

# IEEE 802.11 (WLAN)

## Other WGs and WLAN Implementation issues

Luciano Bononi (bononi@cs.unibo.it)

## 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 Mbit/s, 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 <b>qualità del servizio</b>
IEEE 802.11f	standard per <b>Inter Access Point Protocol (IAPP)</b>
IEEE 802.11g	54 Mbit/s, 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 <b>sicurezza</b> (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 <b>MIMO</b> (trasmettitori e ricevitori multipli)
IEEE 802.11p	accesso wireless per <b>sistemi veicolari</b> (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

## 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

## 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)?

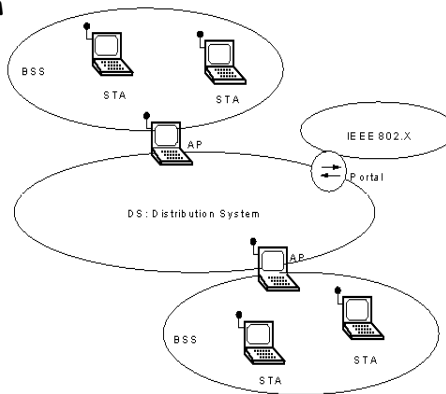
### Independent Basic Service Set (IBSS)

- 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)

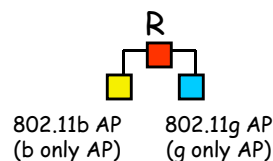
- Switch the AP to repeater mode (see next slides)
- Set the SSID of the same root AP
- Set the preferred AP and secondary AP to forward frames to
- Clients associates with the strongest signal with the same SSID

## 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

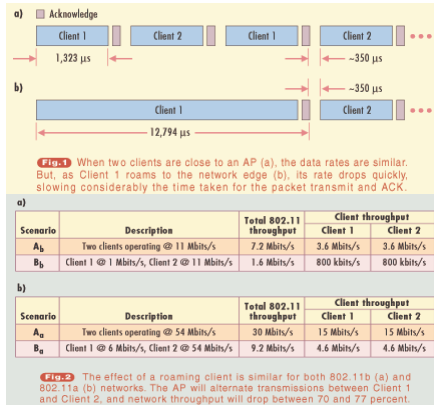
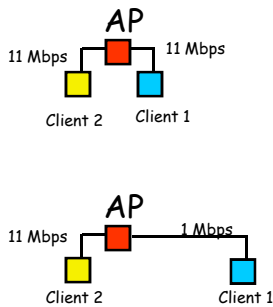
- **IEEE 802.11b and IEEE 802.11g technologies**
  - 802.11b is DSSS (11 Mb/s) in 2.4 Ghz
    - Mbps depend on the distance from AP
  - 802.11g is OFDM (54 Mb/s) in 2.4 Ghz (extra speed)
    - New technology to deploy over 802.11b systems?
    - Mixed mode Wireless router with b/g access support?
    - 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)



## 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

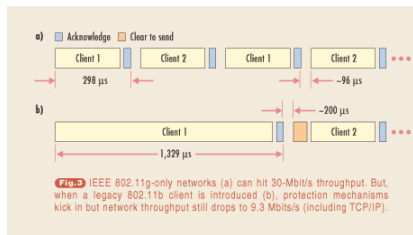
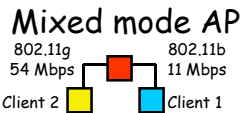
Figure credits: <http://www.commsdesign.com>

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
  - 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)



802.11b clients	0	1	2	3	4	5	6	7	8	9	10
10	5.9	6.2	6.5	6.8	7.0	7.2	7.4	7.6	7.8	8.0	8.2
9	5.9	6.2	6.5	6.8	7.1	7.4	7.6	7.8	8.0	8.2	8.3
8	5.9	6.3	6.6	6.9	7.2	7.5	7.7	8.0	8.2	8.4	8.5
7	5.9	6.3	6.7	7.1	7.4	7.7	7.9	8.2	8.4	8.6	8.8
6	5.9	6.4	6.8	7.2	7.6	7.9	8.2	8.4	8.7	8.9	9.1
5	5.9	6.5	7.0	7.4	7.8	8.2	8.5	8.7	9.0	9.2	9.4
4	5.9	6.6	7.2	7.7	8.2	8.5	8.9	9.2	9.4	9.6	9.8
3	5.9	6.8	7.6	8.2	8.7	9.1	9.4	9.7	9.9	10.2	10.4
2	5.9	7.2	8.2	8.9	9.4	9.8	10.2	10.4	10.7	10.9	11.1
1	5.9	8.2	9.4	10.2	10.7	11.1	11.3	11.6	11.7	11.9	12.0
0	0.0	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1	22.1

Fig. 4 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.

Figure credits: <http://www.commsdesign.com>

MenzoWentink, Tim Godfrey and Jim Zyren  
Overcoming IEEE 802.11g's Interoperability Hurdles  
COMMUNICATION SYSTEMS DESIGN, May 2003

© 2005 Luciano Bononi

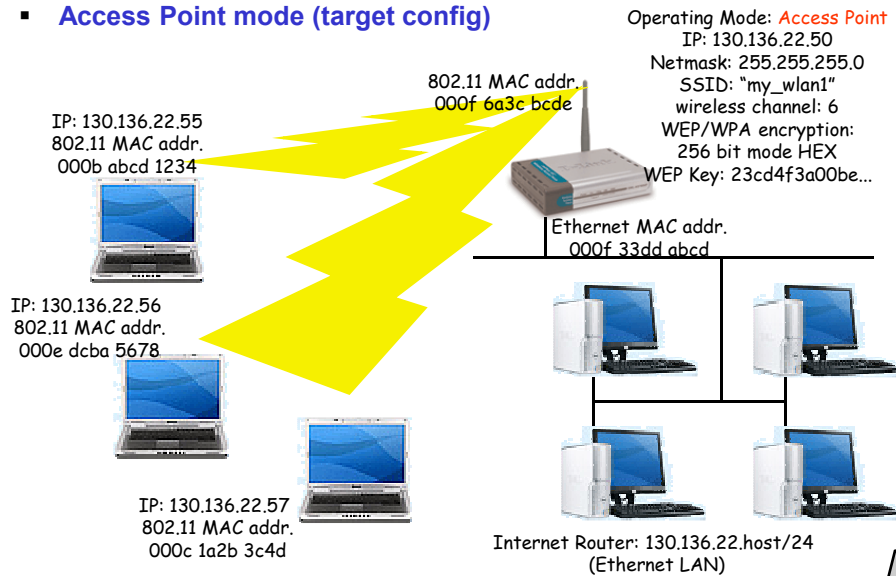
Sistemi e Reti Wireless

16



## Configuration of a Wireless Network

- Access Point mode (target config)



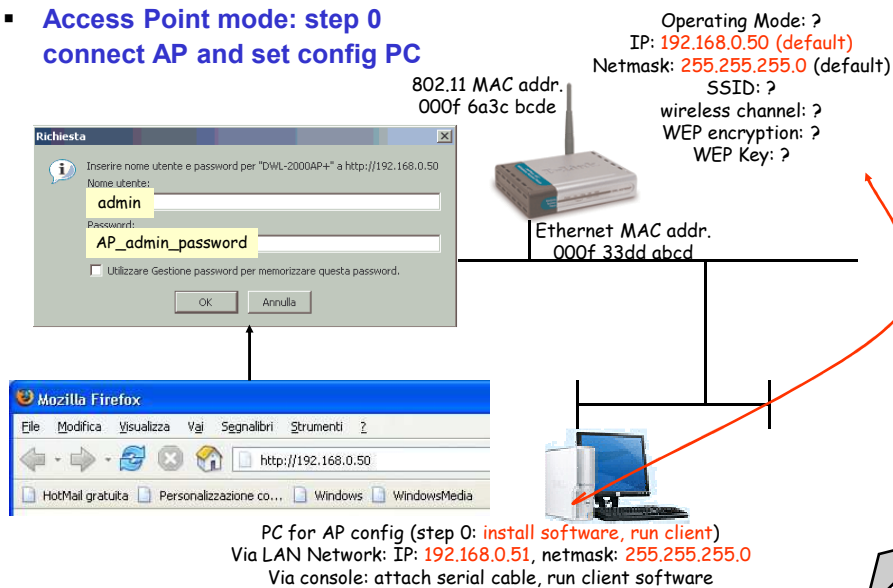
© 2005 Luciano Bononi

Sistemi e Reti Wireless

17

## Configuration of a Wireless Network

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



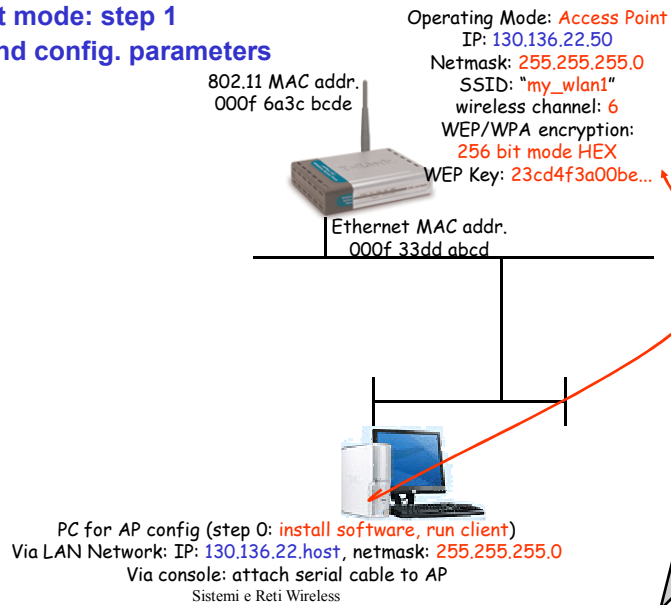
© 2005 Luciano Bononi

Sistemi e Reti Wireless

18

## Configuration of a Wireless Network

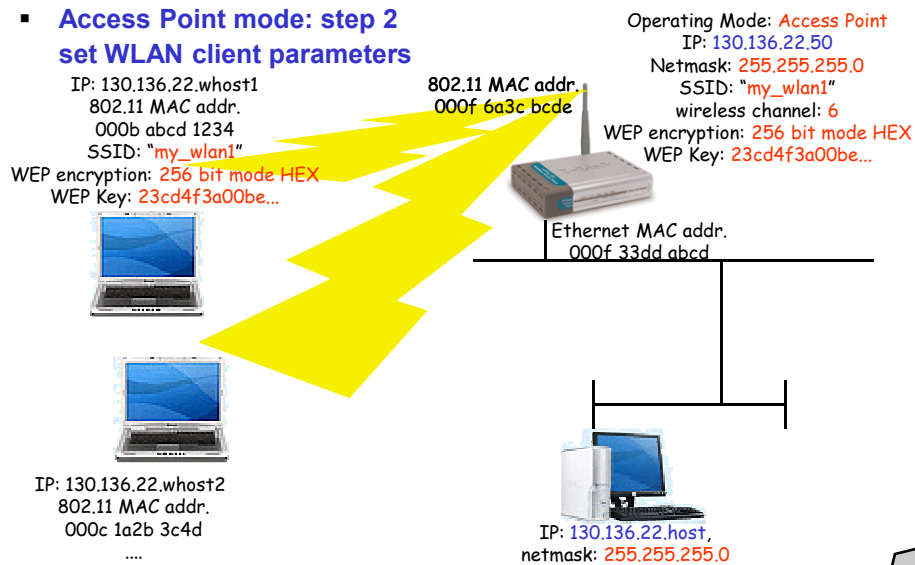
- Access Point mode: step 1  
set LAN IP and config. parameters



19

## Configuration of a Wireless Network

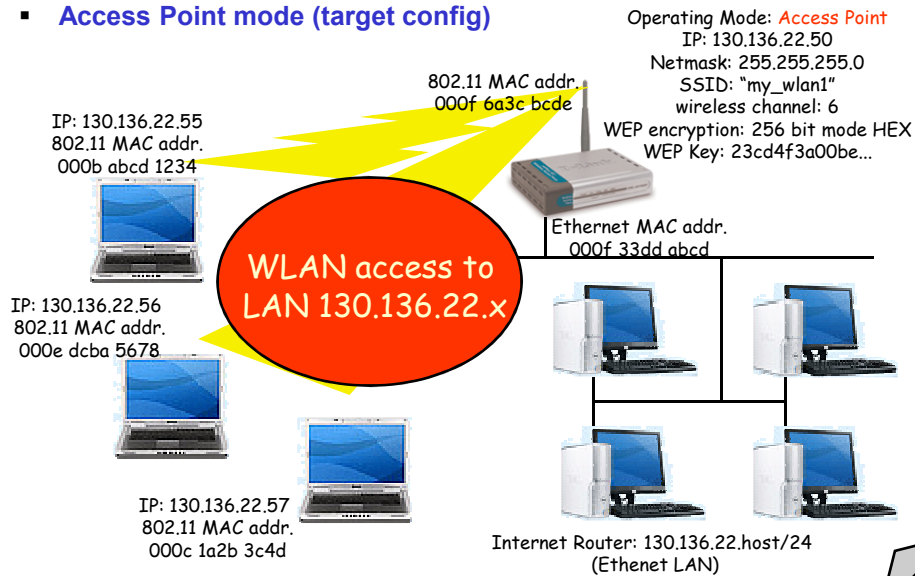
- Access Point mode: step 2  
set WLAN client parameters



20

## Configuration of a Wireless Network

### Access Point mode (target config)



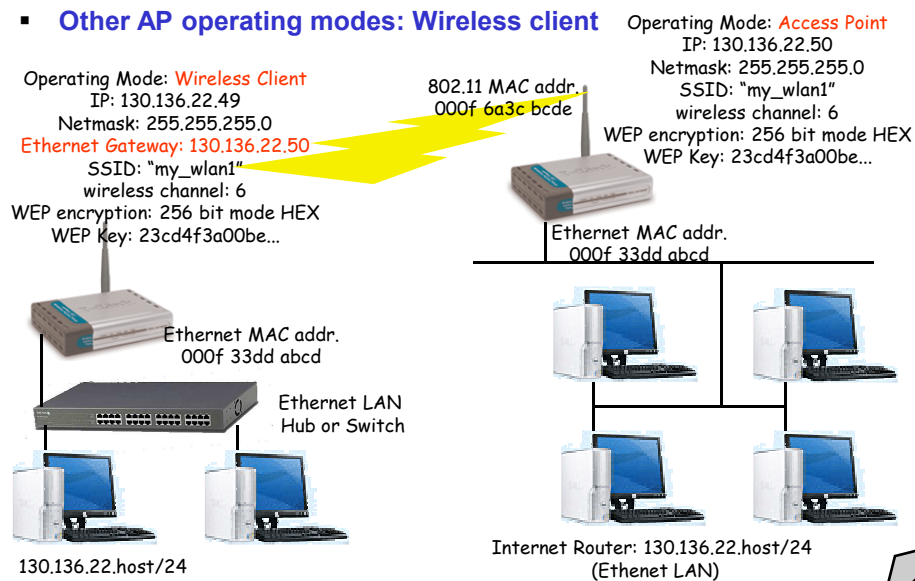
© 2005 Luciano Bononi

Sistemi e Reti Wireless

21

## Configuration of a Wireless Network

### Other AP operating modes: Wireless client



© 2005 Luciano Bononi

Sistemi e Reti Wireless

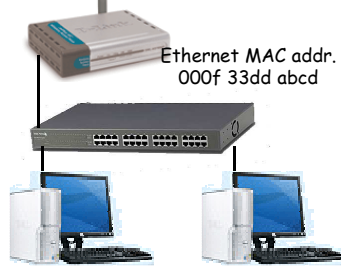
22

## Configuration of a Wireless Network

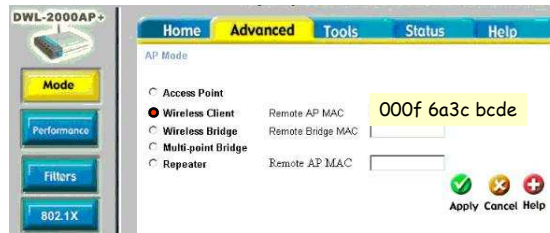
### Other AP operating modes: Wireless client

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 6a3c bcde



130.136.22.host/24



© 2005 Luciano Bononi

Sistemi e Reti Wireless

23

## Configuration of a Wireless Network

### Other AP operating modes: Wireless Bridge Mode

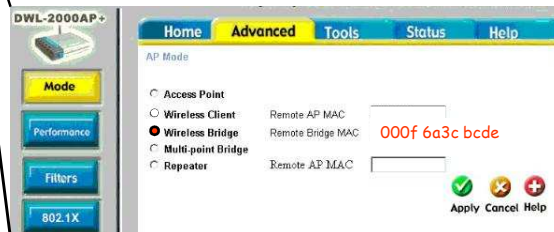
Only the two APs can wirelessly connect each other!



802.11 MAC: 000f 6a3c bcde  
 SSID: "my\_two\_bridged\_LANs"  
 wireless channel: 6  
 WEP encryption: 256 bit mode HEX  
 WEP Key: 23cd4f3a00be...



Only two APs can connect each other!  
 SSID: "my\_two\_bridged\_LANs"  
 wireless channel: 6  
 WEP encryption: 256 bit mode HEX  
 WEP Key: 23cd4f3a00be...



© 2005 Luciano Bononi

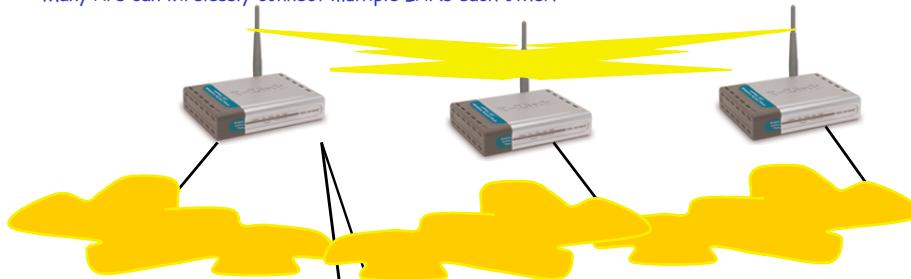
Sistemi e Reti Wireless

24

## 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...

DWL-2000AP+ configuration interface showing the 'Advanced' tab. The 'AP Mode' section has the following options:

- Access Point
- Wireless Client
- Wireless Bridge
- Multi-point Bridge
- Repeater

Fields for Remote AP MAC, Remote Bridge MAC, and Remote AP MAC are visible. The 'Apply' button is highlighted.

## 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...

DWL-2000AP+ configuration interface showing the 'Advanced' tab. The 'AP Mode' section has the following options:

- Access Point
- Wireless Client
- Wireless Bridge
- Multi-point Bridge
- Repeater

The 'Remote AP MAC' field is populated with the value '000f 6a3c bcde'. The 'Apply' button is highlighted.

## Configuration of a Wireless Network

- Typical AP config. Mask: general configuration parameters



The screenshot shows the configuration interface for a D-Link DWL-2000AP+ wireless access point. The page has a sidebar with navigation buttons for Wizard, Wireless, LAN, and DHCP. The main content area is titled 'Wireless Settings' and includes the following fields and options:

- AP Name: DWL-2000AP+
- SSID: default
- Channel: 6
- Authentication:  Open System  Shared Key  WPA  WPA-PSK
- WEP:  Enabled  Disabled
- WEP Encryption: 64Bit
- WEP Mode: HEX
- Key1: 1234512345
- Key2: 0000000000
- Key3: 0000000000
- Key4: 0000000000

## Configuration of a Wireless Network

- Typical AP config. Mask: LAN IP address



The screenshot shows the configuration interface for a D-Link DWL-2000AP+ wireless access point, specifically the LAN Settings section. The page header includes the D-Link logo and 'AirPlus Xtreme G+ High-Speed 2.4GHz Wireless Access Point'. The sidebar has navigation buttons for Wizard, Wireless, LAN, and DHCP. The main content area is titled 'LAN Settings' and includes the following fields and options:

- LAN IP:  Dynamic IP Address  Static IP Address
- IP Address: 192.168.0.52
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.0.52

At the bottom right of the form, there are three icons: a green checkmark, a red X, and a red plus sign, with the text 'Apply Cancel Help' below them.

## Configuration of a Wireless Network

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



The screenshot shows the configuration interface for a D-Link DWL-2000AP+ wireless access point. The page title is "AirPlus Xtreme G+ High-Speed 2.4GHz Wireless Access Point". The "Status" tab is selected, displaying the following information:

Device Information	
Firmware Version 1.13 , 18 Feb 2004	
<b>Ethernet</b>	
MAC Address	0005d34cccc
IP Address	192.168.0.52
Subnet Mask	255.255.255.0
Gateway	192.168.0.50
<b>Wireless</b>	
MAC Address	0005d34c69
SSID	default
Encryption Function	64 bits
Channel	6

## Configuration of a Wireless Network

- Typical AP config. Mask: set AP operating mode



The screenshot shows the configuration interface for a D-Link DWL-2000AP+ wireless access point. The "Advanced" tab is selected, displaying the "AP Mode" configuration options:

Mode	Remote AP MAC
<input type="radio"/> Access Point	
<input checked="" type="radio"/> Wireless Client	0003d34cccc
<input type="radio"/> Wireless Bridge	
<input type="radio"/> Multi-point Bridge	
<input type="radio"/> Repeater	

Buttons: Apply, Cancel, Help

## Configuration of a Wireless Network

- Typical AP config. Mask: check MAC layer connection



The screenshot shows the configuration page for a D-Link DWL-2000AP+ wireless access point. The 'Status' tab is selected, displaying traffic statistics. The page includes a sidebar with navigation buttons for Device Info, Log, Stats, and Wireless. The main content area shows Ethernet and Wireless statistics.

Ethernet		
Send	Good Packets	1240
	Dropped Packets	0
Recv	Good Packets	1177
	Dropped Packets	0

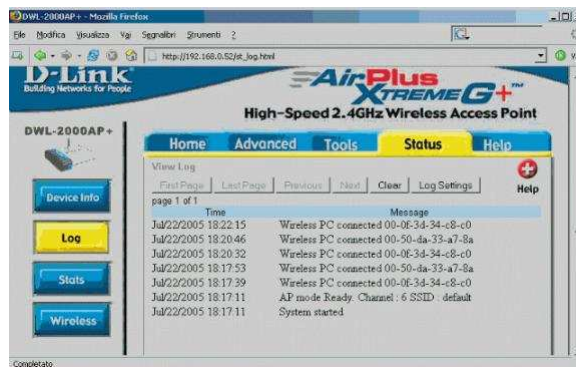
  

Wireless		
Send	Good Packets	0
	Dropped Packets	0
Recv	Good Packets	0
	Dropped Packets	0



## Configuration of a Wireless Network

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



The screenshot shows the configuration page for a D-Link DWL-2000AP+ wireless access point. The 'Status' tab is selected, displaying the connection log. The page includes a sidebar with navigation buttons for Device Info, Log, Stats, and Wireless. The main content area shows a log of connection events.

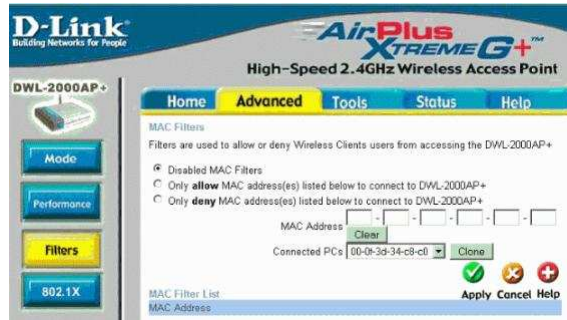
Time	Message
Jul22/2005 18:22:15	Wireless PC connected 00-0E-34-34-c8-c0
Jul22/2005 18:20:46	Wireless PC connected 00-50-da-33-a7-8a
Jul22/2005 18:20:32	Wireless PC connected 00-0E-34-34-c8-c0
Jul22/2005 18:17:53	Wireless PC connected 00-50-da-33-a7-8a
Jul22/2005 18:17:39	Wireless PC connected 00-0E-34-34-c8-c0
Jul22/2005 18:17:11	AP mode Ready Channel : 6 SSID : default
Jul22/2005 18:17:11	System started





## Configuration of a Wireless Network

- Typical AP config. Mask: MAC filtering

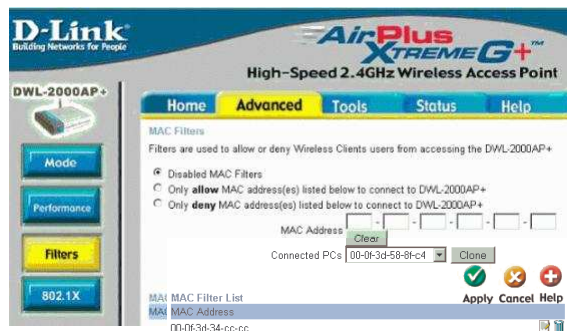


The screenshot shows the configuration page for a D-Link DWL-2000AP+ wireless access point. The interface is titled "AirPlus Xtreme G+ High-Speed 2.4GHz Wireless Access Point". The "Advanced" tab is selected. Under the "MAC Filters" section, the "Disabled MAC Filters" radio button is selected. Below this, there are three radio button options: "Only allow MAC address(es) listed below to connect to DWL-2000AP+", "Only deny MAC address(es) listed below to connect to DWL-2000AP+", and "Only deny MAC address(es) listed below to connect to DWL-2000AP+". The "MAC Address" field is empty, and the "Connected PCs" dropdown menu shows "00-0F-3D-34-C8-C0". There are "Clear" and "Clone" buttons. At the bottom, there is a "MAC Filter List" table with columns for "MAC Filter List" and "MAC Address".



## Configuration of a Wireless Network

- Typical AP config. Mask: MAC filtering



The screenshot shows the same configuration page as above, but with the "MAC Filter List" table populated. The table has two columns: "MAC Filter List" and "MAC Address". The first row shows "MAC Filter List" with a checkmark icon and "MAC Address" with the value "00-0F-3D-34-CC-CC".

