Nomadic Communications Labs

Alessandro Villani
avillani@science.unitn.it

IEEE 802.11b in brief

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

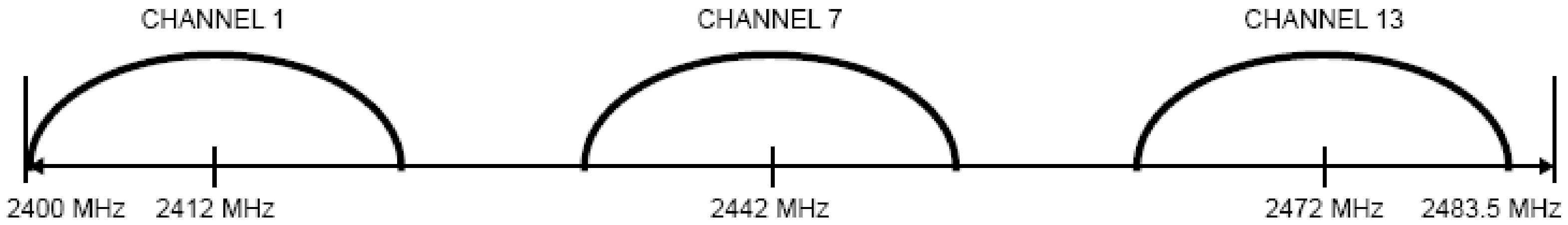


Figure 143—European channel selection—non-overlapping

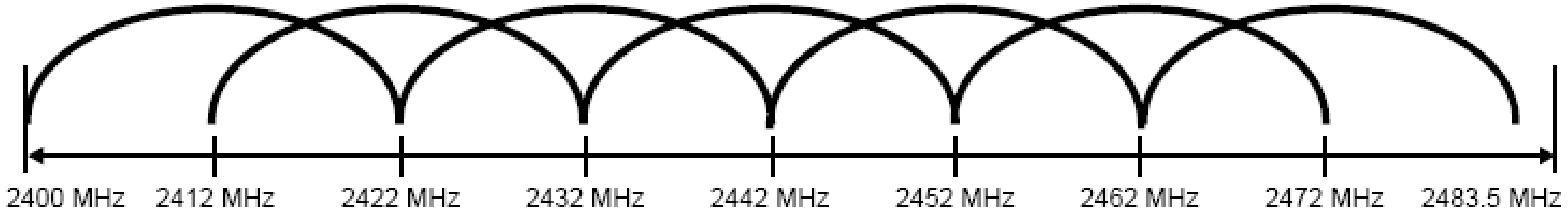


Figure 144—European channel selection—overlapping

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

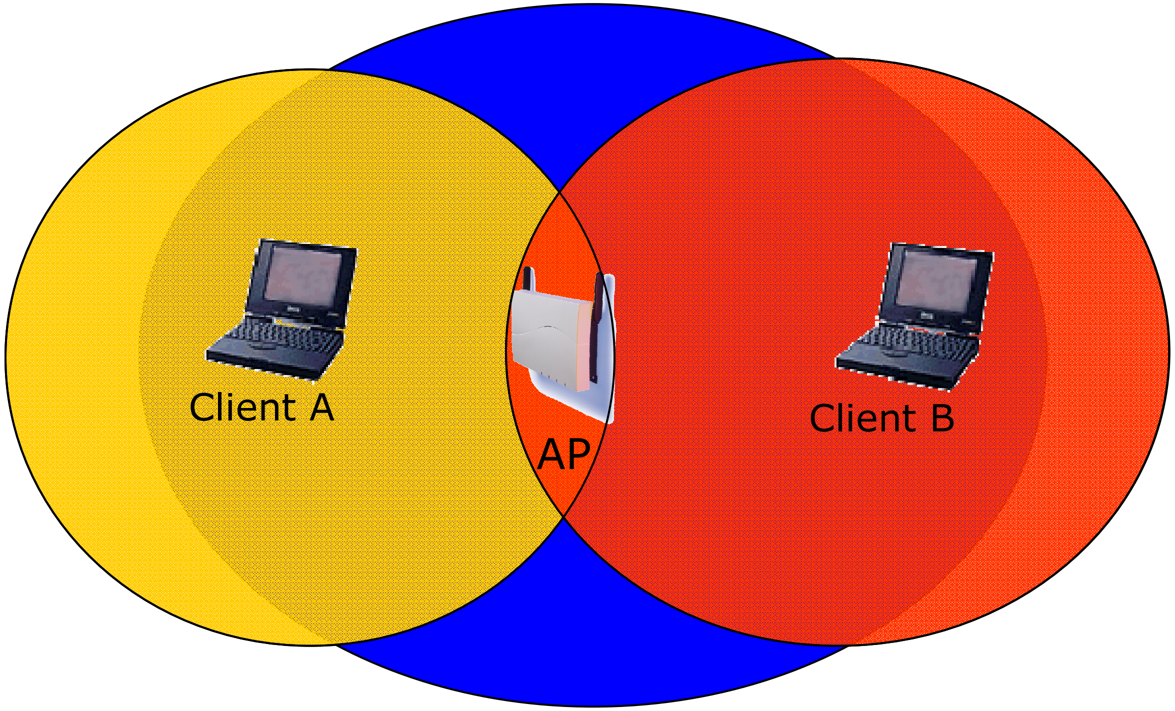
- The transmission speeds supported by the standard are:

  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:

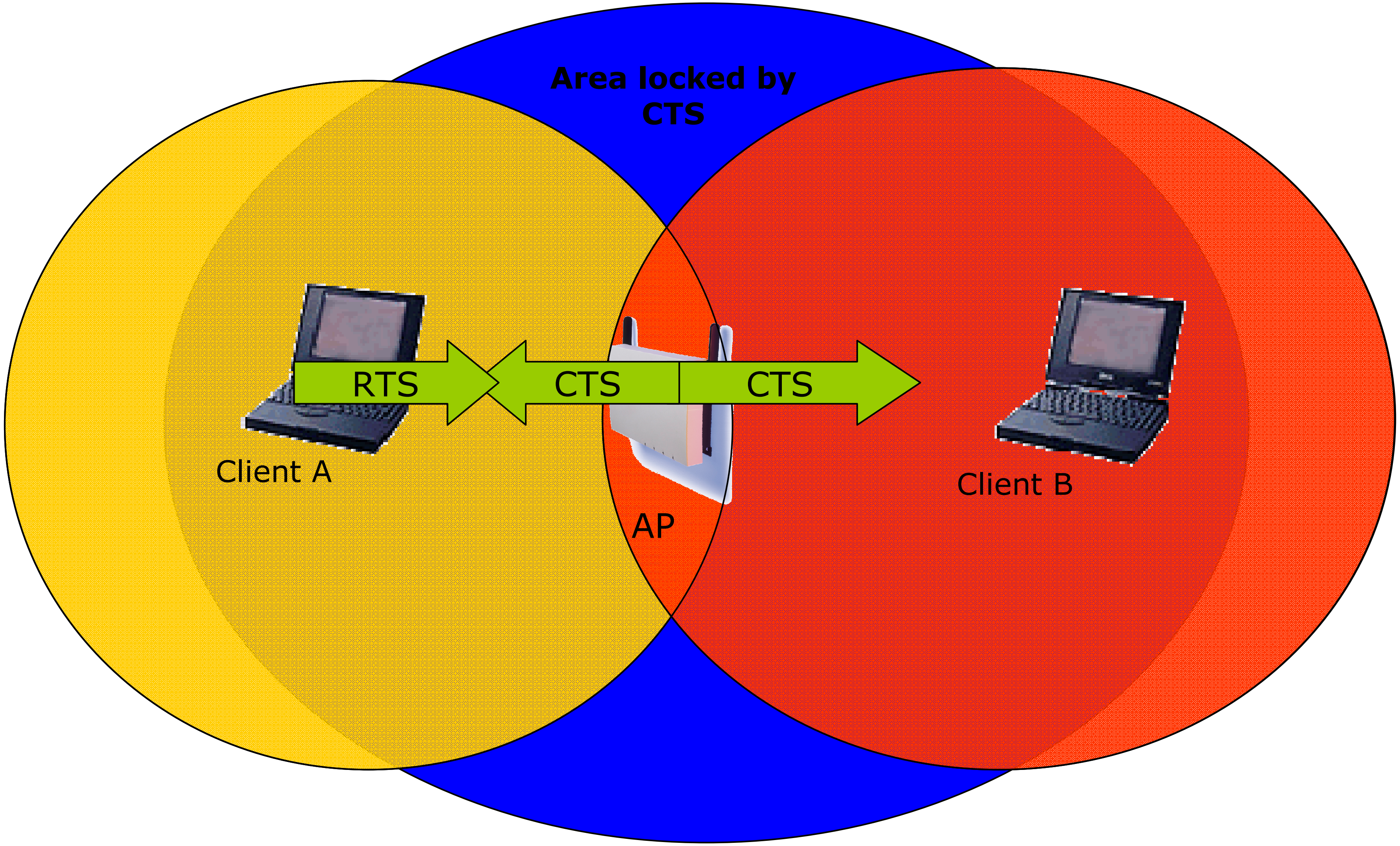


- A talk with AP (but not with B)
- B talk with AP (but not with A)

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: 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 802.11g: Speed

- The 802.11g standard introduce eight more speeds:
  - 6, 9, 12, 18, 24, 36, 48, 54
- Use OFDM (Orthogonal Frequency Division Multiplexing) for these speeds

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

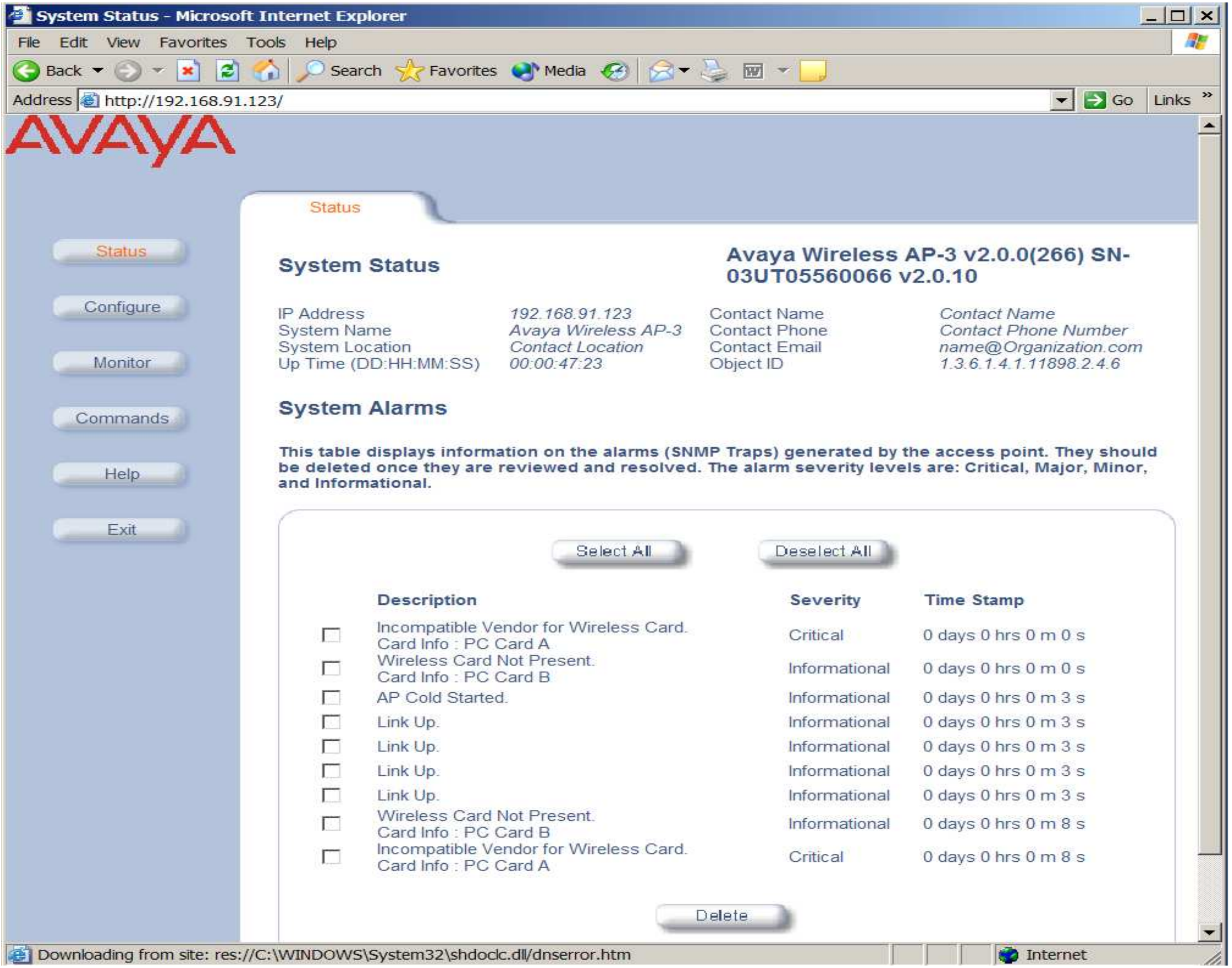
- The default IP address of the Avaya AP is 10.0.0.1
- So it is possible to reach them also via network using a cross cable or a switch/hub and using an IP in the same subnet
- Together with the software enclosed there it is a tool to find all the AP connected to the network

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



System Status - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.91.123/
Go
Links
AVAYA
Status
Status
Configure
Monitor
Commands
Help
Exit
Select All
Deselect All
Delete
Downloading from site: res://C:\WINDOWS\System32\shdoclc.dll/dnserror.htm
Internet

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.

	Description	Severity	Time Stamp
□	Incompatible Vendor for Wireless Card. Card Info : PC Card A	Critical	0 days 0 hrs 0 m 0 s
□	Wireless Card Not Present. Card Info : PC Card B	Informational	0 days 0 hrs 0 m 0 s
□	AP Cold Started.	Informational	0 days 0 hrs 0 m 3 s
□	Link Up.	Informational	0 days 0 hrs 0 m 3 s
□	Link Up.	Informational	0 days 0 hrs 0 m 3 s
□	Link Up.	Informational	0 days 0 hrs 0 m 3 s
□	Link Up.	Informational	0 days 0 hrs 0 m 3 s
□	Wireless Card Not Present. Card Info : PC Card B	Informational	0 days 0 hrs 0 m 8 s
□	Incompatible Vendor for Wireless Card. Card Info : PC Card A	Critical	0 days 0 hrs 0 m 8 s

Avaya AP: End Of Life!

- 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: 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: Channels 1-13, World: Channels 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

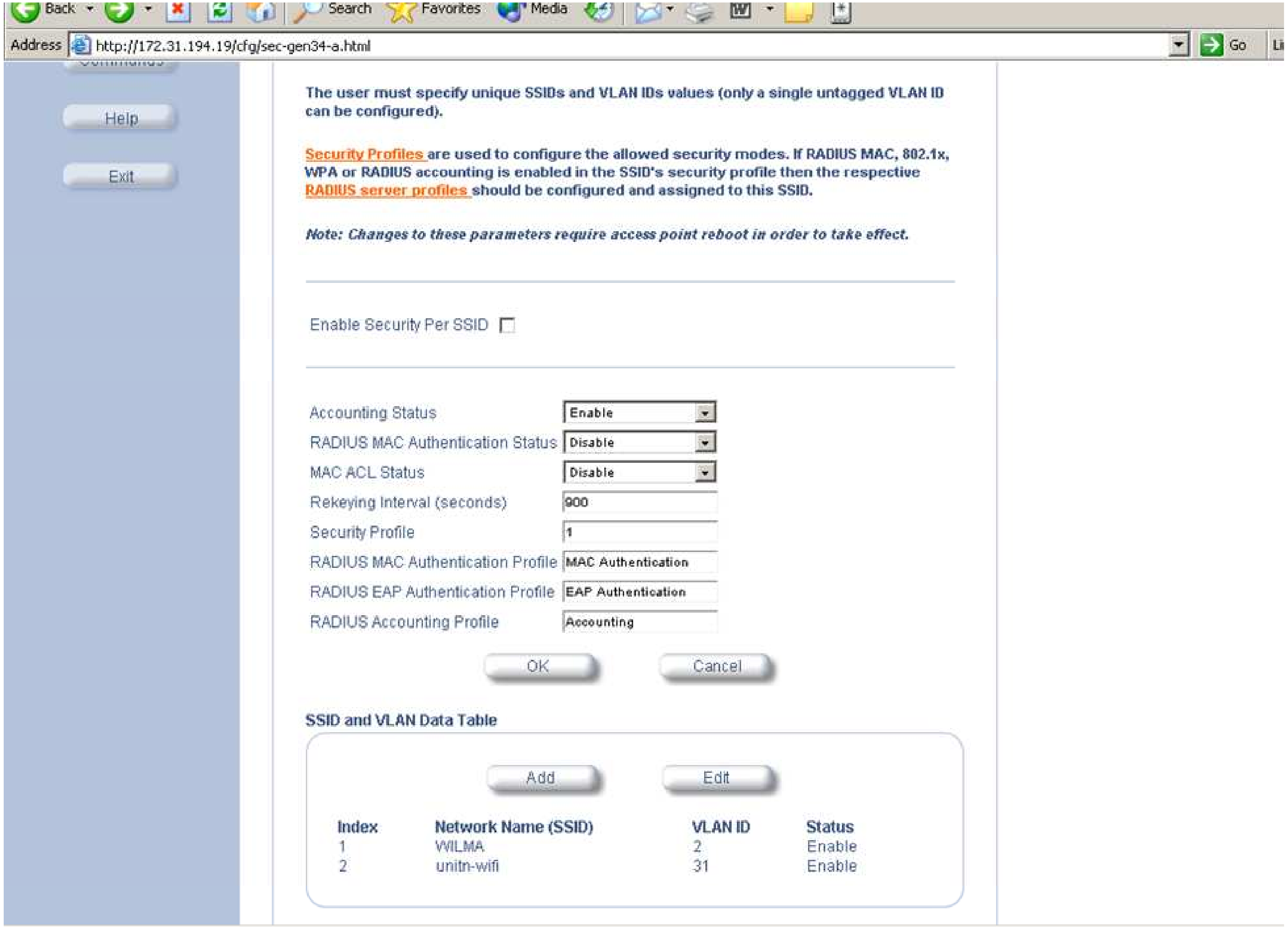
Avaya AP: Wireless Interfaces

- 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



http://172.31.194.19/cfg/sec-gen34-a.html

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)JEA3) 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

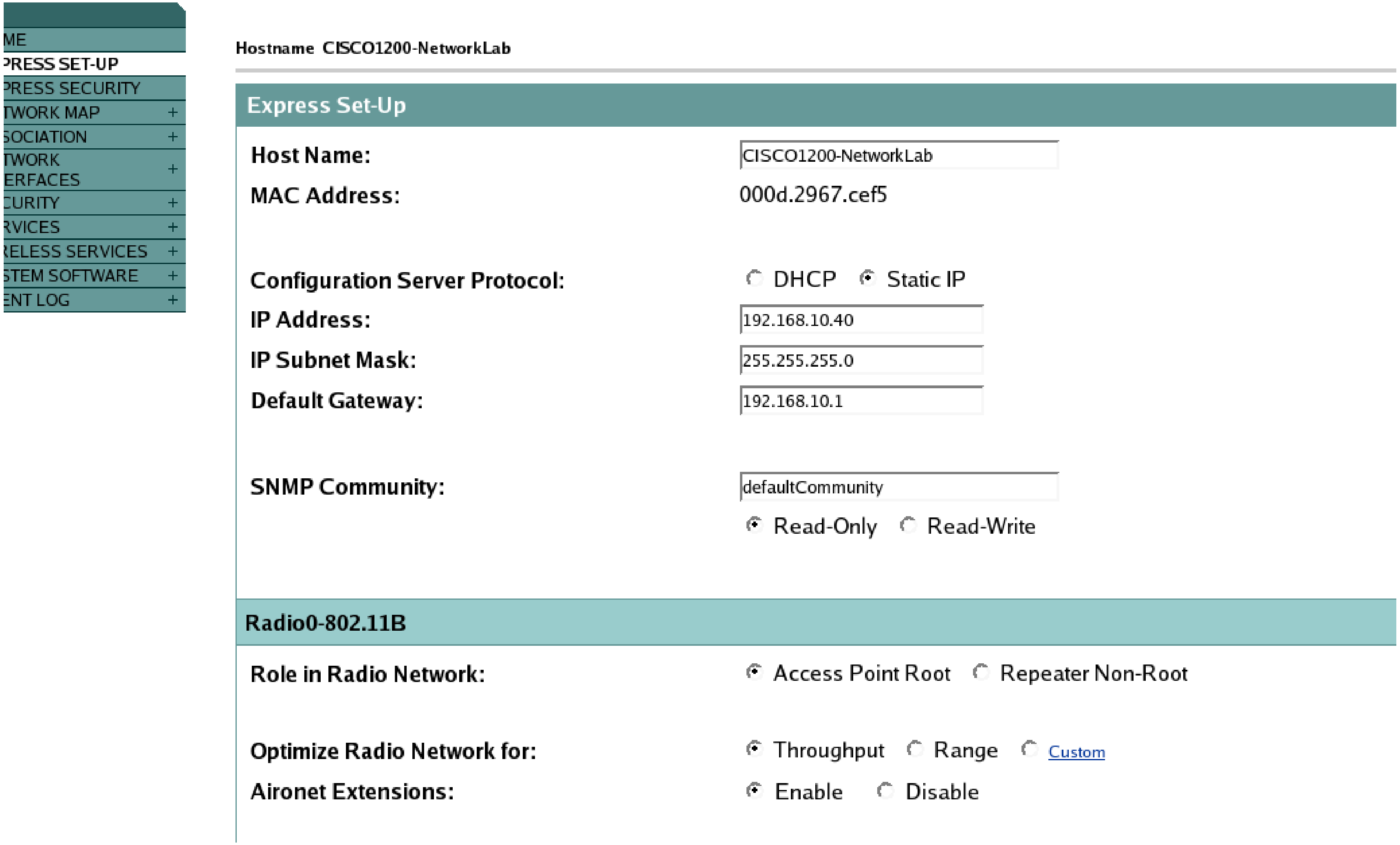
- “Standard” CISCO commands:
  - `enable`
  - *Password* → `Cisco`
  - `configure` *[terminal]*
  - `ip default-gateway 192.168.10.1`
  - `interface FastEthernet 0`
  - `ip address 192.168.10.40 255.255.255.0`
  - `exit`
  - `Ctrl-z`
  - `copy running-config startup-config`
  - `reload`

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:



Hostname CISCO1200-NetworkLab

Express Set-Up

Host Name: CISCO1200-NetworkLab

MAC Address: 000d.2967.cef5

Configuration Server Protocol: ○ DHCP ● Static IP

IP Address: 192.168.10.40

IP Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

SNMP Community: defaultCommunity

● Read-Only ○ Read-Write

Radio0-802.11B

Role in Radio Network: ● Access Point Root ○ Repeater Non-Root

Optimize Radio Network for: ● Throughput ○ Range ○ Custom

Aironet Extensions: ● Enable ○ 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.JEA3.tar
  - The AP firmware can be updated via tftp or via http

AP 1200: Wireless Configuration

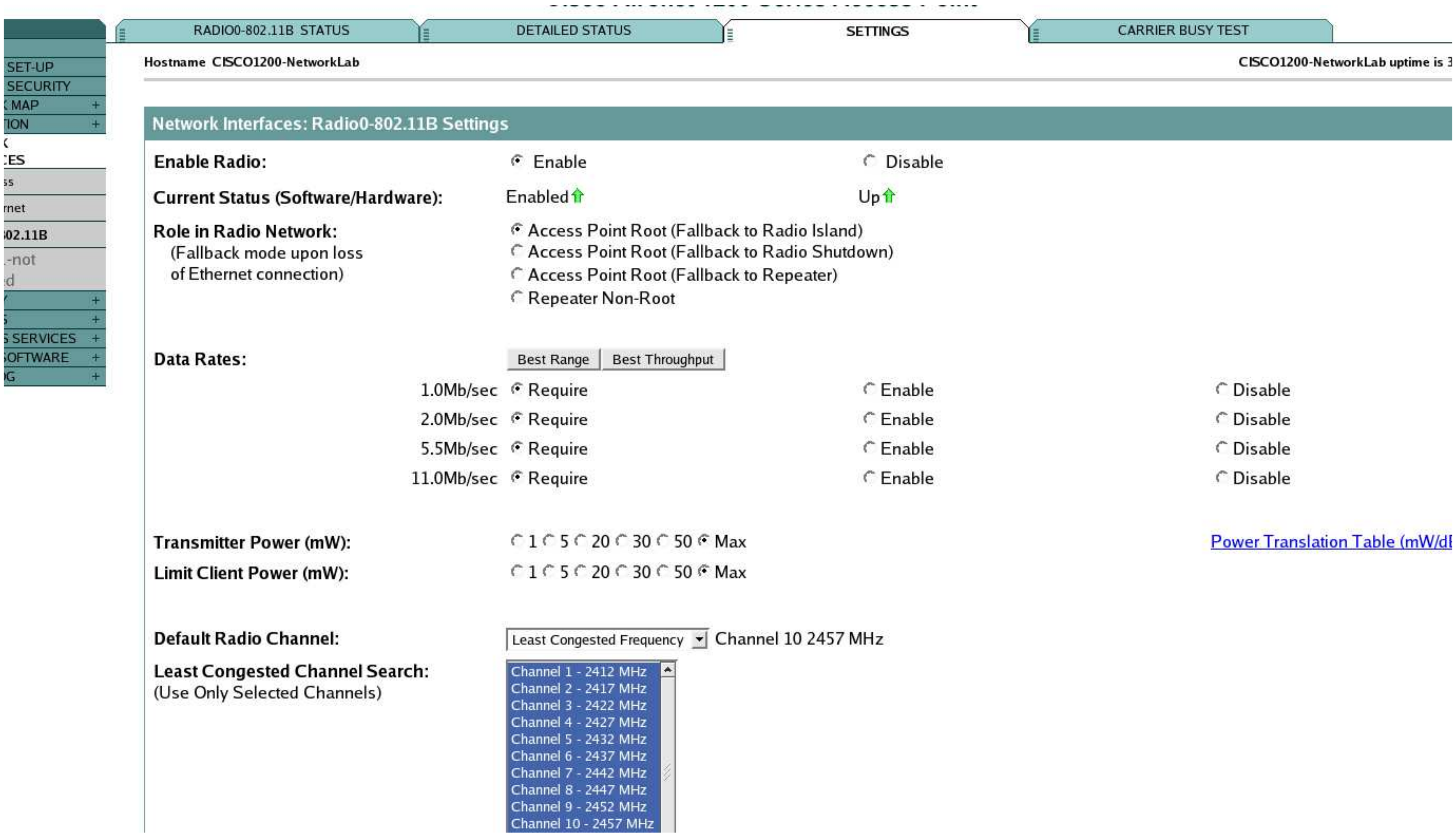
- Role in a Wireless Network:
  - Root or repeater
- Power:
  - You can limit the power of the AP radio
  - It is also possible to limit the power (in transmission) of the client stations (CISCO extensions)

AP 1200: Wireless Configuration

- Speed:
  - Basic (Require in WEB Interface): unicast and multicast traffic, used from the highest to the lowest. At least one rate must be set to basic. Note that if the client doesn’t support a Basic rate, it can not associate to the AP
  - Enabled: Unicast traffic only
  - Disabled: This speed is not usable

AP 1200: Wireless Configuration

- Configuration of the basic parameters



Hostname CISCO1200-NetworkLab

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		Power Translation Table (mW/dI
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

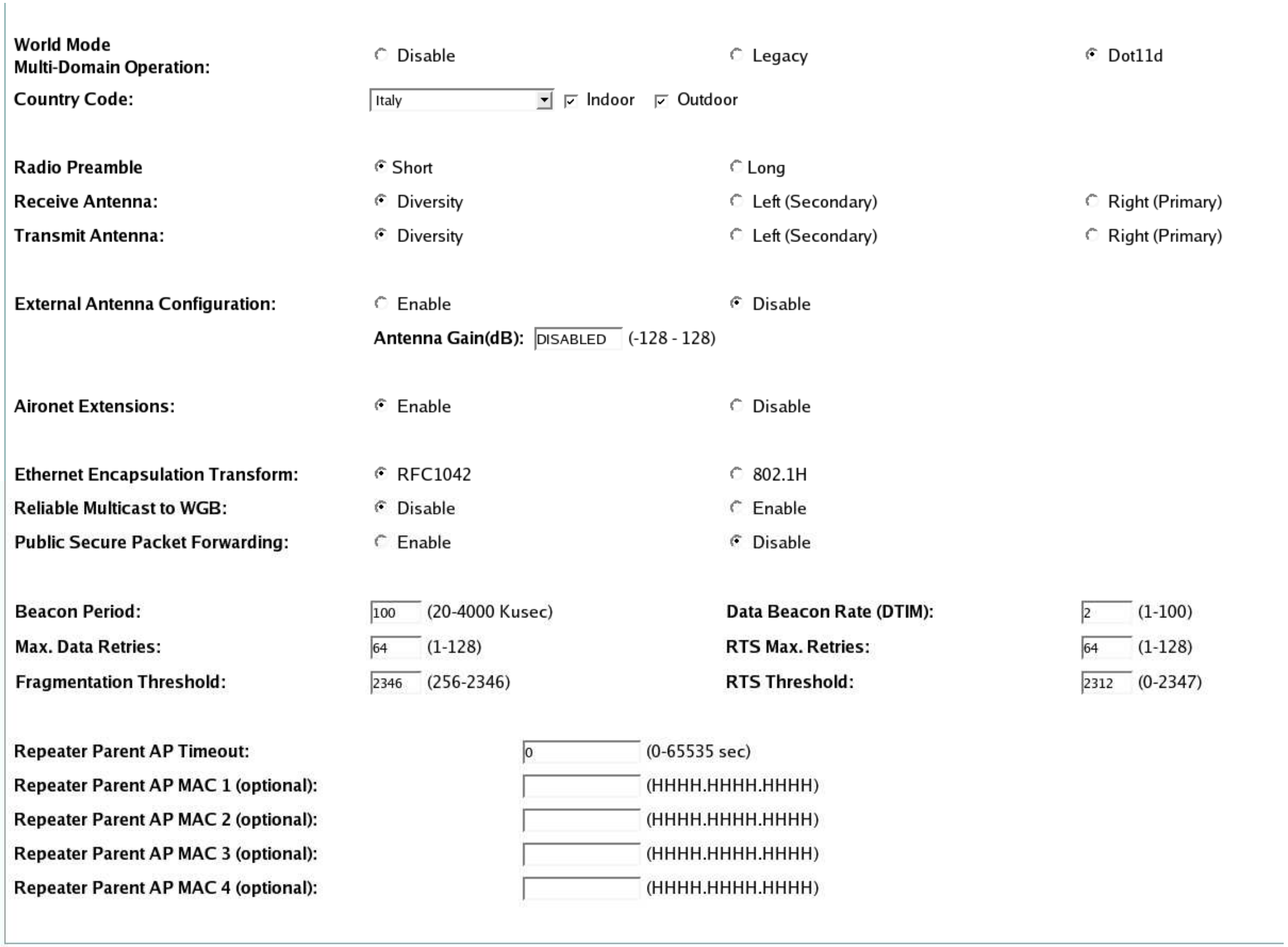
- World Mode:
  - Clients can receive “national” information about setting. Legacy for CISCO compatibility, 802.11d new standards
- Antenna:
  - Diversity: both antennas are used and the one that receives the best signal is chosen
- Encapsulation:
  - To manage the non 802.3 packages, these have to be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

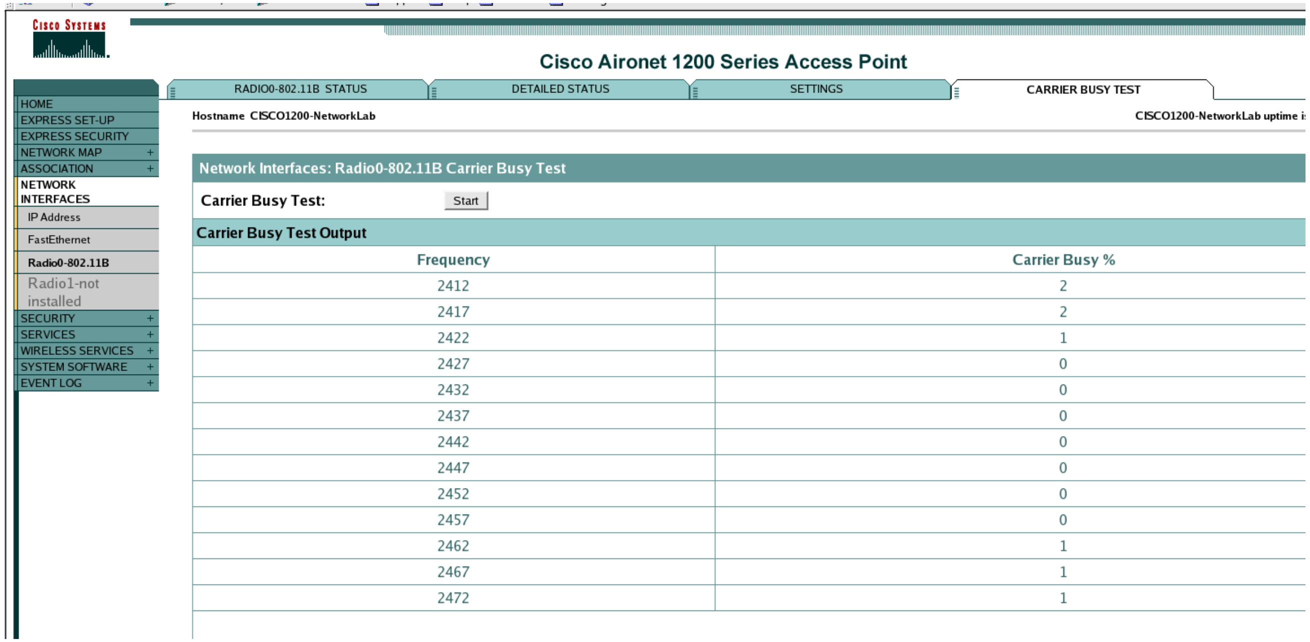
- Configuration of the basic parameters



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



Cisco Aironet 1200 Series Access Point

Hostname CISCO1200-NetworkLab

CISCO1200-NetworkLab uptime i

Network Interfaces: Radio0-802.11B Carrier Busy Test

Carrier Busy Test: Start

Carrier Busy Test Output

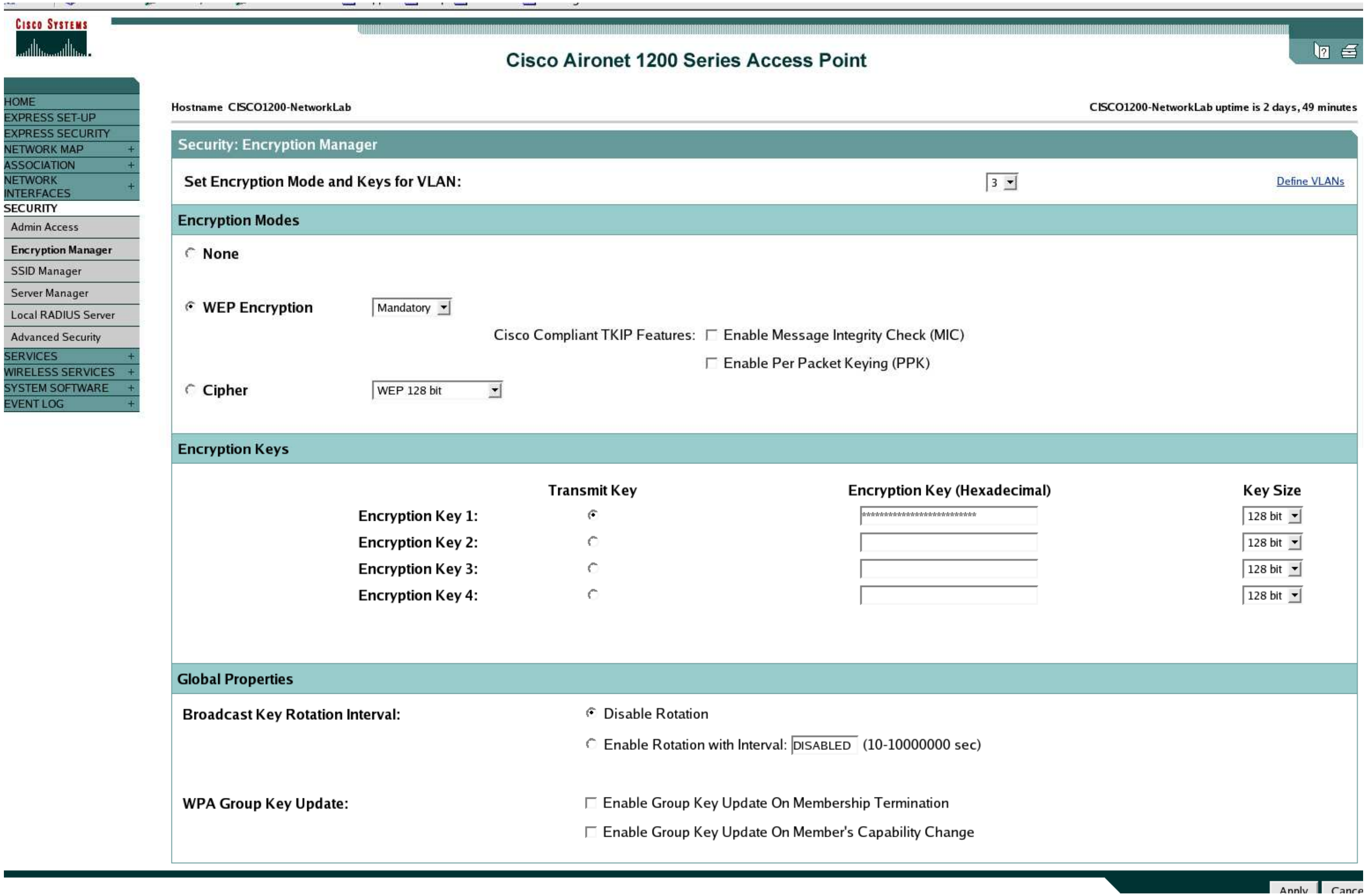
Frequency	Carrier Busy %
2412	2
2417	2
2422	1
2427	0
2432	0
2437	0
2442	0
2447	0
2452	0
2457	0
2462	1
2467	1
2472	1

AP 1200: 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

- Definition of Cryptography



Cisco Aironet 1200 Series Access Point

Hostname CISCO1200-NetworkLab

CISCO1200-NetworkLab uptime is 2 days, 49 minutes

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 3

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:	●	**************************	128 bit
Encryption Key 2:	○		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Global Properties

Broadcast Key Rotation Interval: ● Disable Rotation

○ Enable Rotation with Interval: DISABLED (10-10000000 sec)

WPA Group Key Update: □ Enable Group Key Update On Membership Termination

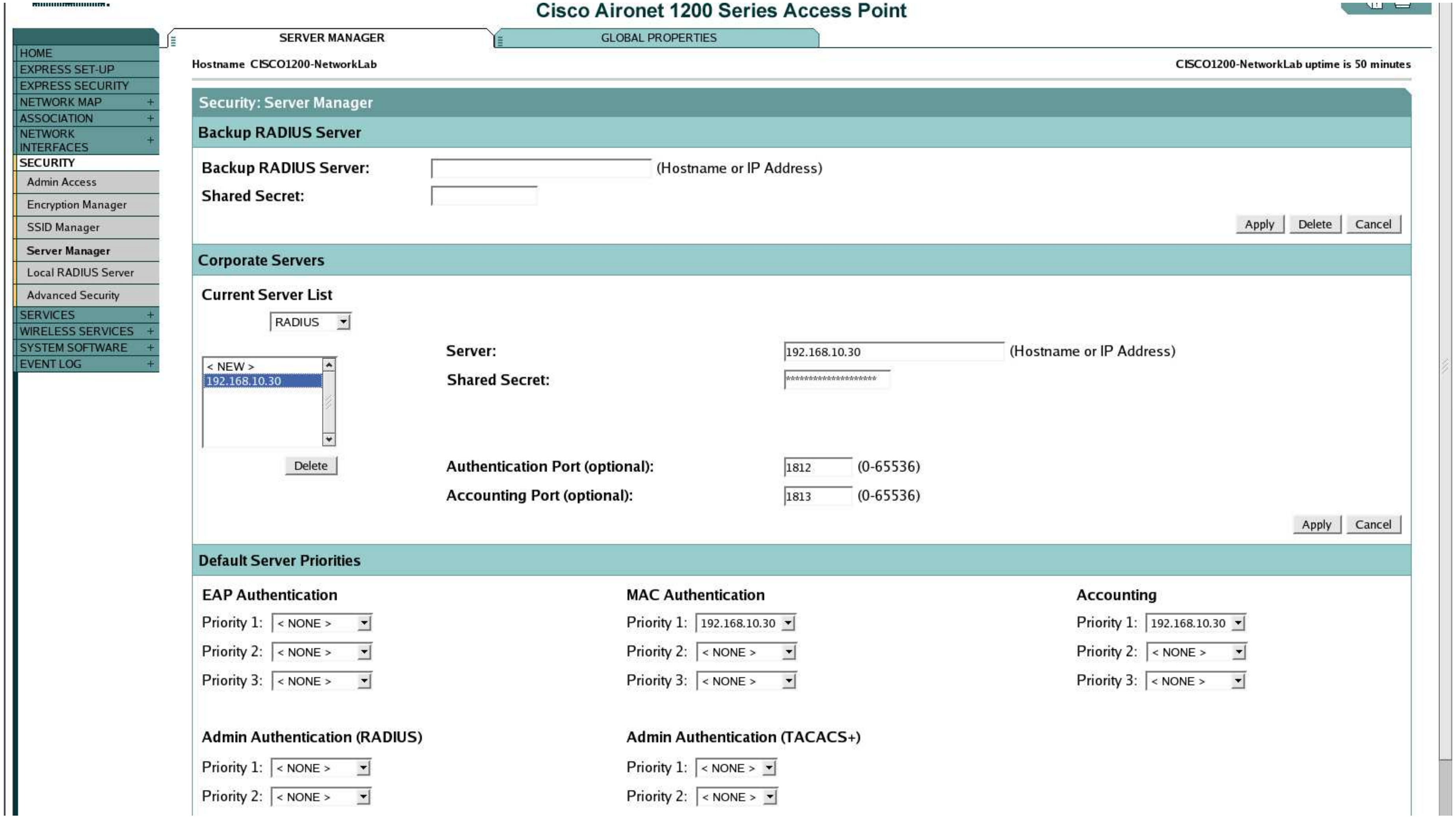
□ Enable Group Key Update On Member's Capability Change

AP 1200: 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: Radius Server

- Radius Server Configuration:



Hostname CISCO1200-NetworkLab

CISCO1200-NetworkLab uptime is 50 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Corporate Servers

Current Server List

RADIUS

< NEW >
192.168.10.30

Server: 192.168.10.30 (Hostname or IP Address)

Shared Secret: *******************

Authentication Port (optional): 1812 (0-65536)

Accounting Port (optional): 1813 (0-65536)

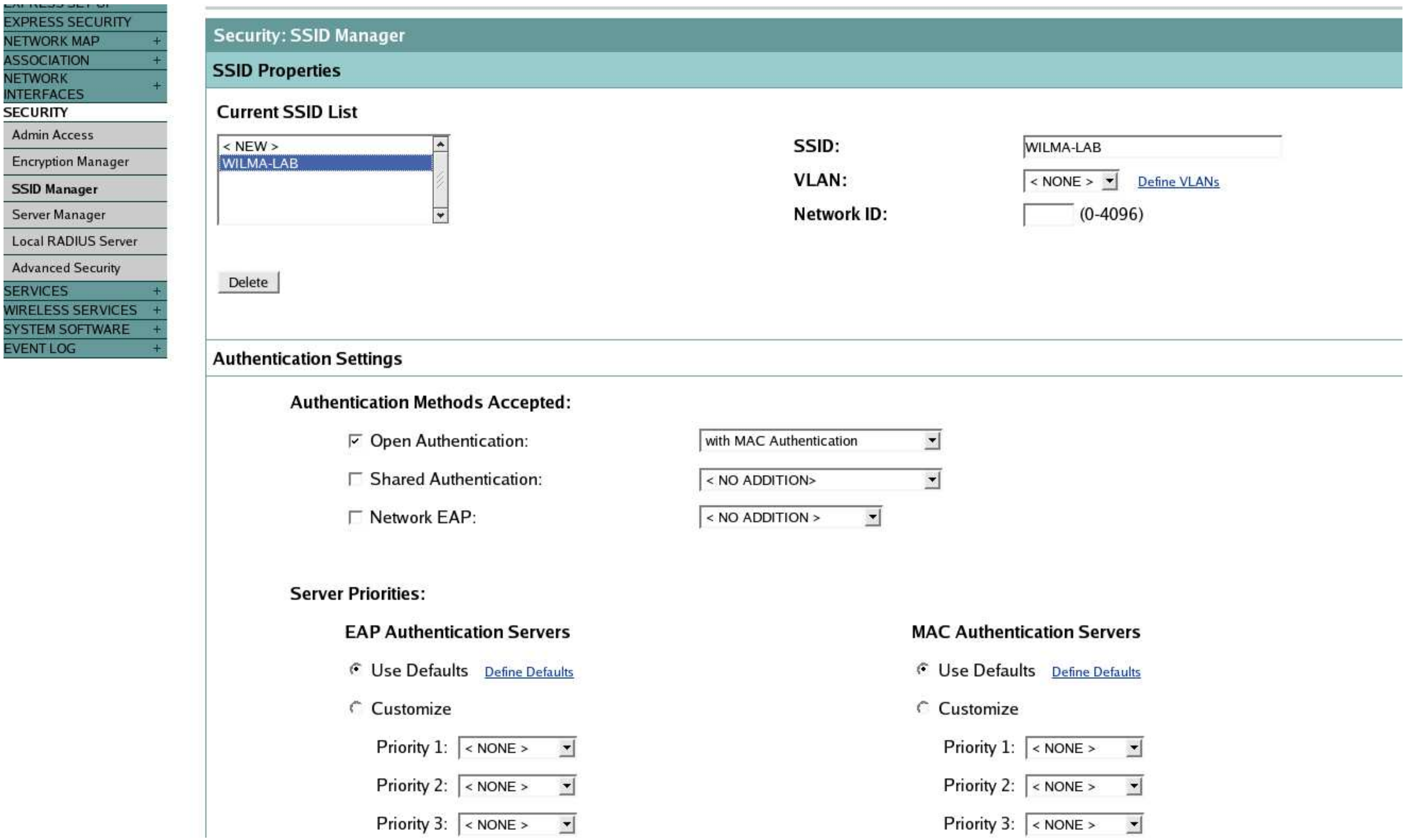
Default Server Priorities

EAP Authentication		MAC Authentication		Accounting	
Priority 1:	< NONE >	Priority 1:	192.168.10.30	Priority 1:	192.168.10.30
Priority 2:	< NONE >	Priority 2:	< NONE >	Priority 2:	< NONE >
Priority 3:	< NONE >	Priority 3:	< NONE >	Priority 3:	< NONE >

Admin Authentication (RADIUS)		Admin Authentication (TACACS+)	
Priority 1:	< NONE >	Priority 1:	< NONE >
Priority 2:	< NONE >	Priority 2:	< NONE >

AP 1200: SSID and Authentication

- SSID and Radius Server:



Security: SSID Manager

SSID Properties

Current SSID List

< NEW >
WILMA-LAB

SSID: WILMA-LAB

VLAN: < NONE > Define VLANs

Network ID: (0-4096)

Authentication Settings

Authentication Methods Accepted:

☑ Open Authentication: with MAC Authentication

☐ Shared Authentication: < NO ADDITION>

☐ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

● Use Defaults Define Defaults

○ Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

● Use Defaults Define Defaults

○ Customize

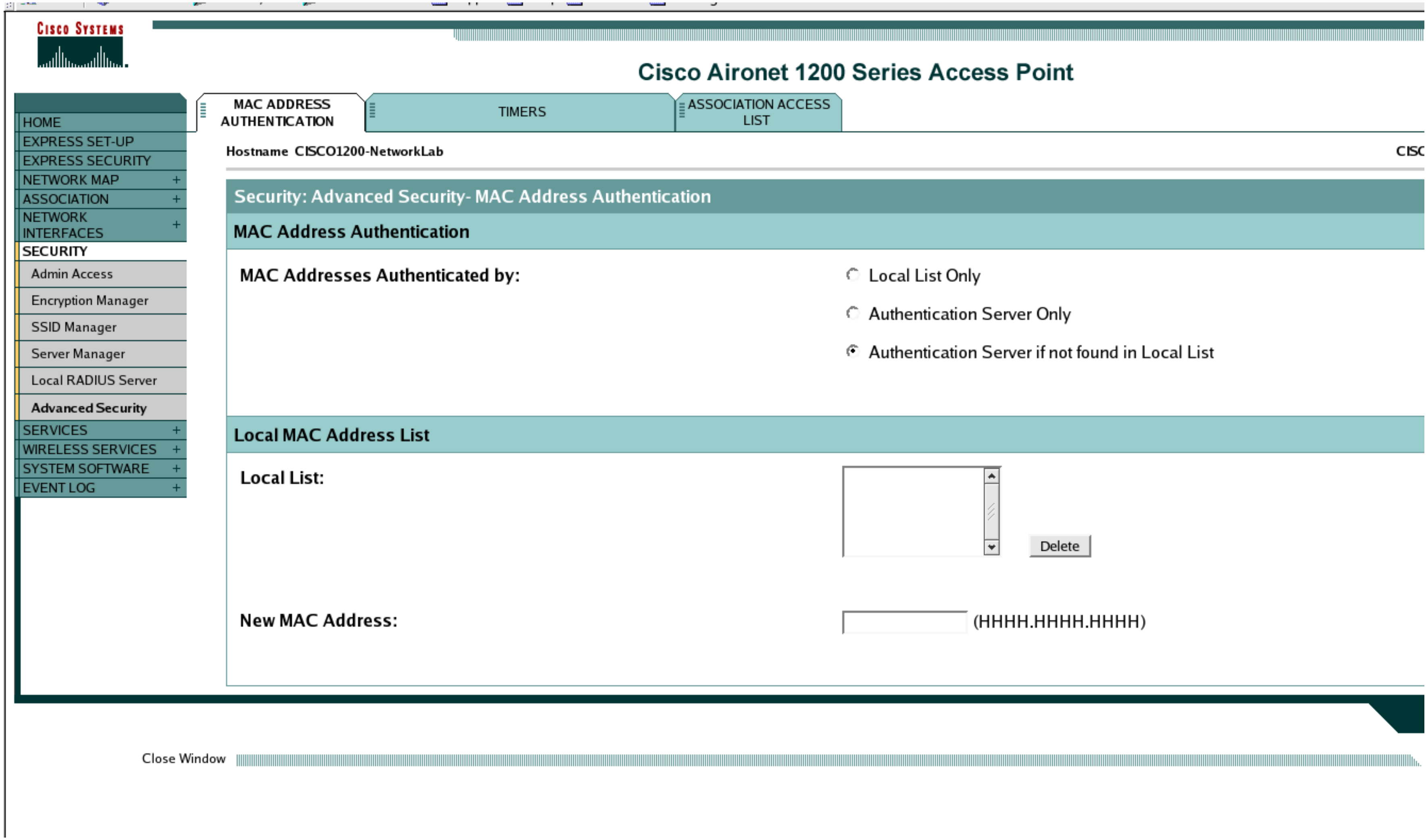
Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

AP 1200: SSID and Authentication

- MAC Address Authentication:



Hostname CISCO1200-NetworkLab

Security: Advanced Security- MAC Address Authentication

MAC Address Authentication

MAC Addresses Authenticated by:
○ Local List Only
○ Authentication Server Only
● Authentication Server if not found in Local List

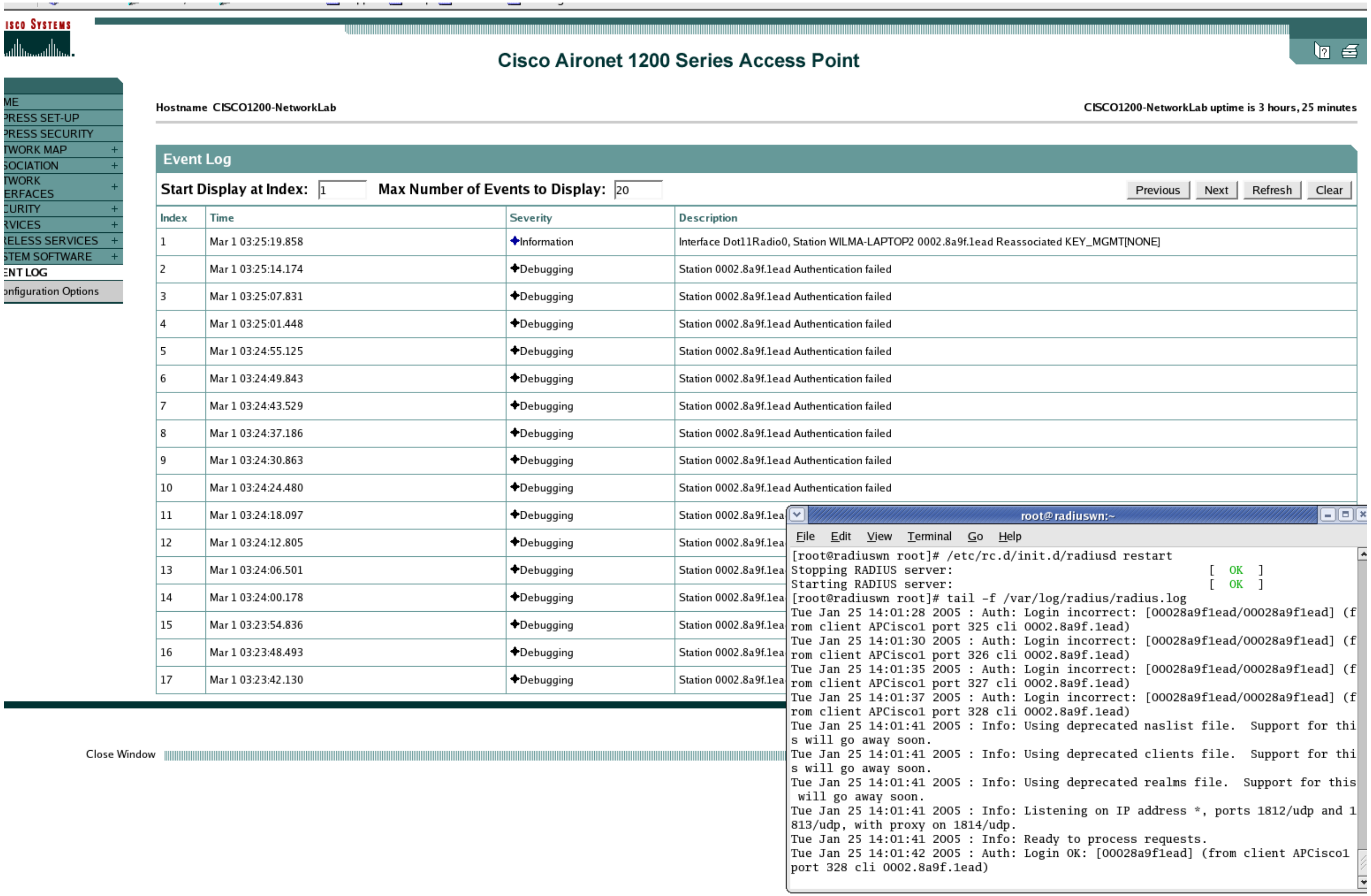
Local MAC Address List

Local List:

New MAC Address: (HHHH.HHHH.HHHH)

AP 1200: SSID and Authentication

- MAC Address Authentication:



Hostname CISCO1200-NetworkLab

CISCO1200-NetworkLab uptime is 3 hours, 25 minutes

Start Display at Index: 1 Max Number of Events to Display: 20

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.1ea
12	Mar 1 03:24:12.805	✦Debugging	Station 0002.8a9f.1ea
13	Mar 1 03:24:06.501	✦Debugging	Station 0002.8a9f.1ea
14	Mar 1 03:24:00.178	✦Debugging	Station 0002.8a9f.1ea
15	Mar 1 03:23:54.836	✦Debugging	Station 0002.8a9f.1ea
16	Mar 1 03:23:48.493	✦Debugging	Station 0002.8a9f.1ea
17	Mar 1 03:23:42.130	✦Debugging	Station 0002.8a9f.1ea

```
[root@radiuswn root]# /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 this
 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: 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
```

Analysis of the performances of a Wireless network

IPERF

- Several tools exist for the performances measurement of a network each one with different purposes:
  - Iperf:
    - http://dast.nlanr.net/Projects/Iperf/
  - d-itg:
    - http://www.grid.unina.it/software/ITG/
  - Netperf:
    - http://www.netperf.org/netperf/NetperfPage.html

IPERF: the test

- We want to measure how the performances vary changing some parameters of the configuration of the AP
- We choose IPERF
- After every modification of a parameter run N times IPERF (N>20):
  - We remove the lowest values (10%)
  - We compute the average
  - It is of interest also the best result!

IPERF: the test

- For Avaya AP (after any change of the AP parameters you have to reboot it):
  - Change the working mode: 802.11b, 802.11g, 802.11b/g
  - Change the threshold for RTS/CTS
  - Change the transmission speed (not affected the receiving speed of the AP)
- For CISCO AP:
  - Change the threshold for RTS/CTS
  - Change the threshold for fragmentation
  - Change the speed used

IPERF: Examples

- For example for an Avaya AP:

Speed 54 Mb/sec	Speed 11 Mb/sec
10.0 sec, 25.1 MBytes→ 21.1 Mbits/sec	10.0 sec, 7.03 MBytes→ 5.89 Mbits/sec
10.0 sec, 24.4 MBytes→ 20.4 Mbits/sec	10.0 sec, 7.16 MBytes→ 6.00 Mbits/sec

- Therefore approximately:
  - Speed ratio: 54/11 = 4.9
  - Performance ratio: 20.75 / 5.945 = 3.49

IPERF: Examples

- For example for a CISCO AP:

Speed 11 Mb/sec	**Speed 1 Mb/sec**
10.0 sec, 2.75 MBytes→ 2.30 Mbits/sec	10.4 sec, 872 KBytes→ 684 Kbits/sec
10.0 sec, 3.20 MBytes→ 2.67 Mbits/sec	

- Therefore approximately:
  - Speed ratio: 11/1 = 11
  - Performance ratio: 2.49 / 0.684 = 3.64

IPERF: Setup

- The IPERF server (iperf –u –s) is on:
  - 192.168.10.30
- You have to run iperf with a command like:
  - iperf –c 192.168.10.30 –u –b20M –i 5 –t 20
- Where:
  - -i 5 means a report any 5 seconds
  - -t 20 means a simulation 20 seconds long
  - -u means UDP transfer mode
  - -b 20M means a bandwith of 20Megabits

IPERF: setup

- For Avaya AP, RTS/CTS and fragmentation test: use bidirectional run!
  - -r: do a bidirectional test separately
  - -d: do a bidirectional test simultaneously

  Do the analysis of the data obtained for the two direction separately (use –r)
- Pay attention to MTU and packet size: choose the threshold for RTS/CTS and fragmentation accordingly with these lengths!

IPERF: setup

- Avaya AP:
  - IP: 192.168.10.15
  - SSID: NCA
  - Passwd: public
- Cisco 1230B:
  - IP: 192.168.10.10
  - SSID: NCB
  - Passwd: Cisco
- Cisco 1310:
  - IP: 192.168.10.5
  - SSID: NCG
  - Passwd: Cisco

IPERF: setup

- Server: 192.168.10.30
- Login: wifitest
- Passwd: wifitest
- Gain root privileges: sudo bash
- Startup of services (network/dhcpd/iperf): ./nomadic.sh
- Connect all the device (the 3 AP and the laptop-server) to the DLink gigabit switch
- Use the white network cable to connect the laptop

Lab Report

- You have to:
  - Describe the setup of the test
  - Do a theoretical analysis of the expected results
  - Describe the result obtained with graphs and tables
  - **VERY IMPORTANT**: Do some analysis on the data (Average, Max, Min, Standard Deviation, …)
  - Write some conclusions