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!

Regions	Frequencies
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:

Regions	Channels (5MHz)
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

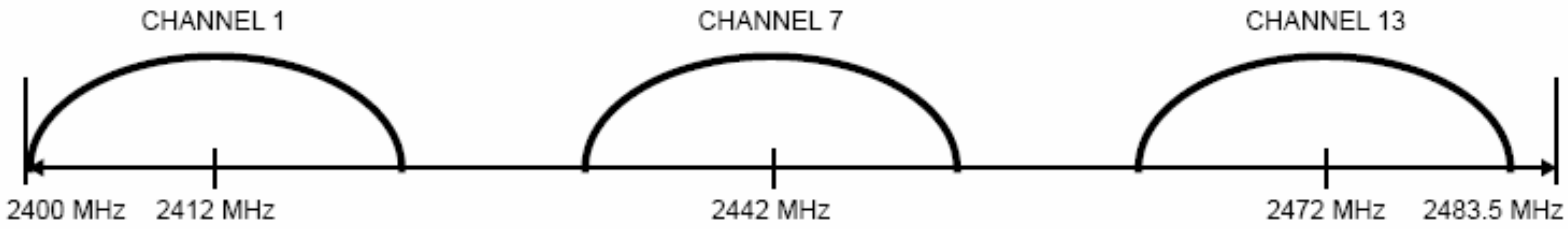


Figure 143—European channel selection—non-overlapping

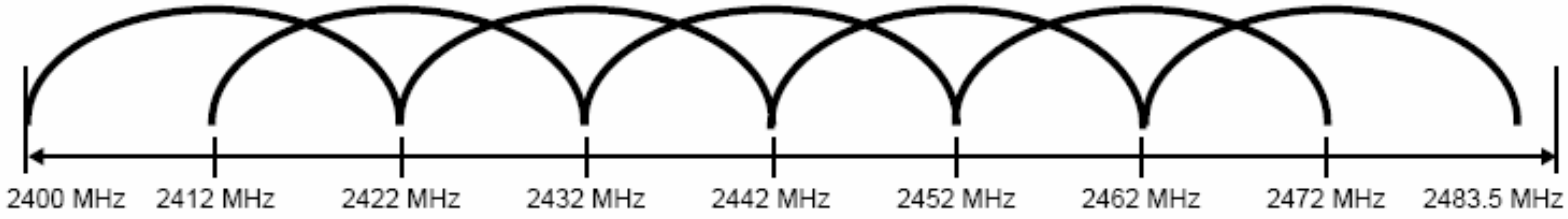


Figure 144—European channel selection—overlapping

IEEE 802.11b in brief : Power

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

Maximum Power Perimitted	Region
1000 mW	USA
100 mW	Europe
10 mW	Japan

IEEE 802.11b in brief : Speed

- The transmission speeds supported by the standard are:

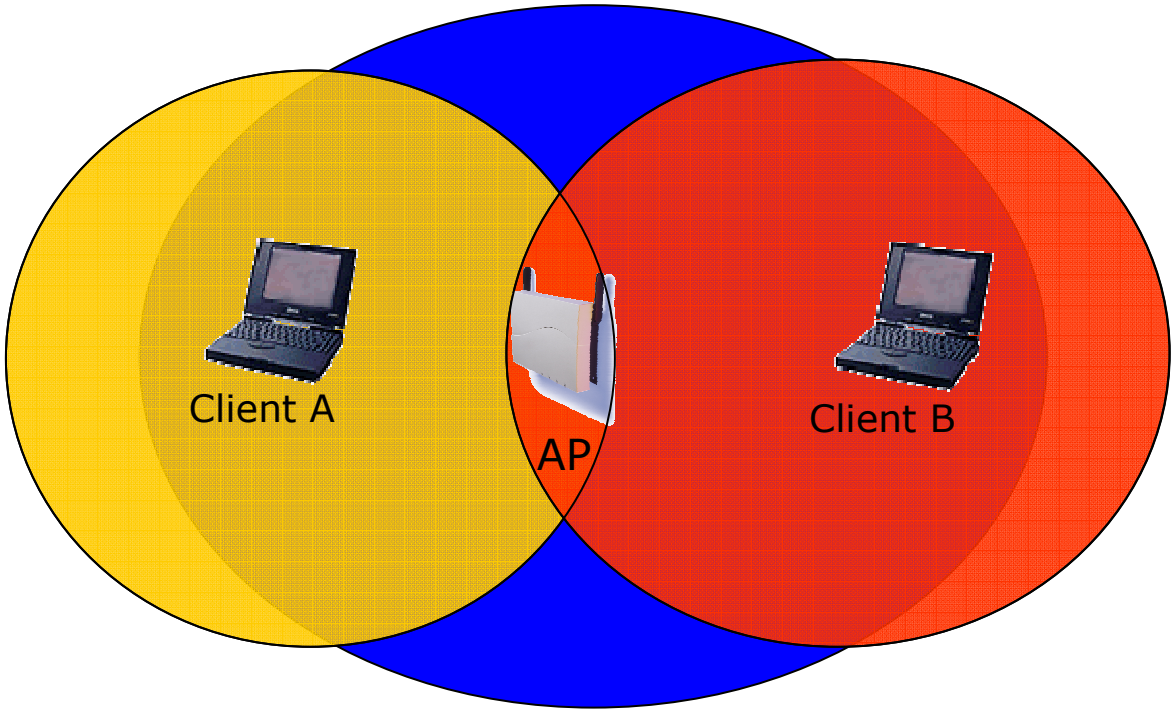
  1, 2, 5.5, 11 Mbps

- 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:

Type of area	**11 Mbs**	**5,5 Mbs**	**2 Mbs**	**1 Mbs**
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:

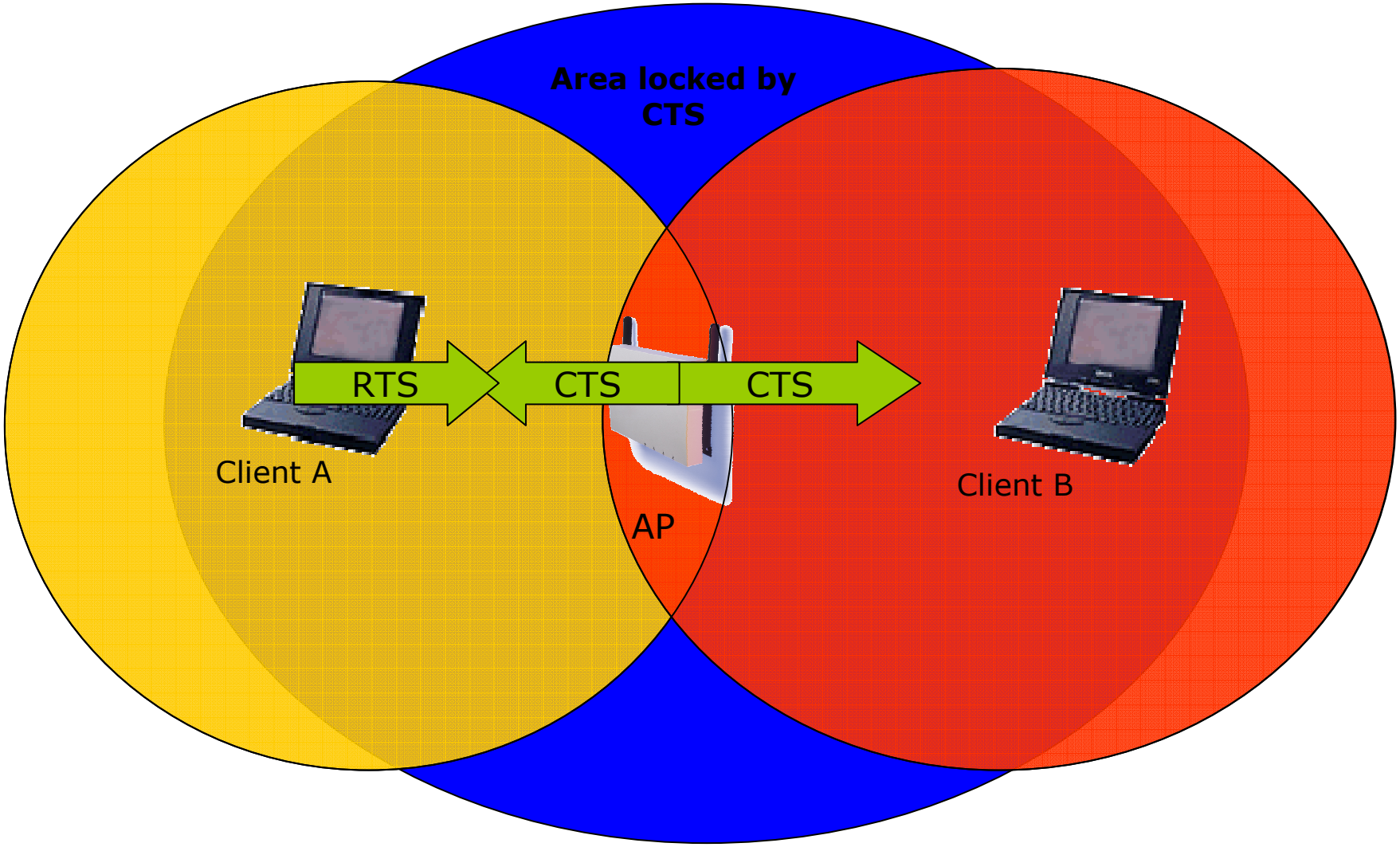


- A talk with AP (but not with B)
- B talk with AP (but not with A)

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

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

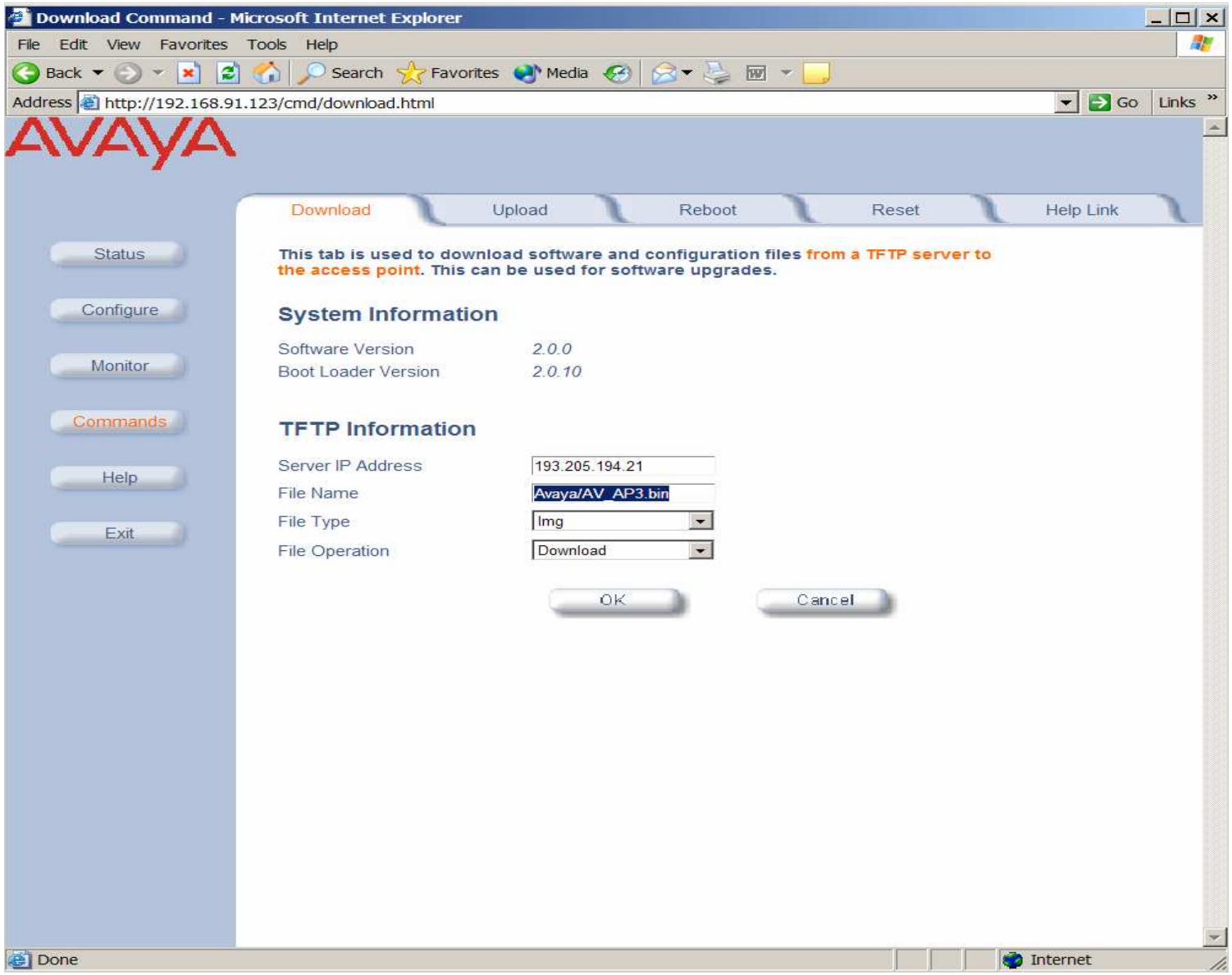
- To update the firmware a tftp server (Transfer Protocol file Trivial) can be used
- Using the CLI:

```
[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



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

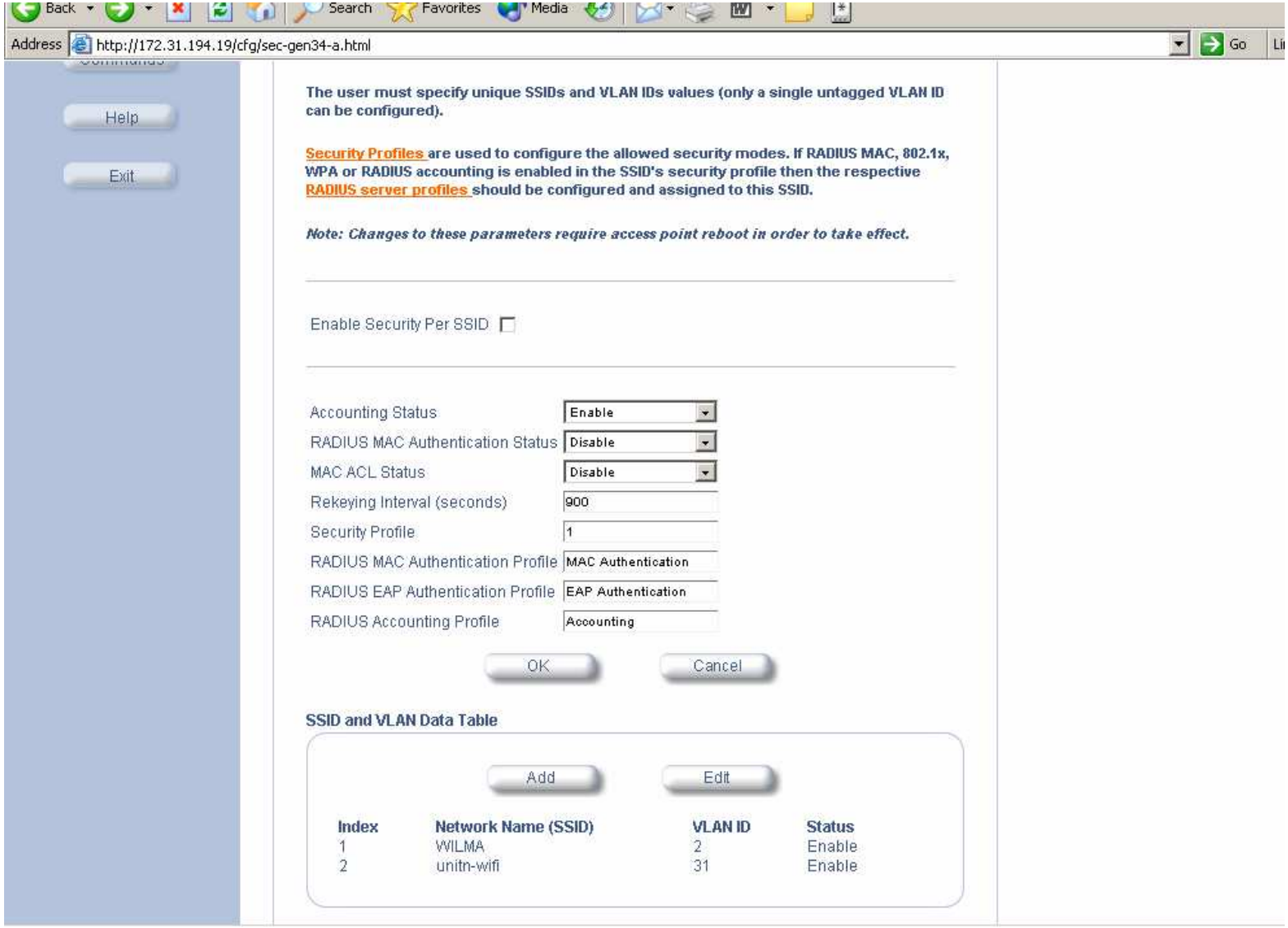
Avaya AP: Wireless Interfaces

- 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



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

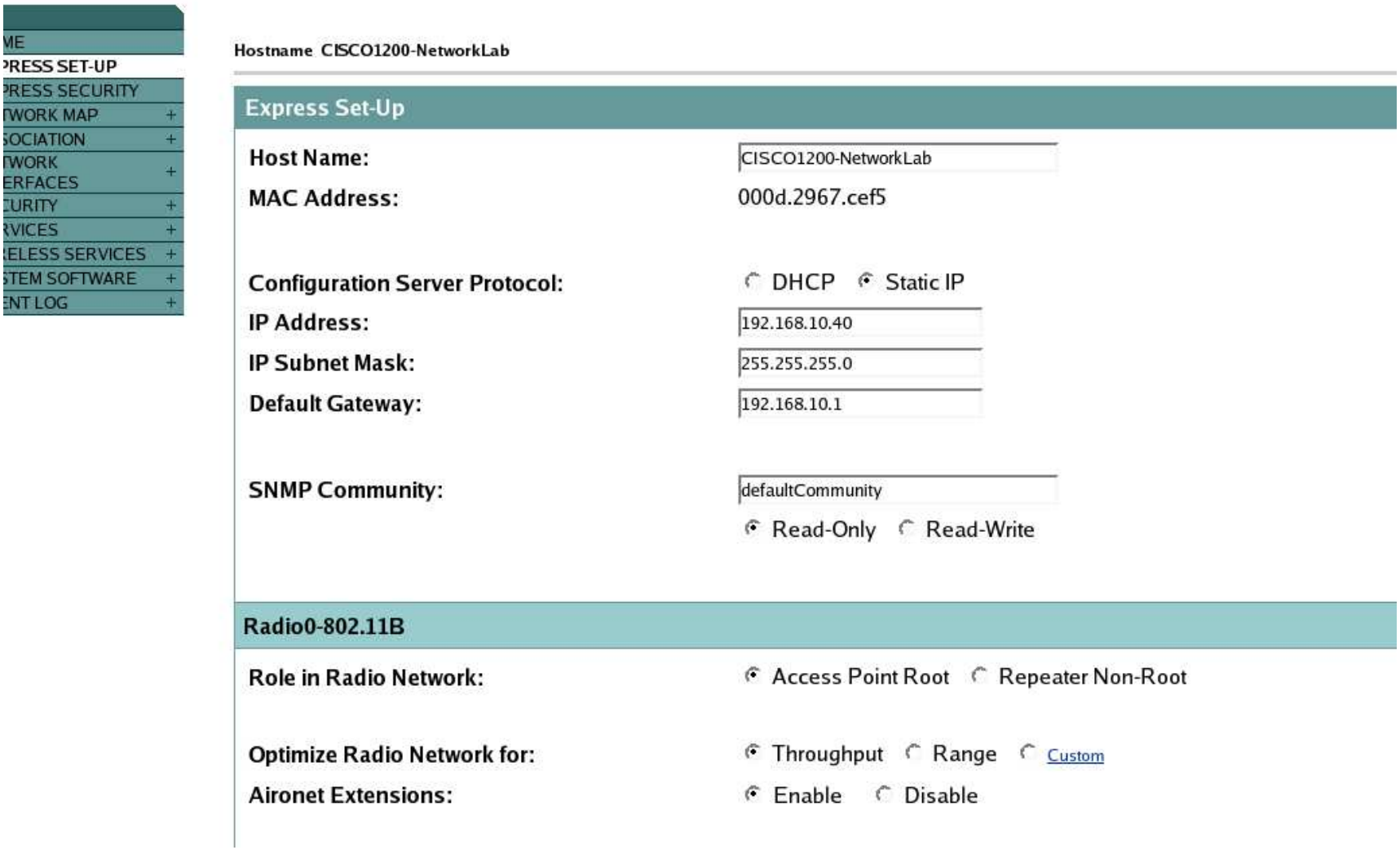
- "Standard" CISCO commands:
  - `enable`
  - *`Password`* → `Cisco`
  - `configure` *`[terminal]`*
  - `ip default-gateway 192.168.10.1`
  - `interface FastEthernet 0`
  - `ip address 192.168.10.40 255.255.255.0`
  - `exit`
  - `Ctrl-z`
  - `copy running-config startup-config`
  - `reload`

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:

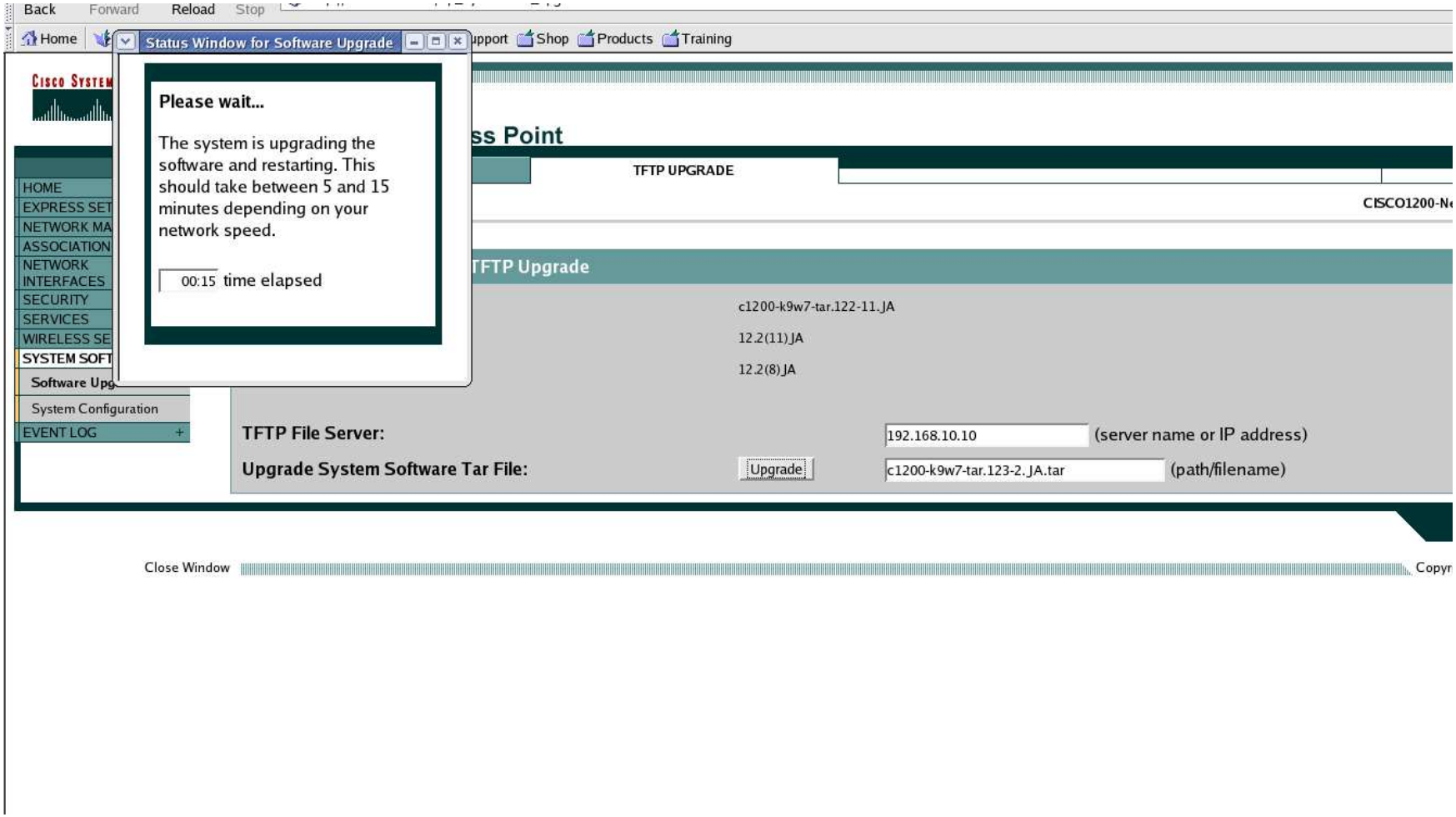


AP 1200: Firmware Update

- 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

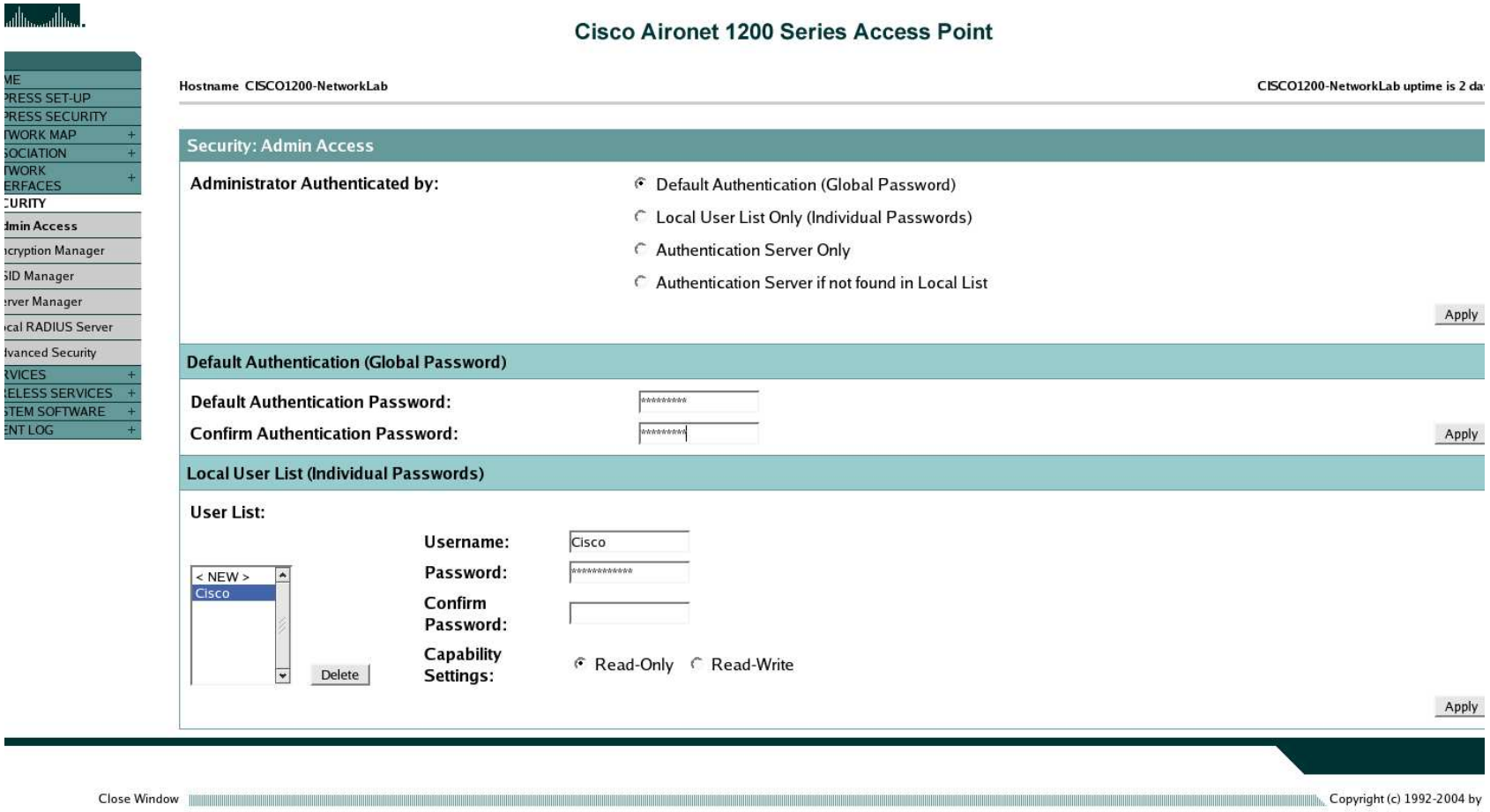
AP 1200: Firmware Update

- Firmware Update via HTTP



AP 1200: Password Administrator

- We can define more than a user with different capabilities

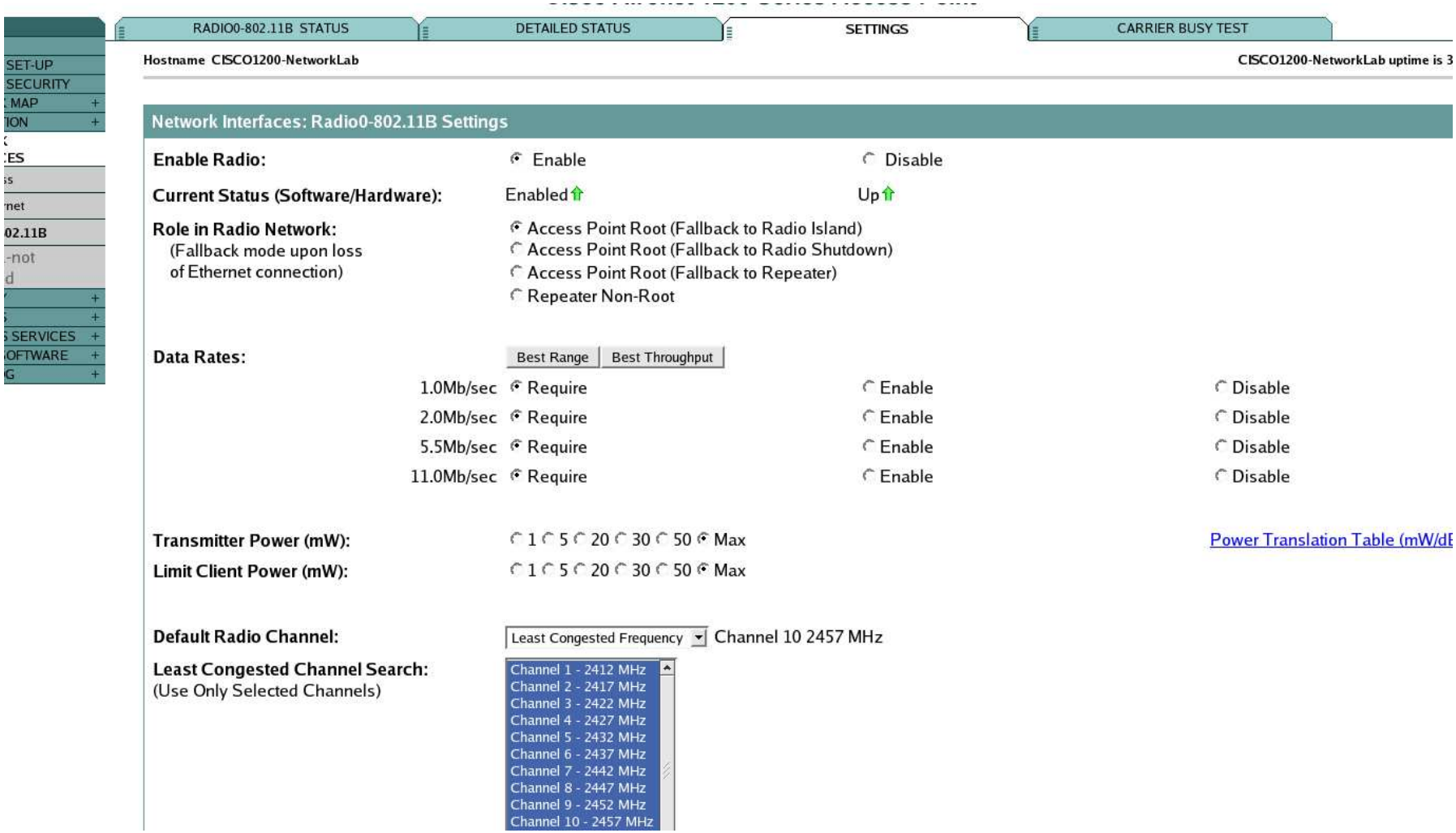


AP 1200: Wireless Configuration

- 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



AP 1200: Wireless Configuration

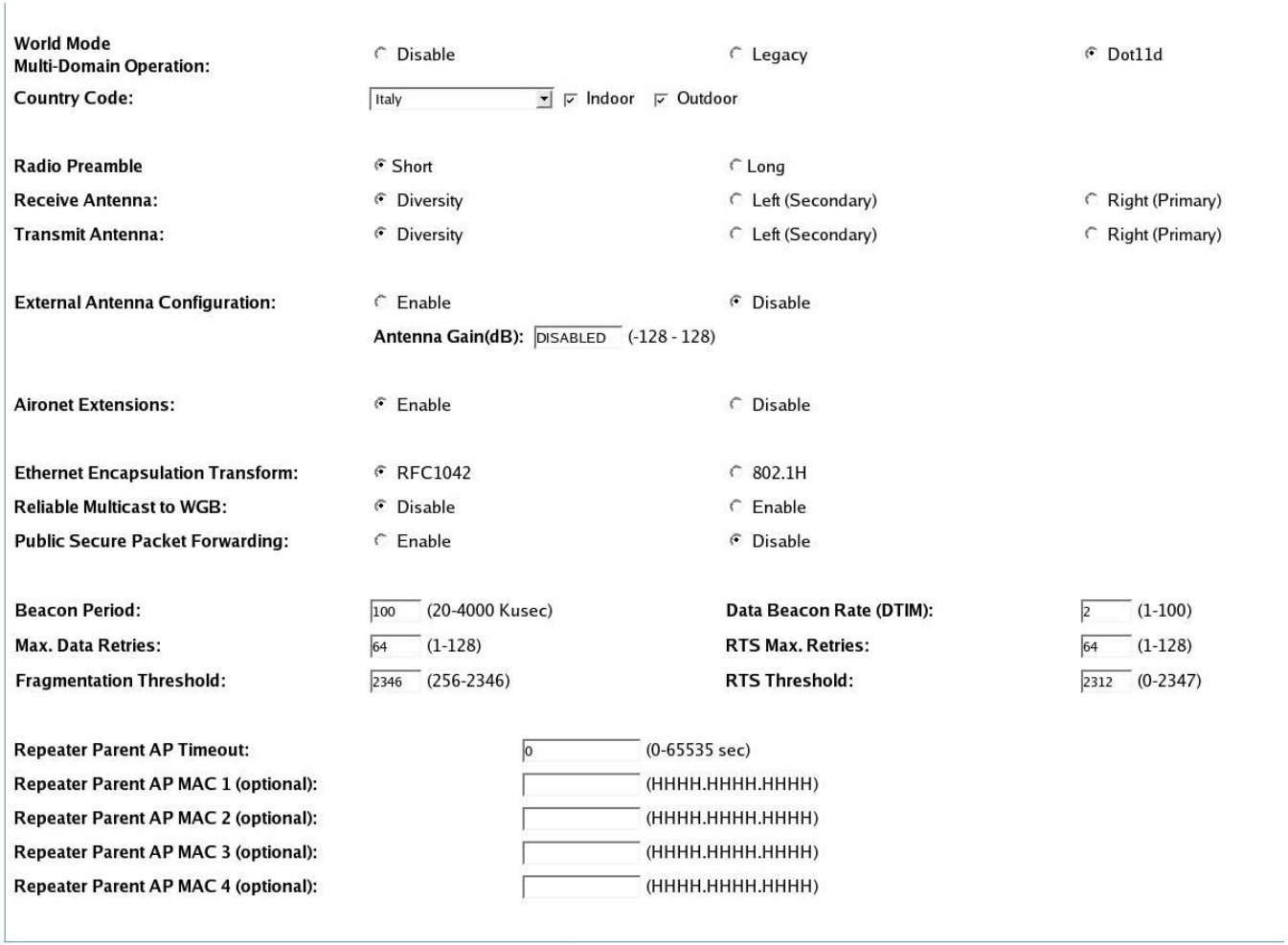
- World Mode:
  - Clients can receive “national” information about setting. Legacy for CISCO compatibility, 802.11d new standards
- Antenna:
  - Diversity: both antennas are used and the one that receives the best signal is chosen
- Encapsulation:
  - To manage the non 802.3 packages, these have to be 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

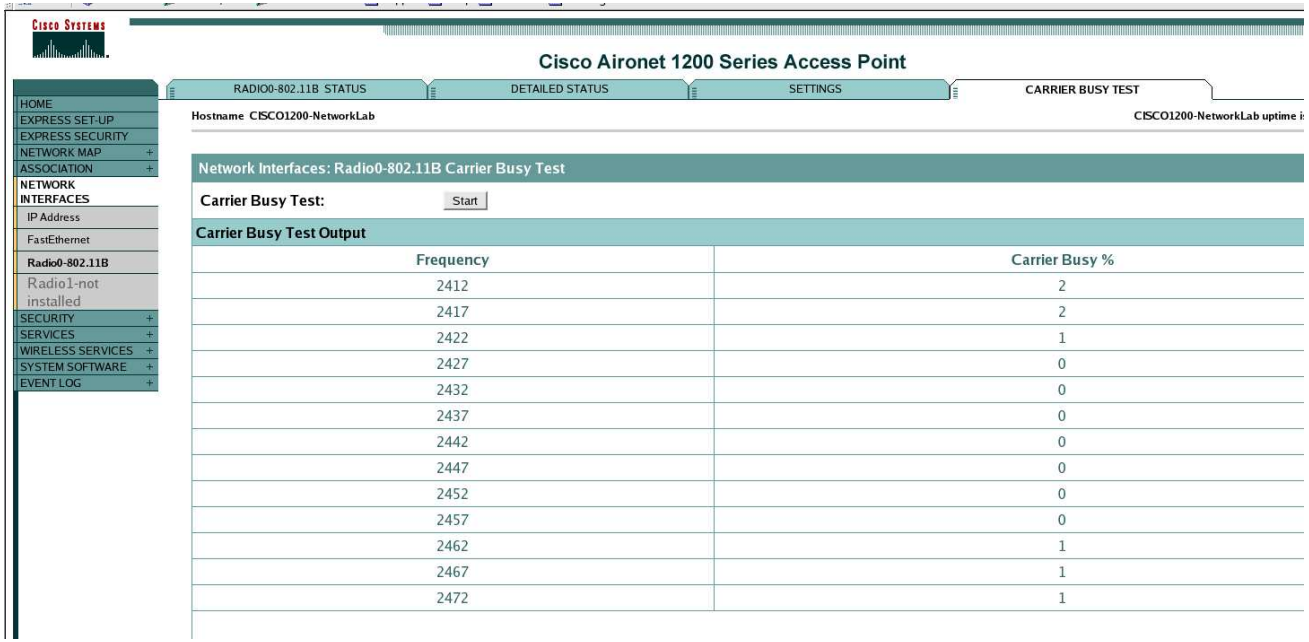
AP 1200: Wireless Configuration

- Configuration of the basic parameters



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



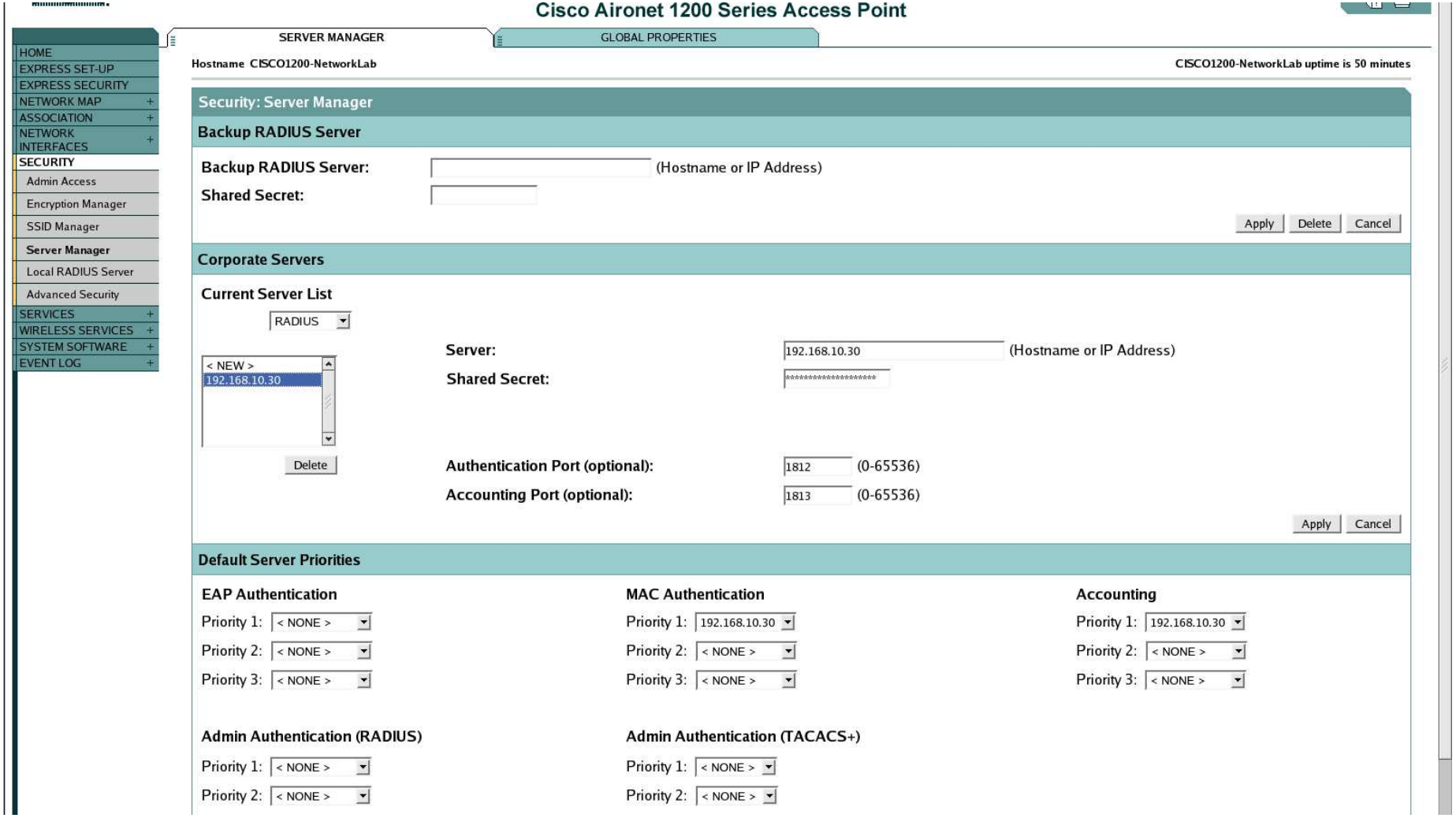
Frequency	Carrier Busy %
2412	2
2417	2
2422	1
2427	0
2432	0
2437	0
2442	0
2447	0
2452	0
2457	0
2462	1
2467	1
2472	1

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:

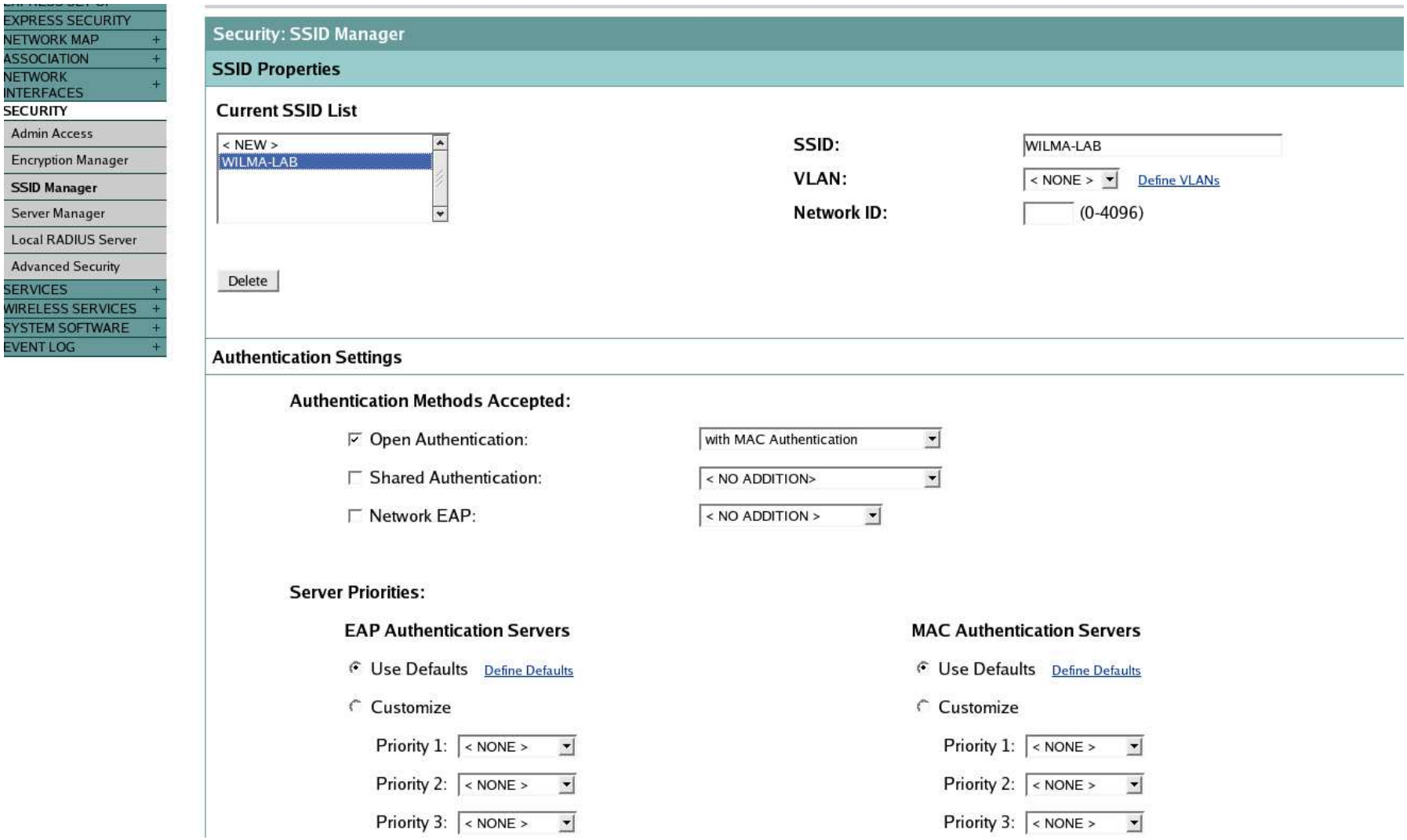


AP 1200: SSID and Authentication

- 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”

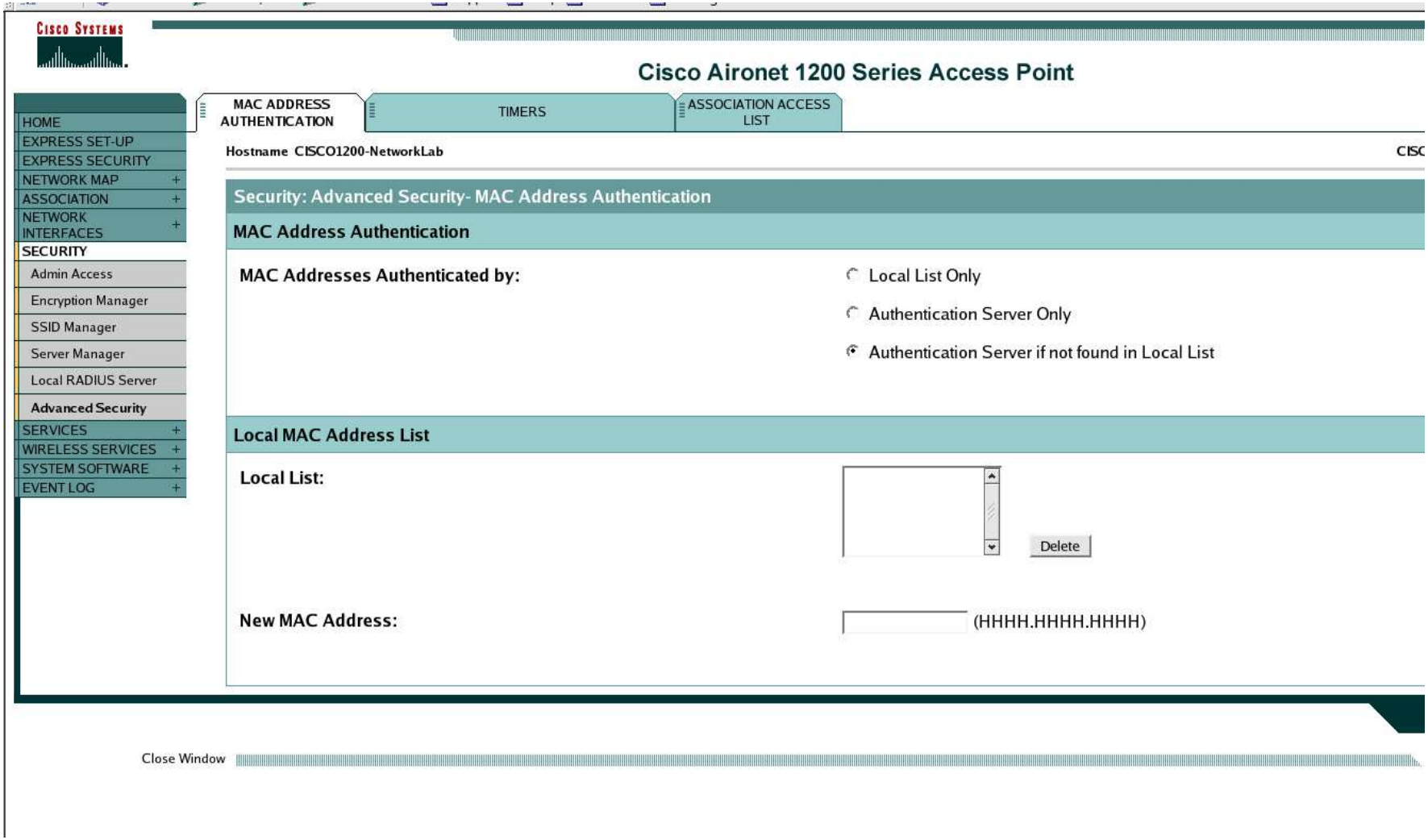
AP 1200: SSID and Authentication

- SSID and Radius Server:



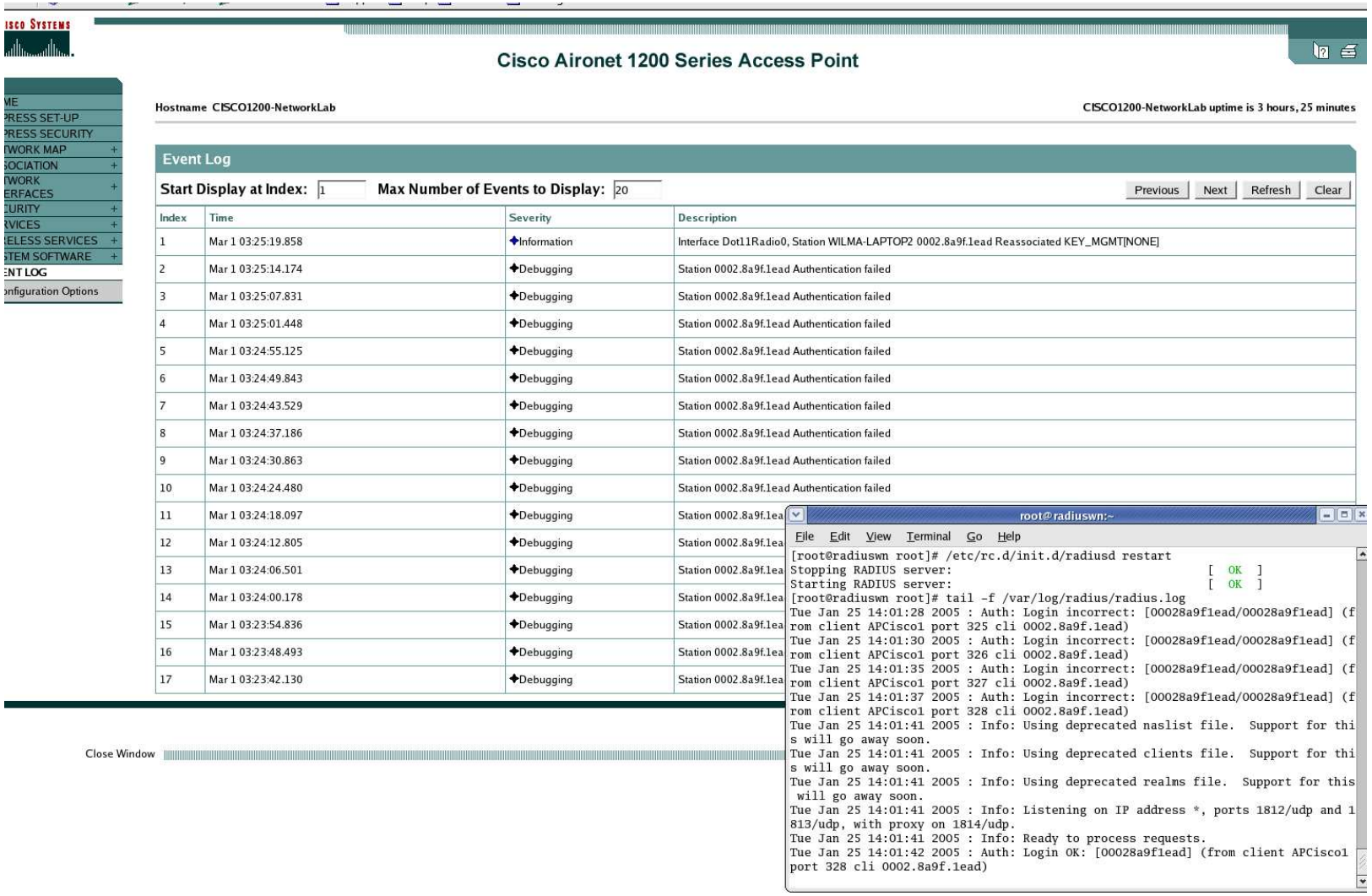
AP 1200: SSID and Authentication

- MAC Address Authentication:



AP 1200: SSID and Authentication

- MAC Address Authentication:

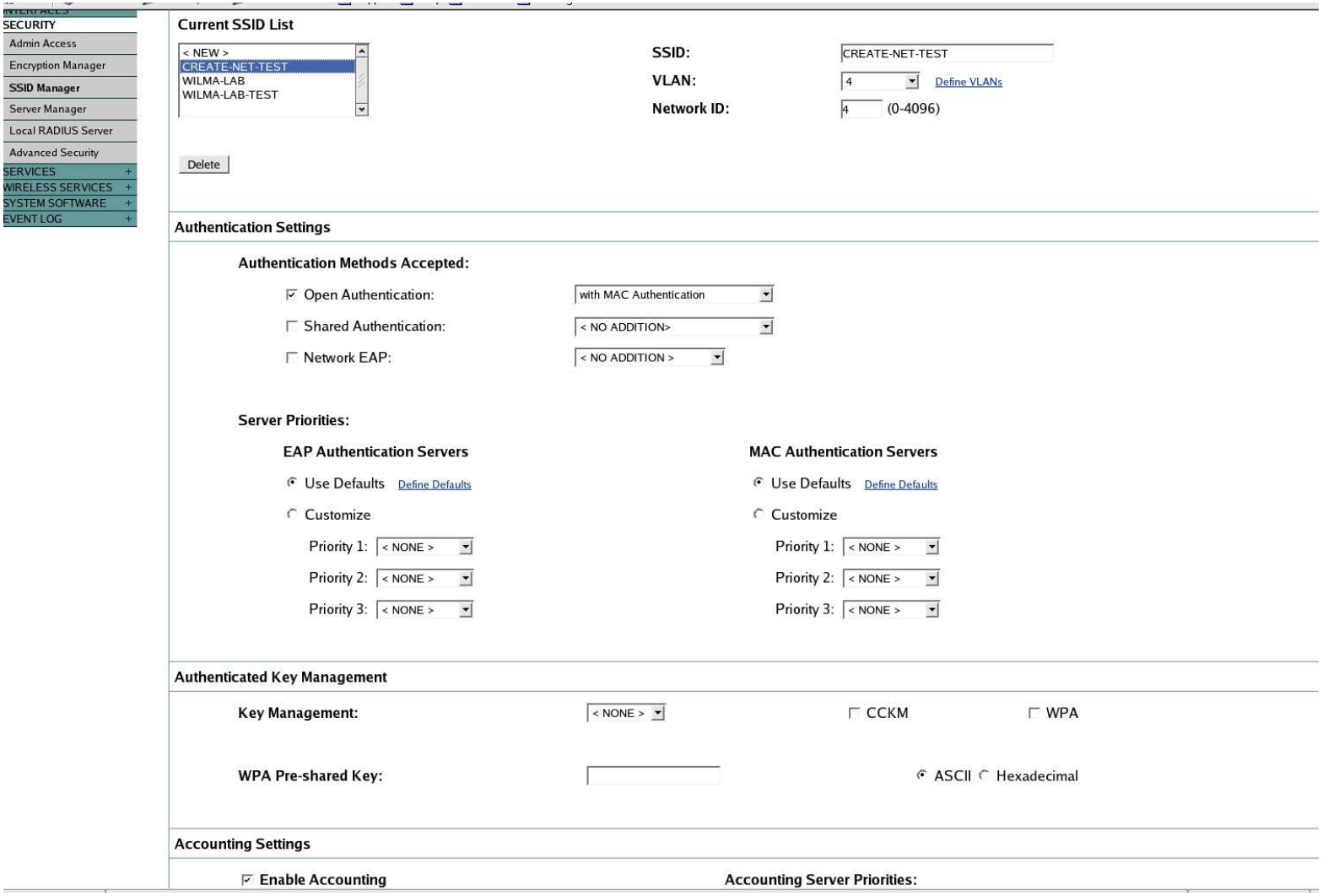


AP 1200: Multi SSID and VLAN

- 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

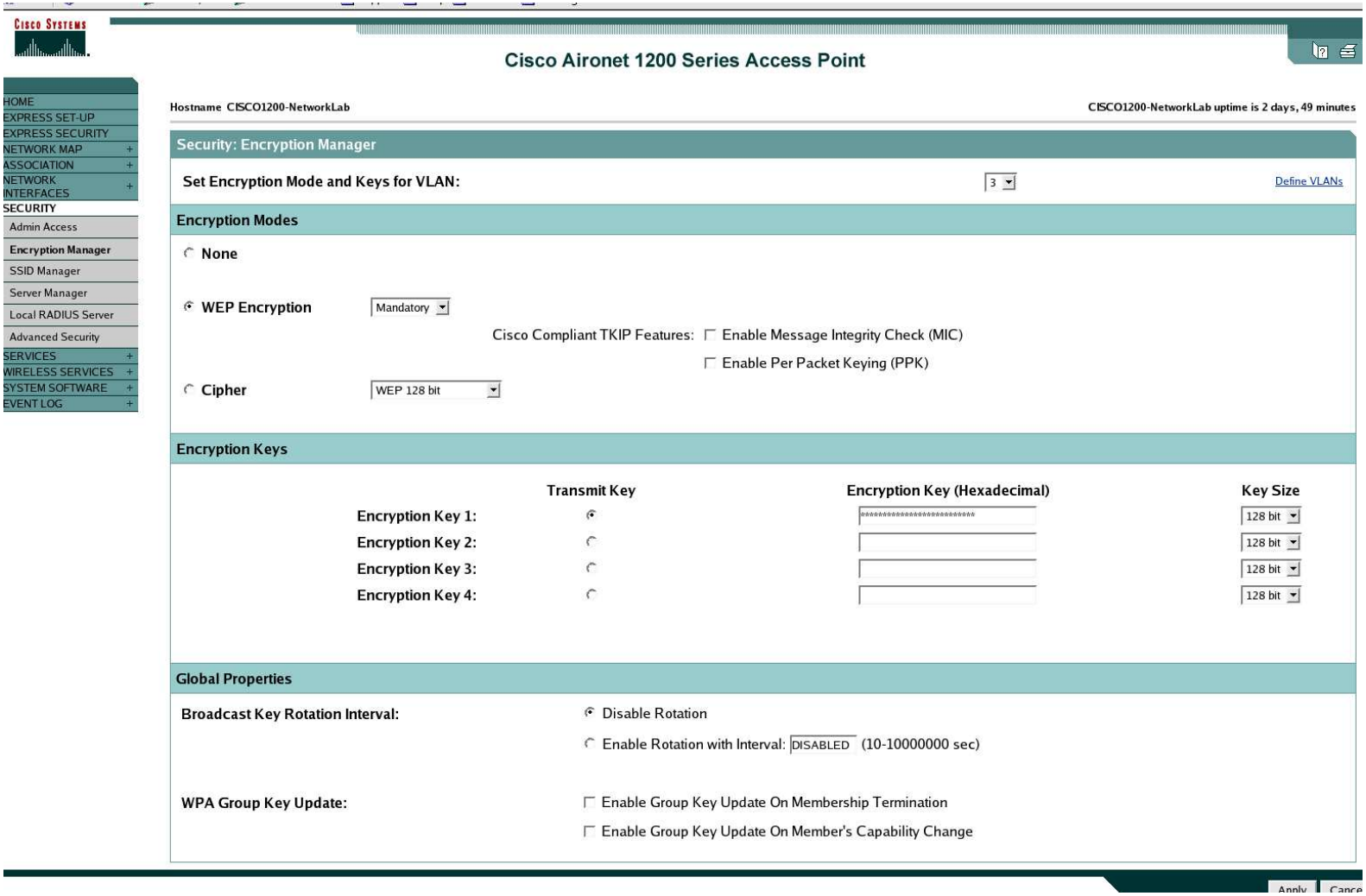
AP 1200: SSID and Authentication

- SSID definition



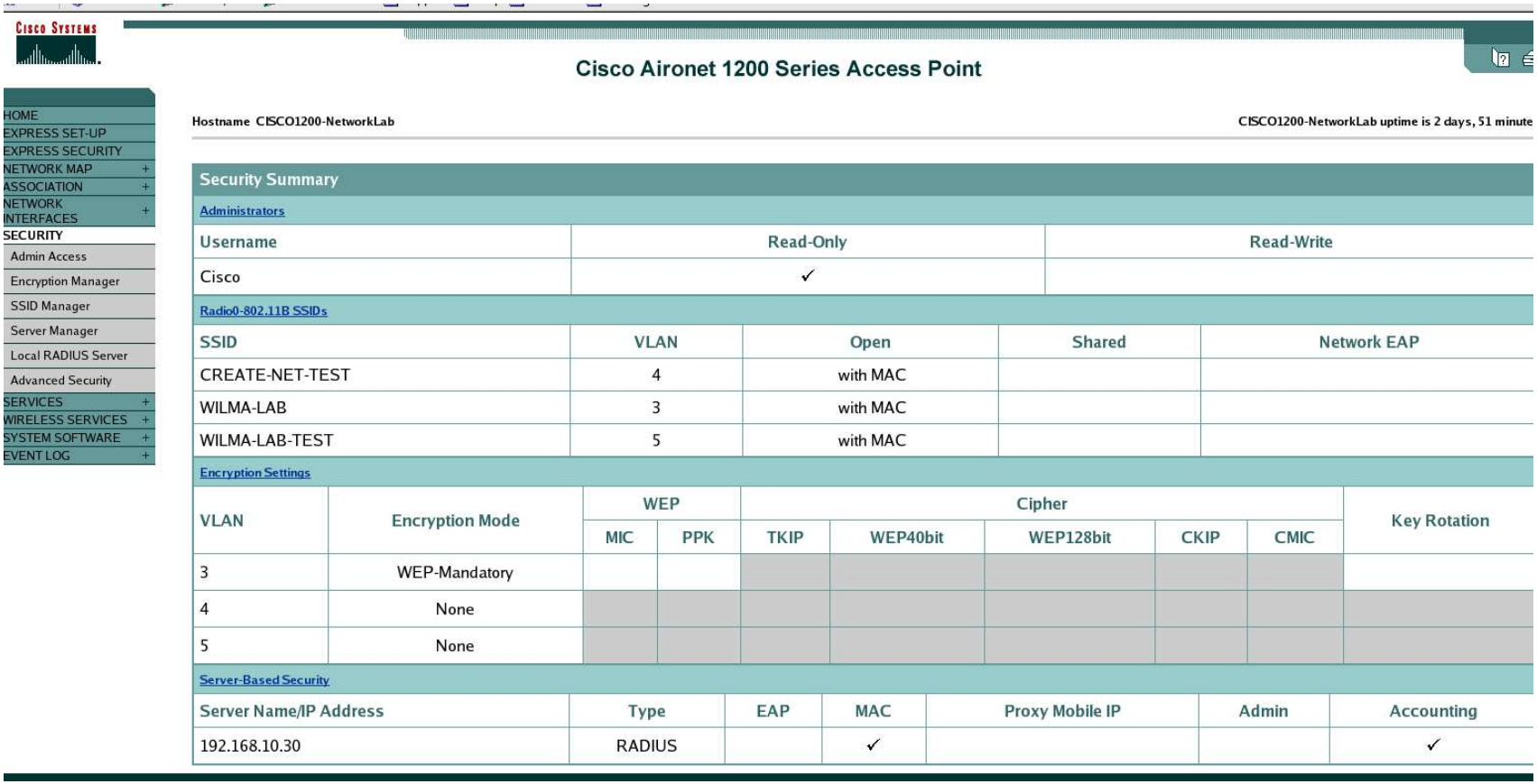
AP 1200: SSID and Authentication

- Definition of Cryptography



AP 1200: SSID and Authentication

- Example of an SSID/VLAN configuration:



Cisco Systems

Cisco Aironet 1200 Series Access Point

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 +

Hostname CISCO1200-NetworkLab

CISCO1200-NetworkLab uptime is 2 days, 51 minute

Security Summary

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

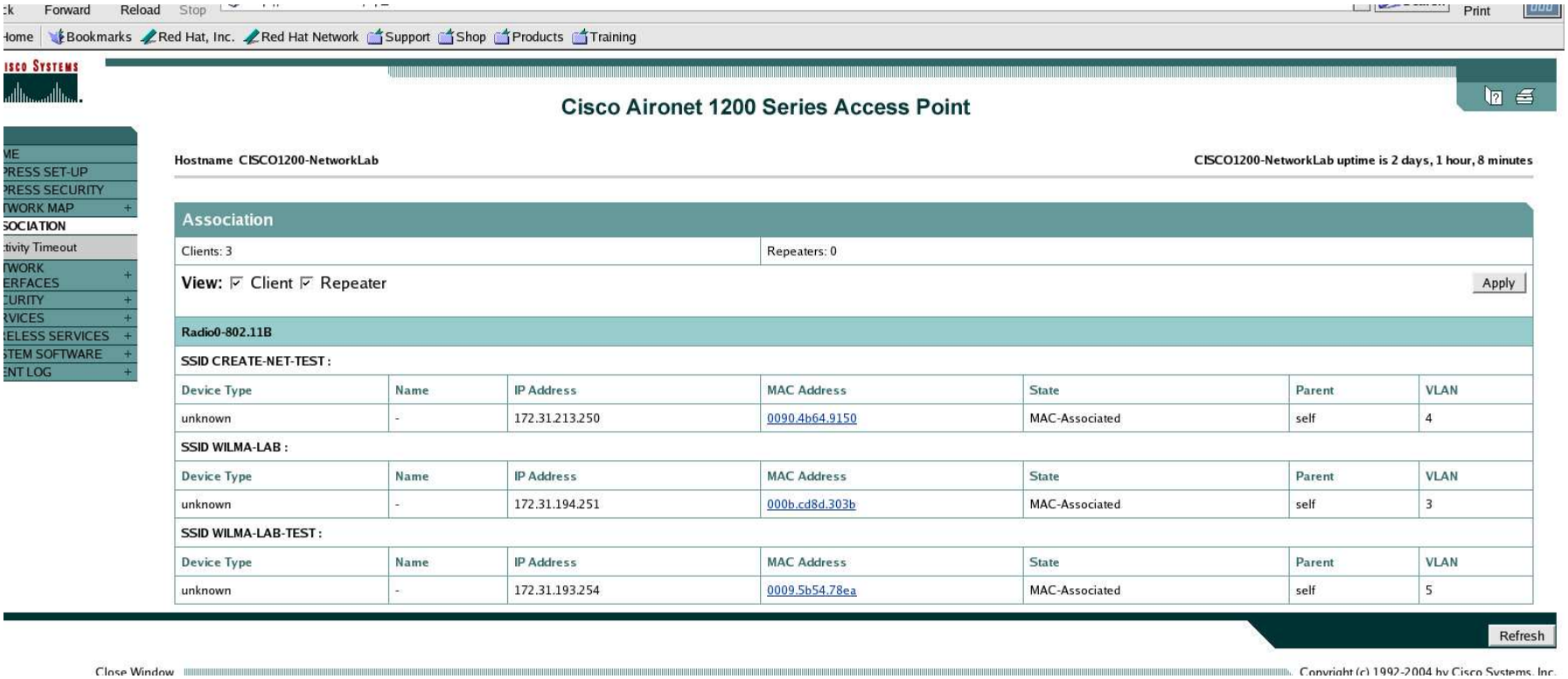
VLAN	Encryption Mode	WEP		Cipher					Key Rotation
		MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	
3	WEP-Mandatory								
4	None								
5	None								

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



Forward Reload Stop Print

Home Bookmarks Red Hat, Inc. Red Hat Network Support Shop Products Training

Cisco Aironet 1200 Series Access Point

Hostname CISCO1200-NetworkLab

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

ME
PRESS SET-UP
PRESS SECURITY
TWORK MAP +
SOCIATION
tivity Timeout
TWORK ERFACES +
CURITY +
RVICES +
ELESS SERVICES +
STEM SOFTWARE +
ENT LOG +

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	0090.4b64.9150	MAC-Associated	self	4

SSID WILMA-LAB :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	-	172.31.194.251	000b.cd8d.303b	MAC-Associated	self	3

SSID WILMA-LAB-TEST :

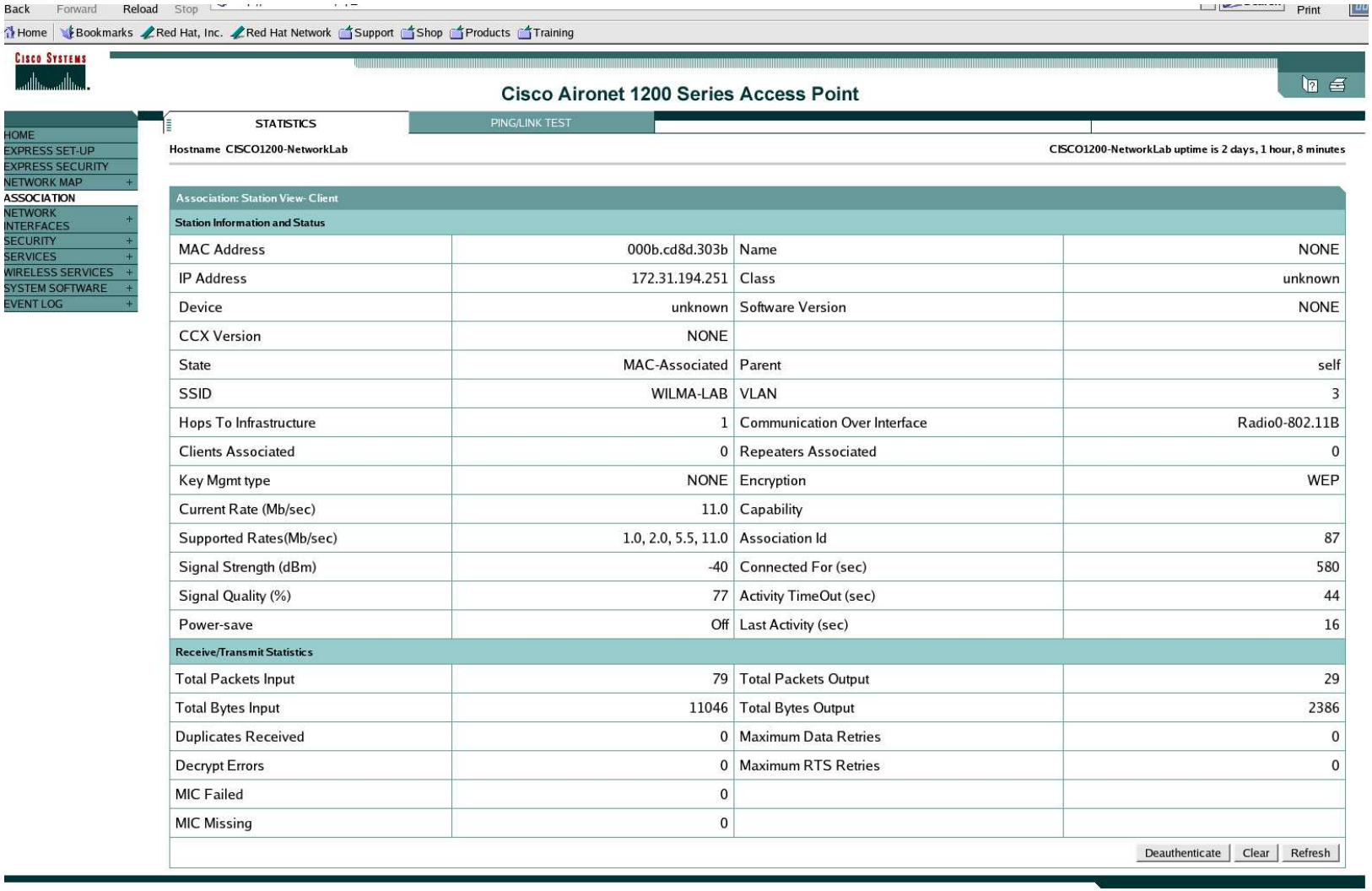
Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
unknown	-	172.31.193.254	0009.5b54.78ea	MAC-Associated	self	5

Refresh

Close Window

AP 1200: SSID and Authentication

- Client statistics



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 ssidl advertisement
 !
 ssid WILMA-LAB
    vlan 3
    authentication open mac-address mac_methods
    accounting acct_methods
    mobility network-id 3
    information-element ssidl 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