets	0
Droped Packets	0
Recv Good Packets	0
Droped Packets	0

## Configuration of a Wireless Network

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

**DWL-2000AP+**

Home Advanced Tools Status Help

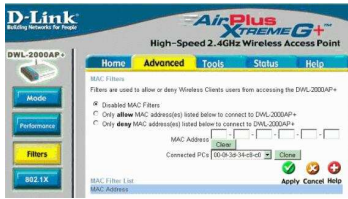
Log

Time	Message
Aug22/2005 18:22:15	Wireless PC connected 00-0E-34-34-08-00
Aug22/2005 18:28:46	Wireless PC connected 00-50-5A-33-A7-3A
Aug22/2005 18:28:52	Wireless PC connected 00-0E-34-34-08-00
Aug22/2005 18:17:53	Wireless PC connected 00-50-5A-33-A7-3A
Aug22/2005 18:15:39	Wireless PC connected 00-0E-34-34-08-00
Aug22/2005 18:17:11	AP mode Ready Channel: 6, SSID: default
Aug22/2005 18:17:11	System started



## Configuration of a Wireless Network

- Typical AP config. Mask: MAC filtering



## Configuration of a Wireless Network

- Typical AP config. Mask: MAC filtering

