


# Nomadic Communications Labs



Alessandro Villani  
avillani@science.unitn.it



# IEEE 802.11b in brief

# IEEE 802.11b in brief

---

- ❑ The 802.11b standard belong to the family of IEEE 802 standard regarding the Local Area Network (LAN) specifications
- ❑ For instance:
  - 802.3 specify Ethernet and CSMA/CD
  - 802.1q specify VLAN
- ❑ The published standards are availables at the address:

<http://standards.ieee.org/getieee802/portfolio.html>

# IEEE 802.11b in brief : Frequencies

---

- ❑ 802.11b works in ISM (*Industrial, Scientific and Medical*) band at 2.4 GHz
- ❑ These frequencies are unlicensed!

<b>Regions</b>	<b>Frequencies</b>
USA	2.4000 – 2.4835 GHz
Europe	2.4000 – 2.4835 GHz
France	2.4465 – 2.4835 GHz
Spain	2.4450 – 2.4750 GHz
Japan	2.4000 – 2.4835 GHz 2.4710 – 2.4970 GHz

# IEEE 802.11b in brief : Frequencies

---

- In Europe: 13 Channels
- The following table summarize the usable channels:

<b>Regions</b>	<b>Channels (5MHz)</b>
USA	1 - 11
Europe	1 - 13
Japan	1 - 13 + 14
France	10 - 13
Spain	10 - 11

# IEEE 802.11b in brief : Frequencies

- The central frequency of each channel is shown in the table
- Central channel frequencies are separated by 5MHz
- A channel bandwidth is 22 MHz
- To avoid interferences, channels in the same area must be 25 MHz apart

3 non-overlapping channels:

(USA) 1,6,11

(EU) 1,7,13 or 1,6,11 or  
2,8,13, or ...

Channel	Frequencies
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz
12	2467 MHz
13	2472 MHz

# IEEE 802.11b in breve: Frequenze

---

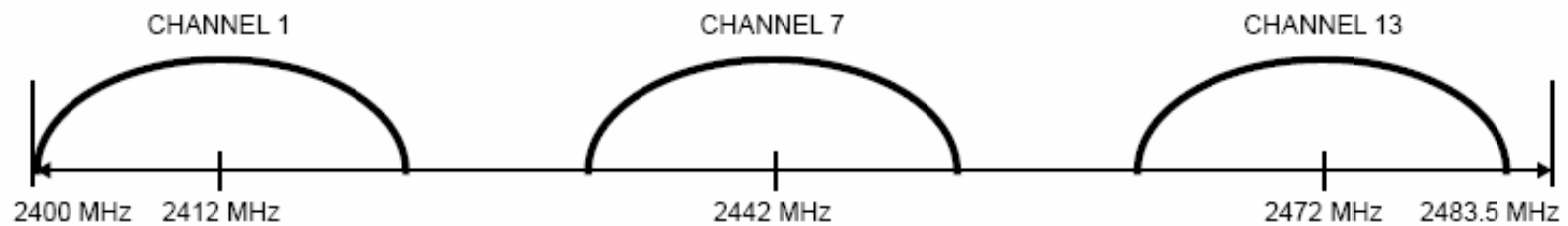


Figure 143—European channel selection—non-overlapping



Figure 144—European channel selection—overlapping

# IEEE 802.11b in brief : Power

---

- The power which can be irradiated depends by the geographic areas

<b>Maximum Power Permitted</b>	<b>Region</b>
1000 mW	USA
100 mW	Europe
10 mW	Japan



# IEEE 802.11b in brief : Speed

---

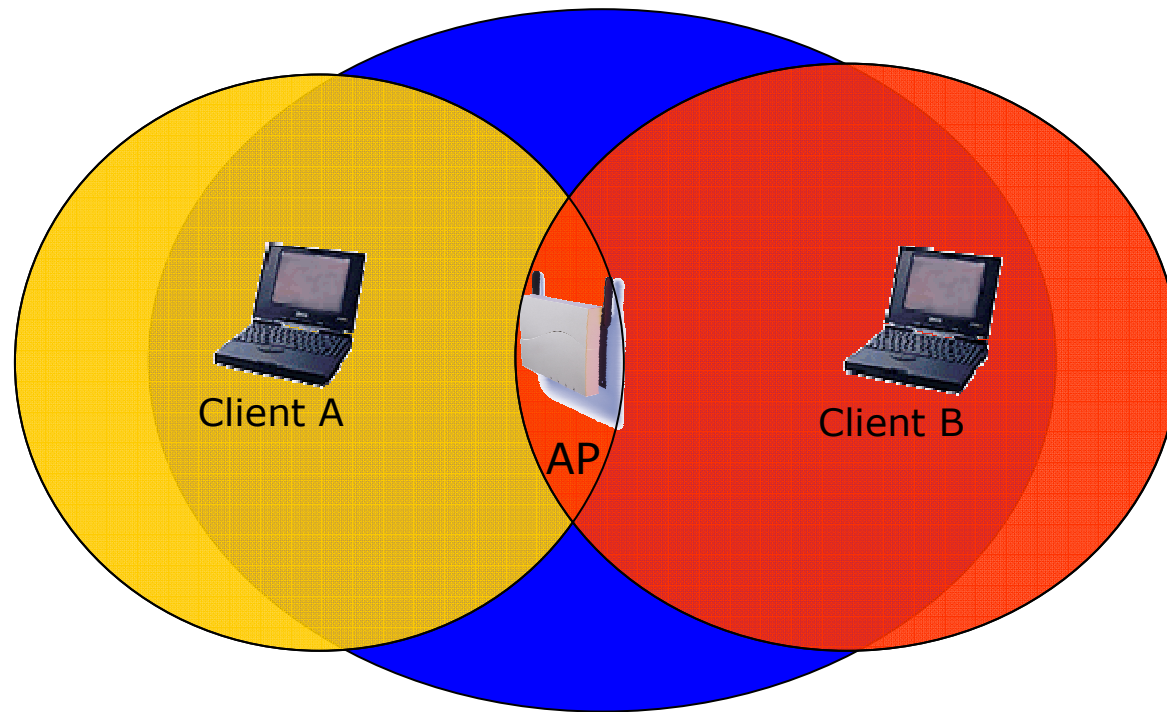
- The transmission speeds supported by the standard are:  
1, 2, 5.5, 11 Mbps
- The speed depends by the distance (channel conditions)
- The following table shows what is declared by Avaya for the its NICs in ideal propagation conditions:

<b>Type of area</b>	<b>11 Mbs</b>	<b>5,5 Mbs</b>	<b>2 Mbs</b>	<b>1 Mbs</b>
Open	160 m	270 m	400 m	550 m
Semi-Open	50 m	70 m	90 m	115 m
Close	25 m	35 m	40 m	50 m

# IEEE 802.11b in brief: RTS/CTS

---

## □ Hidden Node Problem:



- A talk with AP (but not with B)
- B talk with AP (but not with A)

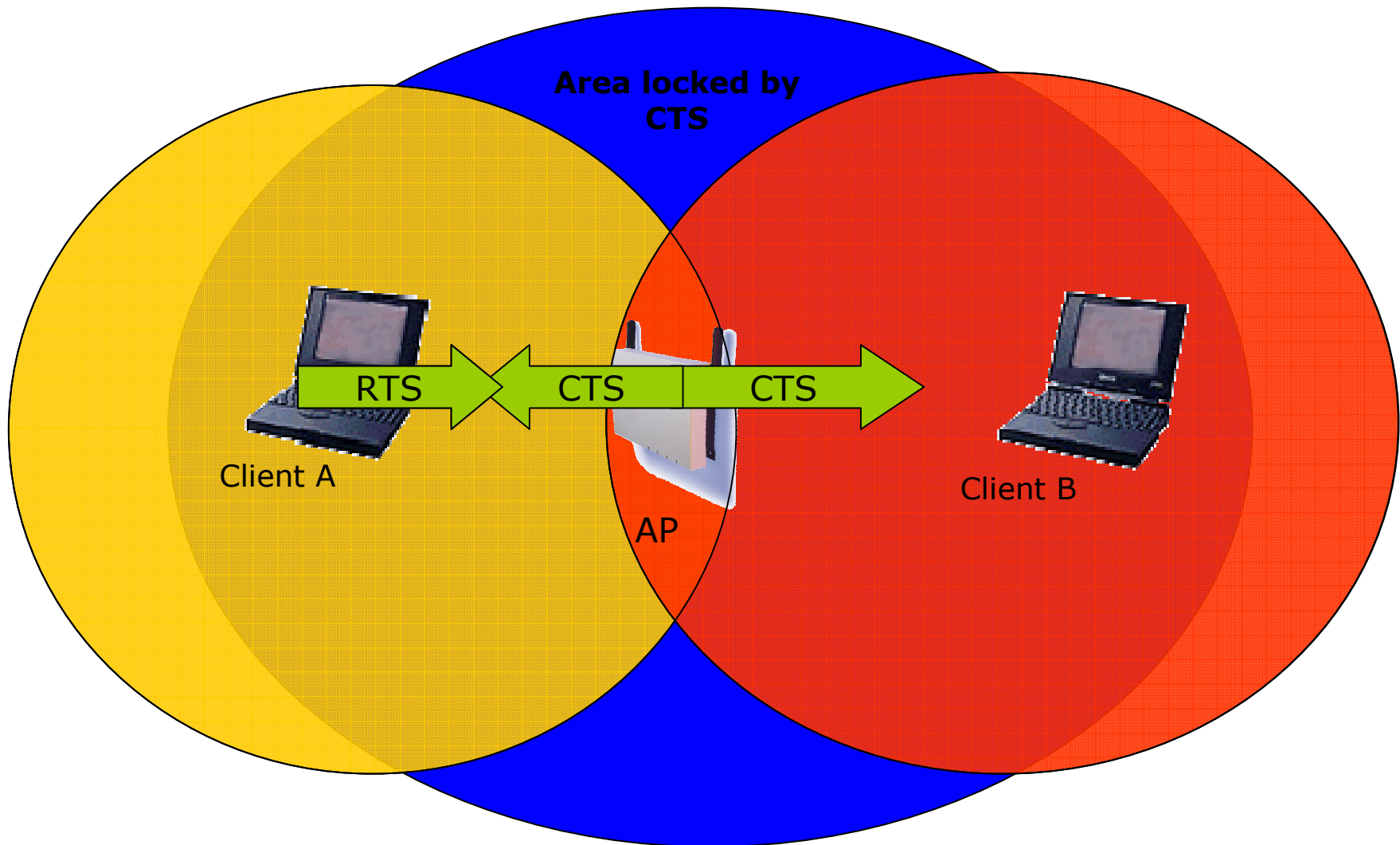
# IEEE 802.11b in brief: RTS/CTS

---

- B starts to transmit
- A does not hear B so starts to transmit →  
**COLLISION**
- To prevent this situation the standard define the mechanism of RTS/CTS:
  - the packets longer than an assigned threshold are transmitted only after a RTS/CTS exchange

# IEEE 802.11b in brief: RTS/CTS

---



# IEEE 802.11b in brief: WEP

---

- ❑ 802.11 defines a mechanism to protect the data privacy and authenticate AP/Mobile Stations :
  - WEP (Wired Equivalent Privacy)
- ❑ The encryption algorithm is a RC4 (a system of encryption based on a shared key)
- ❑ The shared key is long 40 bits and is concatenated to a long vector of initialization (IV) with a length of 24 bits  
→ key to 64 bits

# IEEE 802.11b in brief: WEP

---

- ❑ Evolution from the standard: key of 128 bits, with shared key of 104 bit and IV of 24 bits
- ❑ Have been highlighted weaknesses of WEP and of his implementations (too short key, foreseeable IV).

# IEEE 802.11b in brief: BSS/ESS

---

- ❑ One AP and the mobile stations associated to it define a *Basic Service Set* (BSS).
- ❑ Two or more attached BSS form together an *Extended Set Service* (ESS) if they supply the additional services (support for roaming)
- ❑ The *Independent Basic Service Set* (IBSS), is the simplest form → Ad Hoc Network

# IEEE 802.11b in brief: SSID

---

- ❑ The SSID (*Service Set IDentity*) is a string identifying the WLAN (32 bytes max)
- ❑ The SSID of length 0 corresponds to a broadcast identity and is used in probing the available nets
- ❑ On many AP you can inhibit the transmission of SSID, so that only who knows the SSID of the WLAN can join it (poor protection indeed! you can configure the card to scan other cards associations)



# IEEE 802.11b in brief: DTIM

---

- **DTIM Period.** The *Delivery Traffic Indicator Map* (DTIM) is used by the client when in power saving mode
- It is used to specify to the AP how many periods of beacon the client will be in power saving mode and when it will be “awake” and able to find out if there are data directed to the client itself



# Set up of an Access Point Avaya Ap3

# Access Point: Avaya AP3

---

- Access Point Avaya AP3
- Configurable via serial port:
  - Null-Modem cable
  - Baud Rate: 9600
  - Parity: none
  - Data bit: 8
  - Stop bit: 1
  - Flow Control: none
  - Default passwd: public
  - Line feed con Carriage Returns

# Avaya AP : Boot

---

```
=====  
PowerOn Selftests  
=====
```

Running SDRAM test.....OK

SDRAM Size: 16 Mbyte

CPU id: 4401a104

CPU Frequency: 228.1 MHz

Checking timers....OK

FLASH Manufacturer: Intel (89)

FLASH Device: E28F320J3A(16)

FLASH Size: 8 Mbyte (32 blocks of 256  
kbyte each)

Scanning PCI-Bus...

```
SYSTEM SLOT  
=====
```

Vendor ID: Intel Corporation (1011)

Device ID: 21285 (1065)

SLOT: 1

```
=====
```

Vendor ID: National Semiconductor  
(100b)

Device ID: DP83815 (0020)

SLOT: 2

```
=====
```

Vendor ID: Texas Instruments (104c)

Device ID: PCI1225 (ac1c)

SLOT: 3

```
=====
```

EMPTY

```
=====
```

Selftests OK

```
=====
```

Executing Original BSP/BootLoader.  
Version 2.0.10

Loading image...2641768 + 276792 +  
2441816

[Avaya Wireless AP-3]> Please enter  
password:

# Avaya AP : Configure via CLI

---

- ❑ Available commands list : ?
- ❑ For a short command description do not specify any parameter :

```
[Avaya-Wireless-AP-3]> reboot
```

Command Description:

The reboot command reboots the device in the specified number of seconds.

Command Usage:

```
reboot <number of seconds> <CR>
```

Examples:

```
reboot 0 <CR>
```

```
reboot 100 <CR>
```

# Avaya AP : Configure via CLI

---

- ❑ List of the parameters available:  
show ?
- ❑ List of the parameters beginning for ip:  
show ip?
- ❑ For the list of the settable parameters  
(beginning for ip):  
set ip?

# Avaya AP : Configuration

---

- ❑ The default IP address of the Avaya AP is 10.0.0.1
- ❑ So it is possible to reach them also via network using a cross cable or a switch/hub and using an IP in the same subnet
- ❑ Together with the software enclosed there it is a tool to find all the AP connected to the network

# Avaya AP: Assigning the IP Address

---

## □ To assign an IP address to the AP:

```
[Avaya Wireless AP-3]> set ipaddrtype static
```

```
[Avaya Wireless AP-3]> set ipaddr 192.168.91.123
```

```
[Avaya Wireless AP-3]> set ipgw 192.168.91.1
```

```
[Avaya Wireless AP-3]> show network
```

```
IP/Network Group Parameters
```

```
=====
```

IP Address	:	192.168.91.123
Subnet Mask	:	255.0.0.0
Default Router	:	192.168.91.1
Default TTL	:	64
Address Type	:	static



# Avaya AP: WEB Interfaces

The screenshot shows a Microsoft Internet Explorer browser window displaying the Avaya AP web interface. The address bar shows `http://192.168.91.123/`. The interface features a navigation sidebar on the left with buttons for Status, Configure, Monitor, Commands, Help, and Exit. The main content area is titled "System Status" and displays the following information:

**System Status**

Avaya Wireless AP-3 v2.0.0(266) SN-03UT05560066 v2.0.10

IP Address	192.168.91.123	Contact Name	Contact Name
System Name	Avaya Wireless AP-3	Contact Phone	Contact Phone Number
System Location	Contact Location	Contact Email	name@Organization.com
Up Time (DD:HH:MM:SS)	00:00:47:23	Object ID	1.3.6.1.4.1.11898.2.4.6

**System Alarms**

This table displays information on the alarms (SNMP Traps) generated by the access point. They should be deleted once they are reviewed and resolved. The alarm severity levels are: Critical, Major, Minor, and Informational.

Select All      Deselect All

Description	Severity	Time Stamp
<input type="checkbox"/> Incompatible Vendor for Wireless Card. Card Info : PC Card A	Critical	0 days 0 hrs 0 m 0 s
<input type="checkbox"/> Wireless Card Not Present. Card Info : PC Card B	Informational	0 days 0 hrs 0 m 0 s
<input type="checkbox"/> AP Cold Started.	Informational	0 days 0 hrs 0 m 3 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 3 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 3 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 3 s
<input type="checkbox"/> Link Up.	Informational	0 days 0 hrs 0 m 3 s
<input type="checkbox"/> Wireless Card Not Present. Card Info : PC Card B	Informational	0 days 0 hrs 0 m 8 s
<input type="checkbox"/> Incompatible Vendor for Wireless Card. Card Info : PC Card A	Critical	0 days 0 hrs 0 m 8 s

Delete

Downloading from site: res://C:\WINDOWS\System32\shdocl.dll\dnserror.htm

# Avaya AP: Updating the Firmware

---

- ❑ This Access Point now is in End Of Life!
- ❑ The firmware is still available at the address:

<http://support.avaya.com/>

- ❑ The last version available is the version 2.5.5

# Avaya AP: Updating the Firmware

---

- ❑ To update the firmware a tftp server (Transfer Protocol file Trivial) can be used
- ❑ Using the CLI:

```
[Avaya-Wireless-AP-3]> download 193.205.194.21 Avaya/AV_AP3.bin img  
File Avaya/AV_AP3.bin is being downloaded from 193.205.194.21.
```

```
File Avaya/AV_AP3.bin has been downloaded successfully.
```

```
[Avaya Wireless AP-3]> reboot 0
```

# Avaya AP: Updating the Firmware

The screenshot shows a Microsoft Internet Explorer browser window titled "Download Command - Microsoft Internet Explorer". The address bar displays "http://192.168.91.123/cmd/download.html". The page features the Avaya logo at the top left and a navigation menu with tabs for "Download", "Upload", "Reboot", "Reset", and "Help Link". The "Download" tab is active, displaying instructions: "This tab is used to download software and configuration files from a TFTP server to the access point. This can be used for software upgrades." Below this, there are two sections: "System Information" and "TFTP Information".

**System Information**

Software Version	2.0.0
Boot Loader Version	2.0.10

**TFTP Information**

Server IP Address	<input type="text" value="193.205.194.21"/>
File Name	<input type="text" value="Avaya/AV_AP3.bin"/>
File Type	<input type="text" value="Img"/>
File Operation	<input type="text" value="Download"/>

At the bottom of the form are "OK" and "Cancel" buttons. A left sidebar contains buttons for "Status", "Configure", "Monitor", "Commands", "Help", and "Exit". The browser's status bar at the bottom shows "Done" and "Internet".

# Avaya AP: Wireless Interfaces

---

- In these AP different types of cards can be inserted with different properties:
  - Two maximum lengths for the WEP key are supported (Silver: 64, Gold: 128)
  - Different cards for the various channel sets (ETSI: Canali 1-13, World: Canali 1-11) are available
  - Besides the 802.11b cards there are 802.11a and 802.11b/g cards

# Avaya AP: Wireless Interfaces

---

- Besides the net parameters we will have to set up for the wireless interface
  - The channel to use:
    - We can chose the automatic channel option
  - The SSID of the WLAN:
    - We can enable the Closed System option: the AP are not authorized to connect the terminals with the SSID *any*
  - The threshold for the activation of RTS/CTS:
    - Disabled by default

# Avaya AP: Wireless Interfaces

---

- ❑ Based on the module/model it is possible to define:
  - More than one SSID on the same wireless interfaces
  - The standard adopted
  - The supported speeds
  - The power used
- ❑ Other important configurations:
  - Modify the administrator password
  - Set up the WEP key
  - Configure the IP of a syslog or SNMP server
  - Enable a radius server for the MAC address check
  - Enable an 802.1x server

# Avaya AP: Wireless Interfaces

---

- For instance using the 802.11b/g radio module, several SSID can be managed on the same AP :
  - Each SSID is associated to a distinct VLAN
  - For each SSID a different security profile can be associated with different parameters for the authentication method, for the accounting radius servers , ...



# Avaya AP: Wireless Interfaces

The screenshot shows a web browser window with the address `http://172.31.194.19/cfg/sec-gen34-a.html`. The interface includes a left sidebar with 'Help' and 'Exit' buttons. The main content area contains a warning message, a note about SSID and VLAN ID uniqueness, and a section for configuring security profiles. Below this is a form with various status and profile settings, and a table for SSID and VLAN data.

The user must specify unique SSIDs and VLAN IDs values (only a single untagged VLAN ID can be configured).

**Security Profiles** are used to configure the allowed security modes. If RADIUS MAC, 802.1x, WPA or RADIUS accounting is enabled in the SSID's security profile then the respective **RADIUS server profiles** should be configured and assigned to this SSID.

*Note: Changes to these parameters require access point reboot in order to take effect.*

Enable Security Per SSID

Accounting Status: Enable  
RADIUS MAC Authentication Status: Disable  
MAC ACL Status: Disable  
Rekeying Interval (seconds): 900  
Security Profile: 1  
RADIUS MAC Authentication Profile: MAC Authentication  
RADIUS EAP Authentication Profile: EAP Authentication  
RADIUS Accounting Profile: Accounting

OK Cancel

**SSID and VLAN Data Table**

Add Edit

Index	Network Name (SSID)	VLAN ID	Status
1	WILMA	2	Enable
2	unitn-wifi	31	Enable



# Configuration of CISCO AP 1200 Series

# AP 1200: Features

---

- ❑ With the last firmware (version 12.3(8)JA) the AP supports:
  - Multiple SSID (up to 16), for each one it is possible to choose:
    - ❑ If transmitting in broadcast the SSID (guests mode)
    - ❑ The method of authentication
    - ❑ The maximum number of customers
    - ❑ VLAN: a VLAN for each SSID
  - Authentication Methods:
    - ❑ MAC Address
    - ❑ 802.1x
    - ❑ WPA

# AP 1200: Initial Configuration

---

- Configuration using serial port
  - 9600 baud
  - 8 data bits
  - Parity none
  - stop bit 1
  - flow control no

# AP 1200: Initial Configuration

---

## □ “Standard” CISCO commands:

- enable
- *Password* → Cisco
- `configure [terminal]`
- `ip default-gateway 192.168.10.1`
- `interface FastEthernet 0`
- `ip address 192.168.10.40 255.255.255.0`
- exit
- Ctrl-z
- `copy running-config startup-config`
- reload

# AP 1200: Initial Configuration

---

- ❑ To display the initial configuration:
  - Enable
  - Password: Cisco
  - `show running-config`
- ❑ The network interface to configure in the current release of the firmware is BVI 1 (not FastEthernet 0 as in the previous versions)

# AP 1200: WEB Interface

- After the first configuration via CLI:

HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Hostname CISCO1200-NetworkLab

## Express Set-Up

Host Name:	<input type="text" value="CISCO1200-NetworkLab"/>
MAC Address:	<input type="text" value="000d.2967.cef5"/>
Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address:	<input type="text" value="192.168.10.40"/>
IP Subnet Mask:	<input type="text" value="255.255.255.0"/>
Default Gateway:	<input type="text" value="192.168.10.1"/>
SNMP Community:	<input type="text" value="defaultCommunity"/>
	<input checked="" type="radio"/> Read-Only <input type="radio"/> Read-Write

## Radio0-802.11B

Role in Radio Network:	<input checked="" type="radio"/> Access Point Root <input type="radio"/> Repeater Non-Root
Optimize Radio Network for:	<input checked="" type="radio"/> Throughput <input type="radio"/> Range <input type="radio"/> <a href="#">Custom</a>
Aironet Extensions:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

# AP 1200: Firmware Update

---

- The Firmware is downloadable from the CISCO WEB Site:
  - <http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=wireless>
  - You have to register at least as guest user
  - The current version is: c1200-k9w7-tar.123-8.JEA1.tar
  - The AP firmware can be updated via tftp or via http



# AP 1200: Firmware Update

## □ Firmware Update via HTTP

Back Forward Reload Stop

Home Status Window for Software Upgrade Support Shop Products Training

**CISCO SYSTEM**

HOME  
EXPRESS SET  
NETWORK MA  
ASSOCIATION  
NETWORK  
INTERFACES  
SECURITY  
SERVICES  
WIRELESS SE  
SYSTEM SOFT

Software Upg  
System Configuration  
EVENT LOG +

**Please wait...**

The system is upgrading the software and restarting. This should take between 5 and 15 minutes depending on your network speed.

00:15 time elapsed

**ss Point**

TFTP UPGRADE

CISCO1200-N

TFTP Upgrade

c1200-k9w7-tar.122-11.JA  
12.2(11)JA  
12.2(8)JA

TFTP File Server: 192.168.10.10 (server name or IP address)

Upgrade System Software Tar File: Upgrade c1200-k9w7-tar.123-2.JA.tar (path/filename)

Close Window Copyr

# AP 1200: Password Administrator

- We can define more than a user with different capabilities

The screenshot shows the configuration page for the Password Administrator on a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CISCO1200-NetworkLab" and the uptime is "2 da".

The left sidebar contains a navigation menu with the following items:

- HOME
- PRESS SET-UP
- PRESS SECURITY
- WORK MAP +
- OCIATION +
- WORK ERFACES +
- URITY
- Admin Access
- cription Manager
- id Manager
- rver Manager
- ical RADIUS Server
- vanced Security
- VICES +
- ELESS SERVICES +
- ITEM SOFTWARE +
- ENT LOG +

The main content area is titled "Security: Admin Access". It contains the following sections:

- Administrator Authenticated by:** A radio button selection with four options:
  - Default Authentication (Global Password)
  - Local User List Only (Individual Passwords)
  - Authentication Server Only
  - Authentication Server if not found in Local ListAn "Apply" button is located to the right.
- Default Authentication (Global Password):** A section for configuring the global password.
  - Default Authentication Password:** A text input field containing "\*\*\*\*\*".
  - Confirm Authentication Password:** A text input field containing "\*\*\*\*\*".An "Apply" button is located to the right.
- Local User List (Individual Passwords):** A section for configuring individual users.
  - User List:** A list box containing "Cisco" and a "Delete" button.
  - Username:** A text input field containing "Cisco".
  - Password:** A text input field containing "\*\*\*\*\*".
  - Confirm Password:** A text input field.
  - Capability Settings:** Radio button selection with two options:
    - Read-Only
    - Read-WriteAn "Apply" button is located to the right.

# AP 1200: Wireless Configuration

---

## □ Role in a Wireless Network:

- Root or repeater

## □ Speed:

- Basic: unicast and multicast traffic, used from the highest to the lowest. At least one must be set up.
- Enabled: Unicast traffic only
- Disabled: This speed is not usable

## □ Power:

- It is possible to limit the power (in transmission) of the client stations (CISCO extensions)

# AP 1200: Wireless Configuration

## □ Configuration of the basic parameters

The screenshot displays the configuration page for Radio0-802.11B on a Cisco AP 1200. The page is divided into several sections:

- Hostname:** CISCO1200-NetworkLab
- Uptime:** CISCO1200-NetworkLab uptime is 3
- Network Interfaces: Radio0-802.11B Settings**
  - Enable Radio:**  Enable  Disable
  - Current Status (Software/Hardware):** Enabled  Up
  - Role in Radio Network:** (Fallback mode upon loss of Ethernet connection)
    - Access Point Root (Fallback to Radio Island)
    - Access Point Root (Fallback to Radio Shutdown)
    - Access Point Root (Fallback to Repeater)
    - Repeater Non-Root
  - Data Rates:**  Best Range  Best Throughput
    - 1.0Mb/sec  Require  Enable  Disable
    - 2.0Mb/sec  Require  Enable  Disable
    - 5.5Mb/sec  Require  Enable  Disable
    - 11.0Mb/sec  Require  Enable  Disable
  - Transmitter Power (mW):**  1  5  20  30  50  Max
  - Limit Client Power (mW):**  1  5  20  30  50  Max
  - Default Radio Channel:** Least Congested Frequency Channel 10 2457 MHz
  - Least Congested Channel Search:** (Use Only Selected Channels)
    - Channel 1 - 2412 MHz
    - Channel 2 - 2417 MHz
    - Channel 3 - 2422 MHz
    - Channel 4 - 2427 MHz
    - Channel 5 - 2432 MHz
    - Channel 6 - 2437 MHz
    - Channel 7 - 2442 MHz
    - Channel 8 - 2447 MHz
    - Channel 9 - 2452 MHz
    - Channel 10 - 2457 MHz

# AP 1200: Wireless Configuration

---

## □ World Mode:

- Clients can receive “national” information about setting. Legacy for CISCO compatibility, 802.11d new standards

## □ Antenna:

- Diversity: both antennas are used and the one that receives the best signal is chosen

## □ Encapsulation:

- To manage the non 802.3 packages, these have to be encapsulated. Interoperability with others: RFC1042; 802.1H optimized for CISCO

# AP 1200: Wireless Configuration

---

## □ RTS:

- Choose low values if not all of the stations are within sensing range of each other

## □ Fragmentation:

- Choose low values if the area is disturbed or with low transmission quality

## □ CISCO Extension:

- Used to support special features

# AP 1200: Wireless Configuration

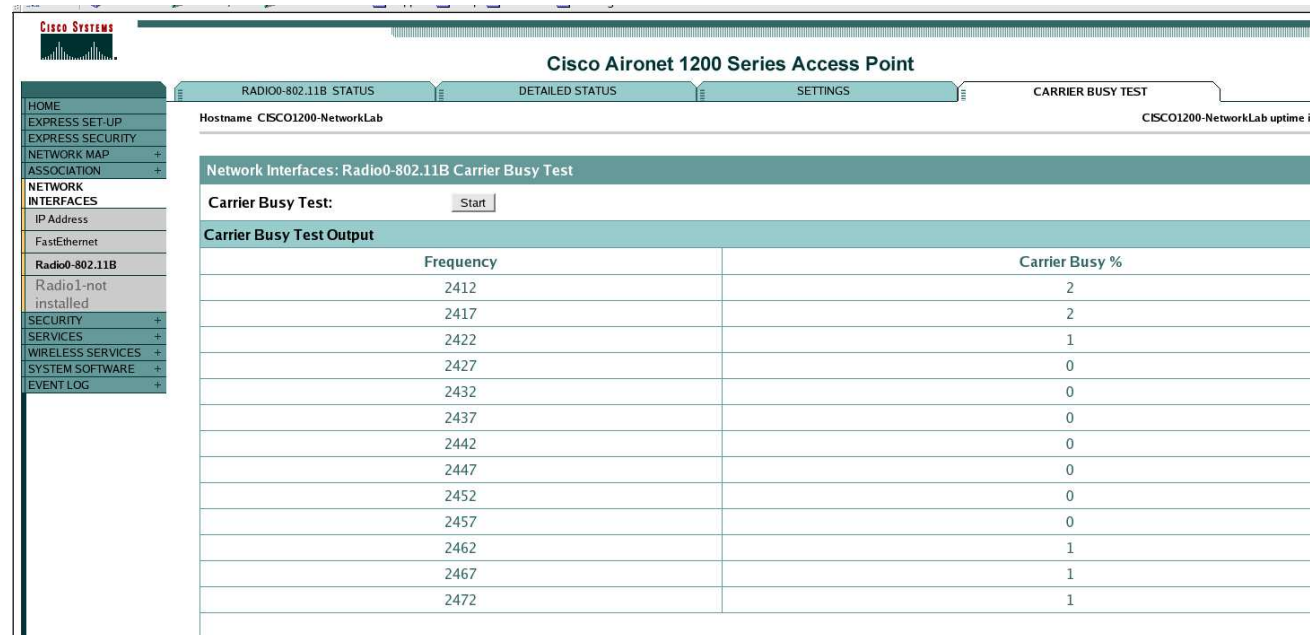
## □ Configuration of the basic parameters

<b>World Mode</b>	<input type="radio"/> Disable	<input type="radio"/> Legacy	<input checked="" type="radio"/> Dot11d
<b>Multi-Domain Operation:</b>			
<b>Country Code:</b>	Italy <input type="text"/>	<input checked="" type="checkbox"/> Indoor	<input checked="" type="checkbox"/> Outdoor
<b>Radio Preamble</b>	<input checked="" type="radio"/> Short	<input type="radio"/> Long	
<b>Receive Antenna:</b>	<input checked="" type="radio"/> Diversity	<input type="radio"/> Left (Secondary)	<input type="radio"/> Right (Primary)
<b>Transmit Antenna:</b>	<input checked="" type="radio"/> Diversity	<input type="radio"/> Left (Secondary)	<input type="radio"/> Right (Primary)
<b>External Antenna Configuration:</b>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
	<b>Antenna Gain(dB):</b> DISABLED (-128 - 128)		
<b>Aironet Extensions:</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
<b>Ethernet Encapsulation Transform:</b>	<input checked="" type="radio"/> RFC1042	<input type="radio"/> 802.1H	
<b>Reliable Multicast to WGB:</b>	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable	
<b>Public Secure Packet Forwarding:</b>	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
<b>Beacon Period:</b>	<input type="text" value="100"/> (20-4000 Kusec)	<b>Data Beacon Rate (DTIM):</b>	<input type="text" value="2"/> (1-100)
<b>Max. Data Retries:</b>	<input type="text" value="64"/> (1-128)	<b>RTS Max. Retries:</b>	<input type="text" value="64"/> (1-128)
<b>Fragmentation Threshold:</b>	<input type="text" value="2346"/> (256-2346)	<b>RTS Threshold:</b>	<input type="text" value="2312"/> (0-2347)
<b>Repeater Parent AP Timeout:</b>	<input type="text" value="0"/> (0-65535 sec)		
<b>Repeater Parent AP MAC 1 (optional):</b>	<input type="text"/> (HHHH.HHHH.HHHH)		
<b>Repeater Parent AP MAC 2 (optional):</b>	<input type="text"/> (HHHH.HHHH.HHHH)		
<b>Repeater Parent AP MAC 3 (optional):</b>	<input type="text"/> (HHHH.HHHH.HHHH)		
<b>Repeater Parent AP MAC 4 (optional):</b>	<input type="text"/> (HHHH.HHHH.HHHH)		

# AP 1200: Wireless Configuration

## □ Channel Selection:

- It is possible to make the AP choose the channel automatically
- It is possible to set it manually
- It is possible to do a survey to determine the state of the channels in the area



The screenshot displays the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The navigation menu on the left includes: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, FastEthernet, Radio0-802.11B, Radio1-not installed, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area shows the "RADIO0-802.11B STATUS" tab selected. Below the navigation menu, the "Carrier Busy Test" section is visible, with a "Start" button. The "Carrier Busy Test Output" table shows the following data:

Frequency	Carrier Busy %
2412	2
2417	2
2422	1
2427	0
2432	0
2437	0
2442	0
2447	0
2452	0
2457	0
2462	1
2467	1
2472	1



# AP 1200: Radius Server

---

## □ Basic Configuration:

- Authentication with client stations MAC address
- Server IP, ports for authentication and accounting
- Shared password between radius server and AP

# AP 1200: Server Radius

## Radius Server Configuration:

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point, specifically the 'Server Manager' section under 'GLOBAL PROPERTIES'. The page is titled 'Cisco Aironet 1200 Series Access Point' and shows the hostname 'CISCO1200-NetworkLab'. The 'Security: Server Manager' section is active, displaying the 'Backup RADIUS Server' configuration. The 'Current Server List' shows a single RADIUS server with the IP address 192.168.10.30. The 'Default Server Priorities' section is also visible, showing the configuration for EAP Authentication, MAC Authentication, Accounting, Admin Authentication (RADIUS), and Admin Authentication (TACACS+).

SERVER MANAGER GLOBAL PROPERTIES

Hostname CISCO1200-NetworkLab CISCO1200-NetworkLab uptime is 50 minutes

**Security: Server Manager**

**Backup RADIUS Server**

Backup RADIUS Server:  (Hostname or IP Address)

Shared Secret:

Apply Delete Cancel

**Corporate Servers**

**Current Server List**

RADIUS

< NEW >

192.168.10.30

Delete

Server:  (Hostname or IP Address)

Shared Secret:

Authentication Port (optional):  (0-65536)

Accounting Port (optional):  (0-65536)

Apply Cancel

**Default Server Priorities**

**EAP Authentication**

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

**MAC Authentication**

Priority 1: 192.168.10.30

Priority 2: < NONE >

Priority 3: < NONE >

**Accounting**

Priority 1: 192.168.10.30

Priority 2: < NONE >

Priority 3: < NONE >

**Admin Authentication (RADIUS)**

Priority 1: < NONE >

Priority 2: < NONE >

**Admin Authentication (TACACS+)**

Priority 1: < NONE >

Priority 2: < NONE >

# AP 1200: SSID and Authentication

---

## □ SSID:

- You have to define an SSID. Default "tsunami"
- Guest SSID: is the SSID advertised

## □ Authentications:

- Open: all the devices are allowed to authenticate with the AP
- Shared: there is an exchange of a message plain or encrypted. Unsafe
- EAP: the safest mode

## □ Authentication based on MAC:

- Open authentication → "With MAC Authentication"

# AP 1200: SSID and Authentication

## □ SSID and Radius Server:

- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY
  - Admin Access
  - Encryption Manager
  - SSID Manager**
  - Server Manager
  - Local RADIUS Server
  - Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

### Security: SSID Manager

#### SSID Properties

**Current SSID List**

< NEW >
WILMA-LAB

Delete

**SSID:** WILMA-LAB

**VLAN:** < NONE > [Define VLANs](#)

**Network ID:** (0-4096)

---

#### Authentication Settings

**Authentication Methods Accepted:**

<input checked="" type="checkbox"/> Open Authentication:	with MAC Authentication
<input type="checkbox"/> Shared Authentication:	< NO ADDITION >
<input type="checkbox"/> Network EAP:	< NO ADDITION >

**Server Priorities:**

EAP Authentication Servers	MAC Authentication Servers
<input checked="" type="radio"/> Use Defaults <a href="#">Define Defaults</a>	<input checked="" type="radio"/> Use Defaults <a href="#">Define Defaults</a>
<input type="radio"/> Customize	<input type="radio"/> Customize
Priority 1: < NONE >	Priority 1: < NONE >
Priority 2: < NONE >	Priority 2: < NONE >
Priority 3: < NONE >	Priority 3: < NONE >

# AP 1200: SSID and Authentication

## □ MAC Address Authentication:

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point" and the hostname is "CISCO1200-NetworkLab". The page is divided into several sections:

- Navigation Menu:** Includes HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (Admin Access, Encryption Manager, SSID Manager, Server Manager, Local RADIUS Server, Advanced Security), SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.
- MAC ADDRESS AUTHENTICATION:** The active section, showing "Security: Advanced Security- MAC Address Authentication".
- MAC Addresses Authenticated by:** Three radio button options: "Local List Only", "Authentication Server Only", and "Authentication Server if not found in Local List" (which is selected).
- Local MAC Address List:** A section with a "Local List:" label, a list box (currently empty), and a "Delete" button.
- New MAC Address:** A text input field with a placeholder "(HHHH.HHHH.HHHH)".

At the bottom left, there is a "Close Window" button.

# AP 1200: SSID and Authentication

## MAC Address Authentication:

The screenshot displays the Cisco Aironet 1200 Series Access Point configuration interface. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CISCO1200-NetworkLab" and the uptime is "3 hours, 25 minutes".

The "Event Log" section shows a table of events:

Index	Time	Severity	Description
1	Mar 1 03:25:19.858	Information	Interface Dot11Radio0, Station WILMA-LAPTOP2 0002.8a9f.1ead Reassociated KEY_MGMT[NONE]
2	Mar 1 03:25:14.174	Debugging	Station 0002.8a9f.1ead Authentication failed
3	Mar 1 03:25:07.831	Debugging	Station 0002.8a9f.1ead Authentication failed
4	Mar 1 03:25:01.448	Debugging	Station 0002.8a9f.1ead Authentication failed
5	Mar 1 03:24:55.125	Debugging	Station 0002.8a9f.1ead Authentication failed
6	Mar 1 03:24:49.843	Debugging	Station 0002.8a9f.1ead Authentication failed
7	Mar 1 03:24:43.529	Debugging	Station 0002.8a9f.1ead Authentication failed
8	Mar 1 03:24:37.186	Debugging	Station 0002.8a9f.1ead Authentication failed
9	Mar 1 03:24:30.863	Debugging	Station 0002.8a9f.1ead Authentication failed
10	Mar 1 03:24:24.480	Debugging	Station 0002.8a9f.1ead Authentication failed
11	Mar 1 03:24:18.097	Debugging	Station 0002.8a9f.1ead Authentication failed
12	Mar 1 03:24:12.805	Debugging	Station 0002.8a9f.1ead Authentication failed
13	Mar 1 03:24:06.501	Debugging	Station 0002.8a9f.1ead Authentication failed
14	Mar 1 03:24:00.178	Debugging	Station 0002.8a9f.1ead Authentication failed
15	Mar 1 03:23:54.836	Debugging	Station 0002.8a9f.1ead Authentication failed
16	Mar 1 03:23:48.493	Debugging	Station 0002.8a9f.1ead Authentication failed
17	Mar 1 03:23:42.130	Debugging	Station 0002.8a9f.1ead Authentication failed

The terminal window shows the following output:

```
root@radiuswn:~# /etc/rc.d/init.d/radiusd restart
Stopping RADIUS server: [ OK ]
Starting RADIUS server: [ OK ]
root@radiuswn root# tail -f /var/log/radius/radius.log
Tue Jan 25 14:01:28 2005 : Auth: Login incorrect: [00028a9f1ead/00028a9f1ead] (f
rom client APCisco1 port 325 cli 0002.8a9f.1ead)
Tue Jan 25 14:01:30 2005 : Auth: Login incorrect: [00028a9f1ead/00028a9f1ead] (f
rom client APCisco1 port 326 cli 0002.8a9f.1ead)
Tue Jan 25 14:01:35 2005 : Auth: Login incorrect: [00028a9f1ead/00028a9f1ead] (f
rom client APCisco1 port 327 cli 0002.8a9f.1ead)
Tue Jan 25 14:01:37 2005 : Auth: Login incorrect: [00028a9f1ead/00028a9f1ead] (f
rom client APCisco1 port 328 cli 0002.8a9f.1ead)
Tue Jan 25 14:01:41 2005 : Info: Using deprecated naslist file. Support for thi
s will go away soon.
Tue Jan 25 14:01:41 2005 : Info: Using deprecated clients file. Support for thi
s will go away soon.
Tue Jan 25 14:01:41 2005 : Info: Using deprecated realms file. Support for thi
s will go away soon.
Tue Jan 25 14:01:41 2005 : Info: Listening on IP address *, ports 1812/udp and 1
813/udp, with proxy on 1814/udp.
Tue Jan 25 14:01:41 2005 : Info: Ready to process requests.
Tue Jan 25 14:01:42 2005 : Auth: Login OK: [00028a9f1ead] (from client APCisco1
port 328 cli 0002.8a9f.1ead)
```

# AP 1200: Multi SSID and VLAN

---

- To use more than one SSID:
  - More than one SSID can be declared
  - At most one is announced
  - It is possible to associate each SSID to a different VLAN
  - For each SSID we can define different policy of authentication, accounting, and encryption
  - We can configure a radius server so that it will be the radius to assign the VLAN to the mobile client

# AP 1200: SSID and Authentication

## □ SSID definition

The screenshot displays the configuration page for an AP 1200, specifically the SSID and authentication settings. The left sidebar shows a navigation menu with categories like SECURITY, SERVICES, WIRELESS SERVICES, and SYSTEM SOFTWARE. The main content area is divided into several sections:

- Current SSID List:** A list box containing '< NEW >', 'CREATE-NET-TEST', 'WILMA-LAB', and 'WILMA-LAB-TEST'. A 'Delete' button is located below the list.
- SSID, VLAN, and Network ID:** Fields for 'SSID:' (CREATE-NET-TEST), 'VLAN:' (4), and 'Network ID:' (4 (0-4096)). A 'Define VLANs' link is next to the VLAN field.
- Authentication Settings:**
  - Authentication Methods Accepted:** Includes checkboxes for 'Open Authentication' (checked), 'Shared Authentication', and 'Network EAP'. Each has a dropdown menu.
  - Server Priorities:** Divided into 'EAP Authentication Servers' and 'MAC Authentication Servers'. Each has a radio button for 'Use Defaults' (selected) and 'Customize', followed by three priority dropdown menus.
- Authenticated Key Management:** Includes 'Key Management' (dropdown), and checkboxes for 'CCKM' and 'WPA'. Below is a 'WPA Pre-shared Key' field and radio buttons for 'ASCII' (selected) and 'Hexadecimal'.
- Accounting Settings:** Includes a checked 'Enable Accounting' checkbox and an 'Accounting Server Priorities' section.



# AP 1200: SSID and Authentication

## □ Definition of Cryptography

The screenshot shows the configuration page for the Cisco Aironet 1200 Series Access Point, specifically the Security: Encryption Manager section. The page is titled "Cisco Aironet 1200 Series Access Point" and shows the hostname "CISCO1200-NetworkLab" and uptime "2 days, 49 minutes".

The left sidebar contains a navigation menu with the following items:

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY
  - Admin Access
  - Encryption Manager**
  - SSID Manager
  - Server Manager
  - Local RADIUS Server
  - Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

The main configuration area is titled "Security: Encryption Manager" and includes the following sections:

- Set Encryption Mode and Keys for VLAN:** A dropdown menu is set to "3". A link "Define VLANs" is visible.
- Encryption Modes:**
  - None
  - WEP Encryption** (Mandatory) Cisco Compliant TKIP Features:  Enable Message Integrity Check (MIC)  Enable Per Packet Keying (PPK)
  - Cipher (WEP 128 bit)
- Encryption Keys:**

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input checked="" type="radio"/>	<input type="text" value="*****"/>	128 bit
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit
- Global Properties:**
  - Broadcast Key Rotation Interval:**  Disable Rotation  Enable Rotation with Interval:  (10-10000000 sec)
  - WPA Group Key Update:**  Enable Group Key Update On Membership Termination  Enable Group Key Update On Member's Capability Change

# AP 1200: SSID and Authentication

- Example of an SSID/VLAN configuration:

The screenshot displays the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CISCO1200-NetworkLab" and the uptime is "2 days, 51 minute".

The left sidebar contains a navigation menu with the following items:

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY
  - Admin Access
  - Encryption Manager
  - SSID Manager
  - Server Manager
  - Local RADIUS Server
  - Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG

The main content area shows the "Security Summary" section, which includes the following tables:

**Administrators**

Username	Read-Only	Read-Write
Cisco	✓	

**Radio0-802.11B SSIDs**

SSID	VLAN	Open	Shared	Network EAP
CREATE-NET-TEST	4	with MAC		
WILMA-LAB	3	with MAC		
WILMA-LAB-TEST	5	with MAC		

**Encryption Settings**

VLAN	Encryption Mode	WEP		Cipher					Key Rotation
		MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	
3	WEP-Mandatory								
4	None								
5	None								

**Server-Based Security**

Server Name/IP Address	Type	EAP	MAC	Proxy Mobile IP	Admin	Accounting
192.168.10.30	RADIUS		✓			✓

# AP 1200: SSID and Authentication

- Examples of client stations assigned to different VLAN based on SSID

The screenshot shows the configuration page for a Cisco Aironet 1200 Series Access Point. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "CISCO1200-NetworkLab" and the uptime is "2 days, 1 hour, 8 minutes".

**Association**

Clients: 3      Repeaters: 0

View:  Client  Repeater Apply

**Radio0-802.11B**

**SSID CREATE-NET-TEST :**

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	-	172.31.213.250	<a href="#">0090.4b64.9150</a>	MAC-Associated	self	4

**SSID WILMA-LAB :**

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	-	172.31.194.251	<a href="#">000b.cd8d.303b</a>	MAC-Associated	self	3

**SSID WILMA-LAB-TEST :**

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	-	172.31.193.254	<a href="#">0009.5b54.78ea</a>	MAC-Associated	self	5

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

# AP 1200: SSID and Authentication

## Client statistics

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page. The page title is "Cisco Aironet 1200 Series Access Point". The main content area is titled "STATISTICS" and shows the following information:

Hostname: CISCO1200-NetworkLab  
CISCO1200-NetworkLab uptime is 2 days, 1 hour, 8 minutes

Association: Station View- Client

Station Information and Status			
MAC Address	000b.cd&d.303b	Name	NONE
IP Address	172.31.194.251	Class	unknown
Device	unknown	Software Version	NONE
CCX Version	NONE		
State	MAC-Associated	Parent	self
SSID	WILMA-LAB	VLAN	3
Hops To Infrastructure	1	Communication Over Interface	Radio0-802.11B
Clients Associated	0	Repeaters Associated	0
Key Mgmt type	NONE	Encryption	WEP
Current Rate (Mb/sec)	11.0	Capability	
Supported Rates(Mb/sec)	1.0, 2.0, 5.5, 11.0	Association Id	87
Signal Strength (dBm)	-40	Connected For (sec)	580
Signal Quality (%)	77	Activity TimeOut (sec)	44
Power-save	Off	Last Activity (sec)	16
Receive/Transmit Statistics			
Total Packets Input	79	Total Packets Output	29
Total Bytes Input	11046	Total Bytes Output	2386
Duplicates Received	0	Maximum Data Retries	0
Decrypt Errors	0	Maximum RTS Retries	0
MIC Failed	0		
MIC Missing	0		

Buttons: Deauthenticate, Clear, Refresh

# AP 1200: Configuration via CLI

---

- All the configurations via HTTP are possible via CLI

- show running-config

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption vlan 3 key 1 size 128bit 7 501B2057424875554B78965D207B
  transmit-key
  encryption vlan 3 mode wep mandatory
  !
  ssid CREATE-NET-TEST
    vlan 4
    authentication open mac-address mac_methods
    accounting acct_methods
    mobility network-id 4
    information-element ssid advertisement
  !
  ssid WILMA-LAB
    vlan 3
    authentication open mac-address mac_methods
    accounting acct_methods
    mobility network-id 3
    information-element ssid advertisement
  !
  ssid WILMA-LAB-TEST
    vlan 5
    authentication open mac-address mac_methods
    accounting acct_methods
    guest-mode
    mobility network-id 5
```

# AP 1200: Multi SSID and VLAN

---

- Other relevant configuration:
  - Syslog
  - SNMP
  - QoS