IV Foro de Seguridad de RedIRIS

Diseño, implantación y securización de redes wifi

fs2006

IV Foro de Seguridad RedIRIS

UPV · EHU

Diseño, implantación y securización de servicios wifi

Toni Pérez
Universitat de les Illes Balears

toni.perez@uib.es

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

RedIRIS

Servicios wifi

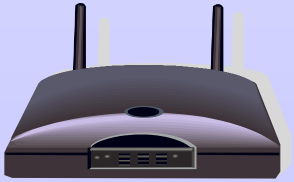
- La seguridad debe de estar presente desde el principio!!
- Diseño:
  - Que tiempos aquellos: hubs sin gestión!!
    - Ahora: UPNs: Redes personalizadas con control de admisión
  - Conocer los protocolos no es suficiente..
    - Conocer los productos y soluciones del mercado
- Implantación
  - Desconfiados …
    - No!!, escarmentados por la experiencia!!!
- Securización
  - Si funciona… para que??
  - Al abrir los ojos…¿Y si eliminamos el servicio?

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Elementos

- Elementos
  - Clientes
    - Centrino
    - PCMCIAs
    - PDAs
    - Teléfonos wifi
    - Cámaras de fotos
    - Discos duros …
  - Puntos de acceso (APs)
    - Antenas (Direccionales, omnidireccionales, arrays)
    - Acceso a la red de distribución



El protocolo

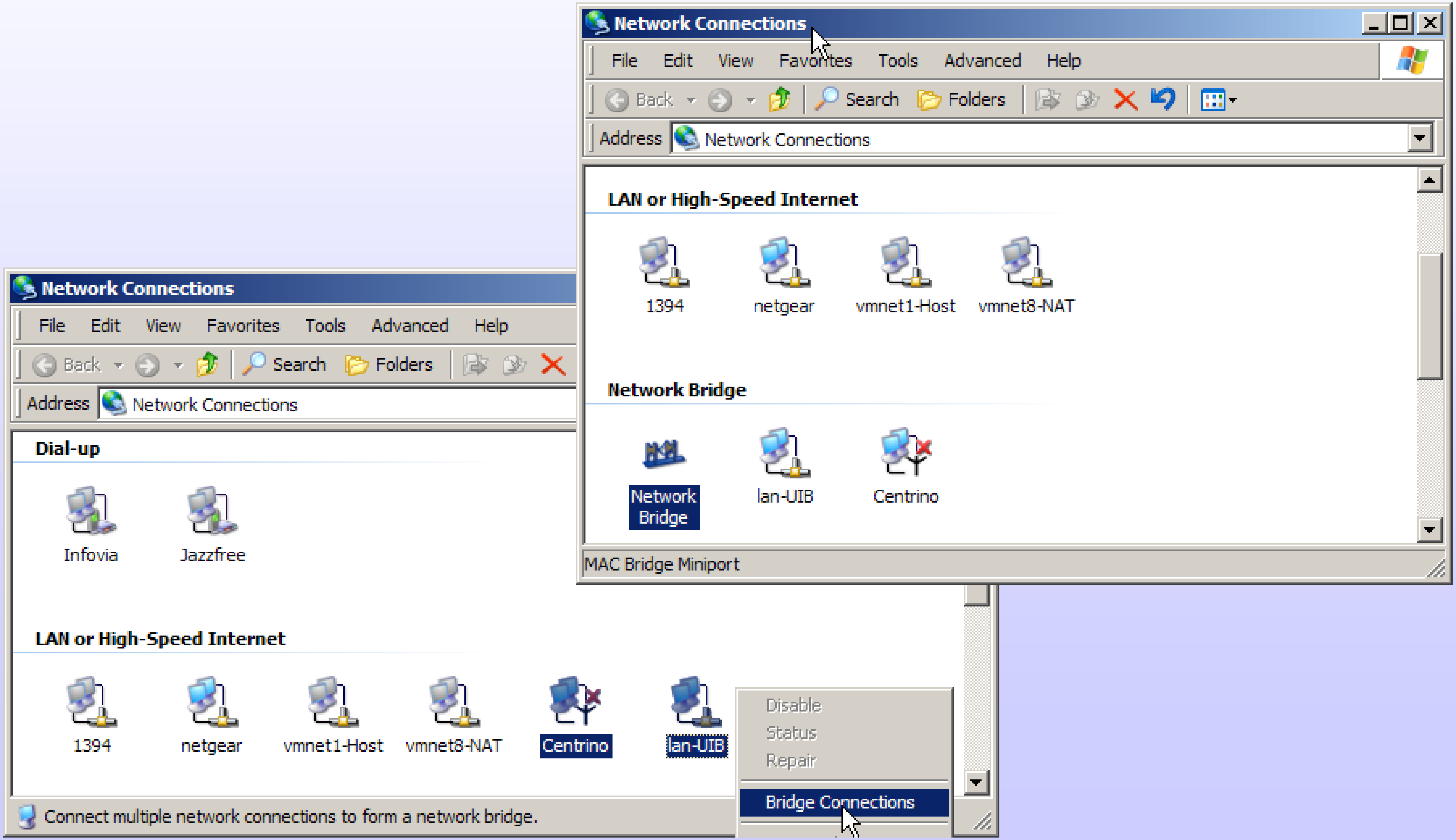
- 802.11: el protocolo
  - Capa física
    - 802.11b/g: 2,4Ghz (13ch Europa, 11ch EEUU, 14ch Japón)
    - 802.11a: 5Ghz (19ch Europa, 12ch EEUU, 4ch Japón)
    - Clientes y APs: b, b/g, a/b/g
  - Capa MAC
    - Direcciones 48bits
      - Destino, Origen, BSSID (MAC-AP), AP-Destino (Punto a Punto-Multipunto)
      - Bits To-DS, From-DS
        - Infraestructura: From DS ó To DS
        - Punto a Punto-Multipunto: From DS y To DS
        - Ad-hoc: Ninguno
    - Bit indicando cifrado WEP

Redes Ad-hoc

- Redes Ad-hoc
  - Entre clientes wifi sin utilizar un AP
  - Clientes expuestos en un medio incontrolable
  - Producen interferencias en el canal
  - Bridge en Windows XP

Redes Ad-hoc

- Windows XP Bridge!!!

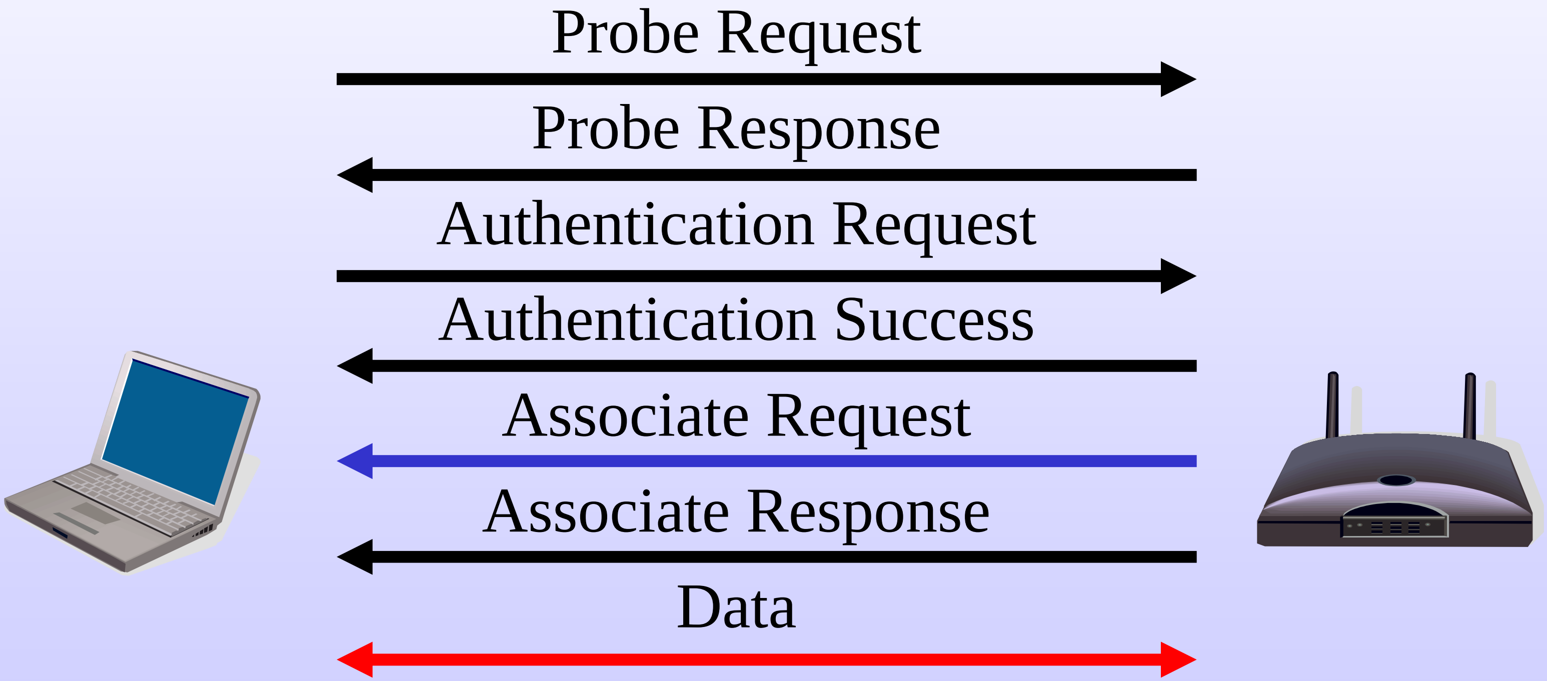


MAC Bridge Miniport

Connect multiple network connections to form a network bridge.

Redes Infraestructura

- Puntos de Acceso y clientes: Asociación
  - El cable “virtual”



Probe Request

Probe Response

Authentication Request

Authentication Success

Associate Request

Associate Response

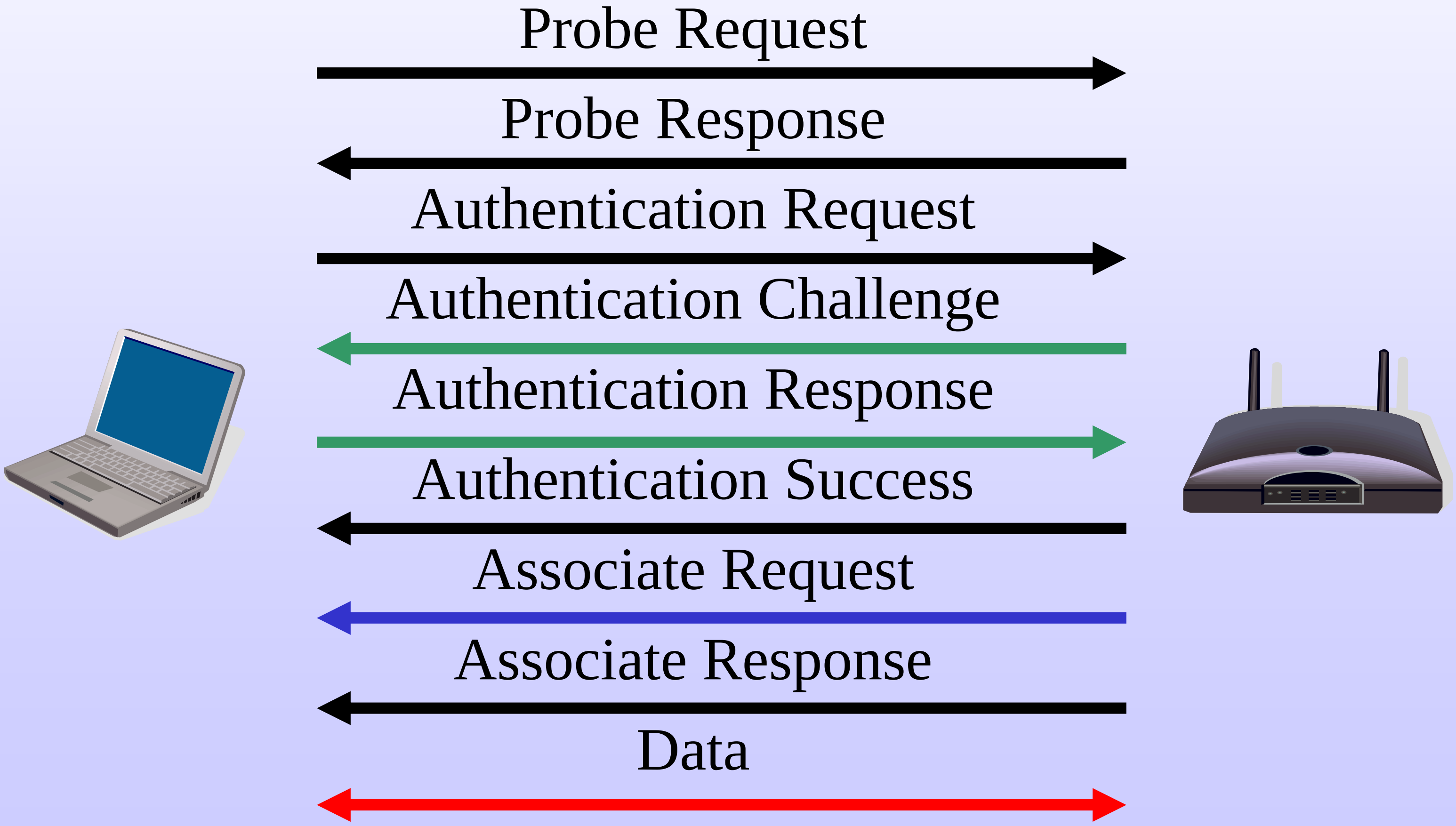
Data

Asociación

- Authentication: ¿Es un secreto el SSID?
  - El AP realiza anuncios con el SSID
  - Podemos optar por ocultarlo → Cloacked Node
  - ¿Es necesario complicar la asociación?
    - Fácilmente se puede capturar con multitud de herramientas
    - Un secreto compartido... ¿Es secreto?
- La asociación debe de ser un proceso sencillo
  - No nos compliquemos la vida....

Redes Infraestructura

- Asociación: Closed Node (cifrado wep)
  - Intentando blindar el cable virtual



Probe Request

Probe Response

Authentication Request

Authentication Challenge

Authentication Response

Authentication Success

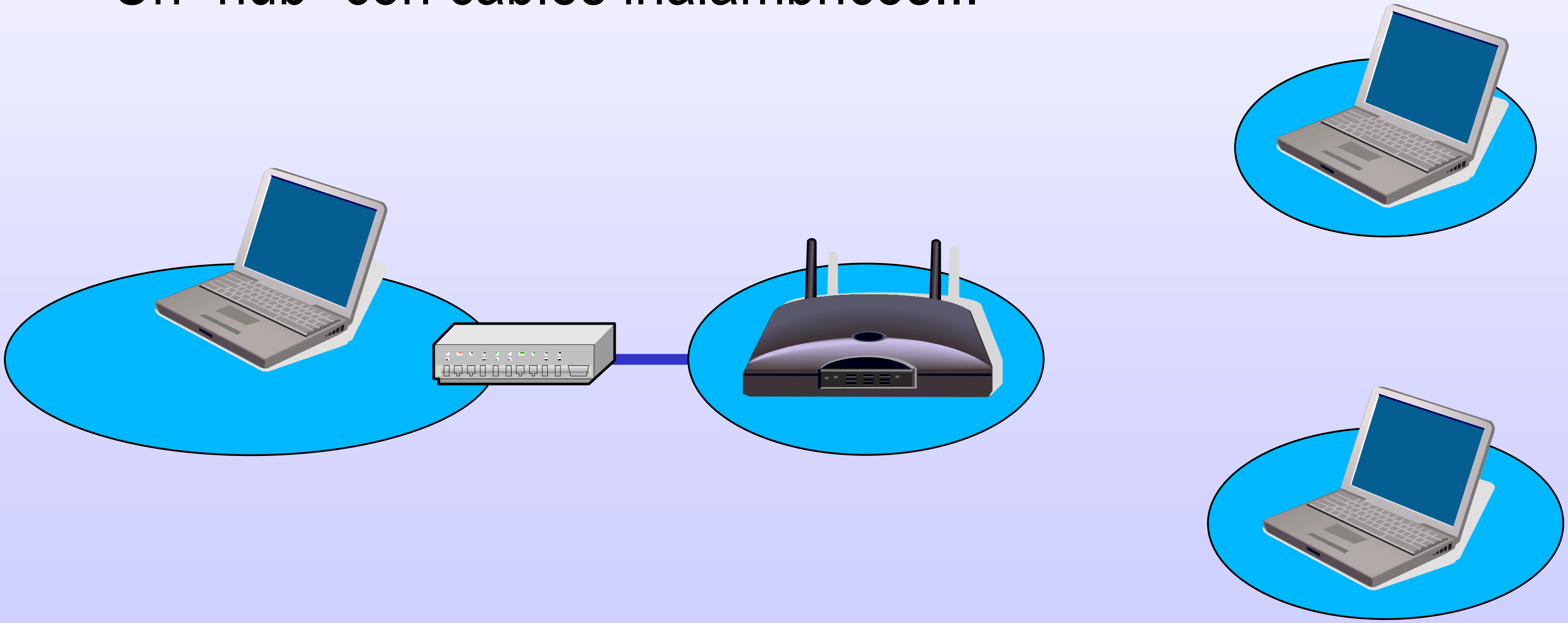
Associate Request

Associate Response

Data

Redes Infraestructura

- Extender un dominio de broadcast al medio inalámbrico
  - Un "hub" con cables inalámbricos...



Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Escenarios

- Usuarios domésticos
  - Usuarios que acceden a servicios corporativos
  - Redes públicas o personales
  - La wifi del vecino…
- La empresa
  - Entorno controlado y gestionado
  - Espacios y usuarios limitados
- La universidad
  - Perfiles de usuarios: PDI, PAS, ALU, temporales, …
  - Eventos temporales (congresos)
  - Gran movilidad de usuarios: espacios abiertos

Agenda

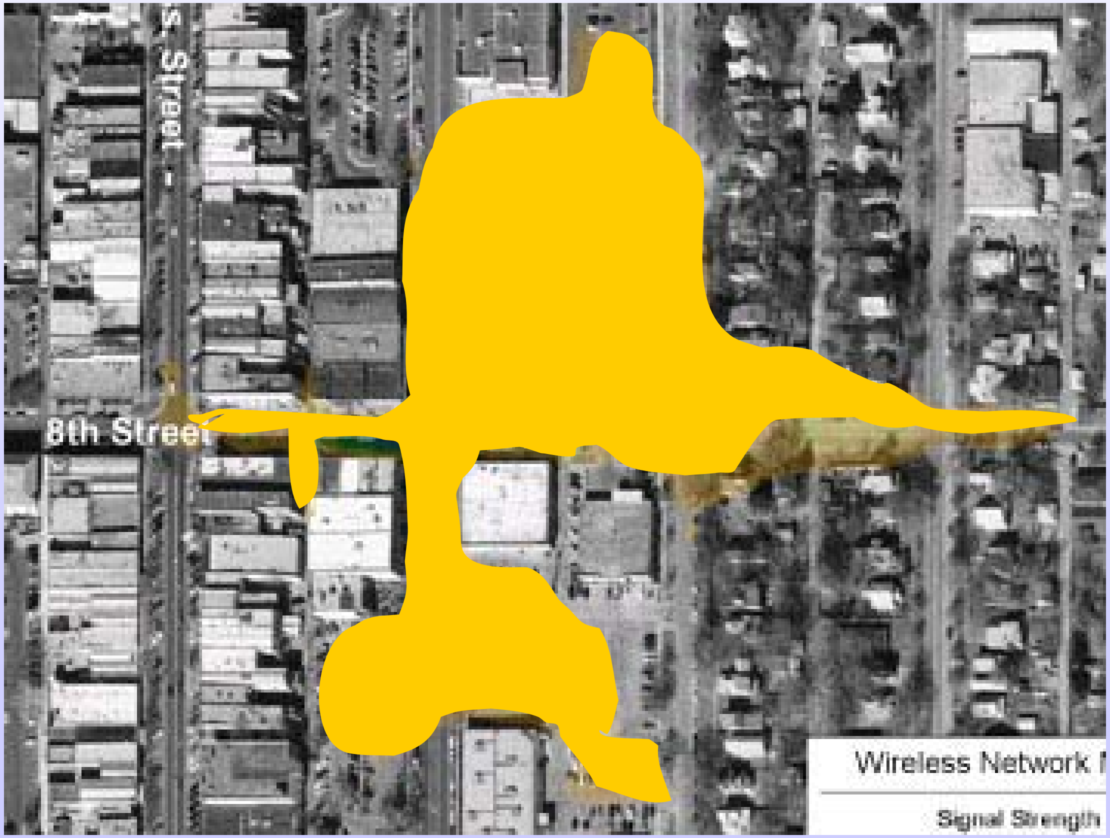
- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Cobertura

- ¿Dónde están nuestros usuarios?
- ¿Se puede medir y predecir la densidad de usuarios?
  - Limitar las zonas de servicio
- La cobertura en función del escenario
  - No molestar al vecino!
  - Cubrir los jardines en primavera!!
- ¿Qué necesidades tienen los usuarios?
  - Velocidad de acceso...
- ¿Existen otras redes wifi?
  - ¿Tenemos una normativa para el espacio radioeléctrico?

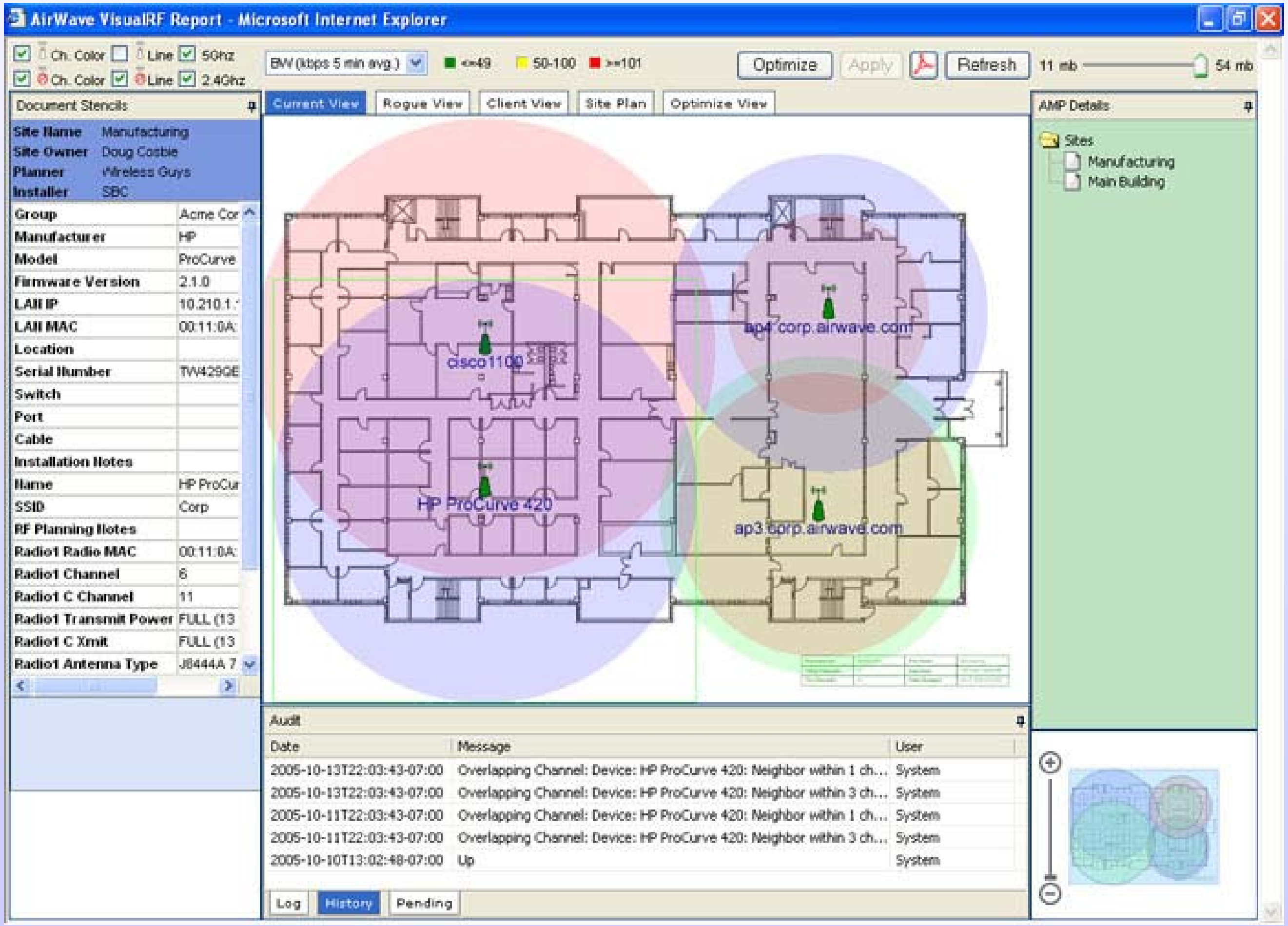
Cobertura

- Soluciones:
  - Planificadores de cobertura
  - Mediciones e inventarios de zona



Cobertura

- Planificadores de cobertura



Site Name	Manufacturing
Site Owner	Doug Cosbie
Planner	Wireless Guys
Installer	SBC

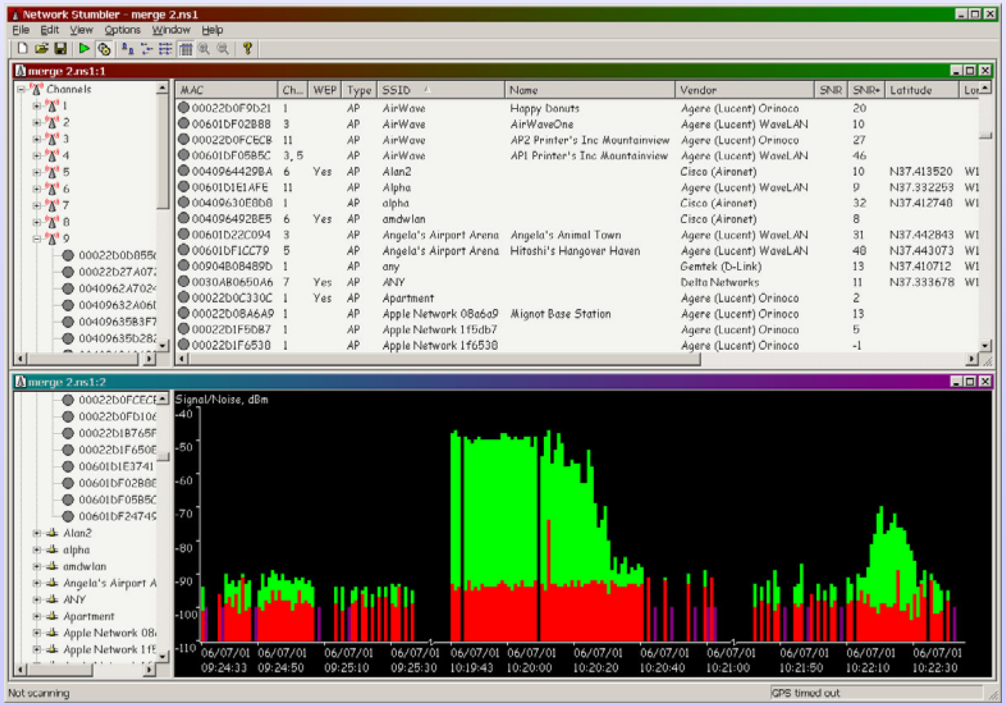
Group	Acme Cor
Manufacturer	HP
Model	ProCurve
Firmware Version	2.1.0
LAN IP	10.210.1.'
LAN MAC	00:11:0A:
Location	
Serial Number	TW429QE
Switch	
Port	
Cable	
Installation Notes	
Name	HP ProCur
SSID	Corp
RF Planning Notes	
Radio1 Radio MAC	00:11:0A:
Radio1 Channel	6
Radio1 C Channel	11
Radio1 Transmit Power	FULL (13
Radio1 C Xmit	FULL (13
Radio1 Antenna Type	J8444A 7

Audit

Date	Message	User
2005-10-13T22:03:43-07:00	Overlapping Channel: Device: HP ProCurve 420: Neighbor within 1 ch...	System
2005-10-13T22:03:43-07:00	Overlapping Channel: Device: HP ProCurve 420: Neighbor within 3 ch...	System
2005-10-11T22:03:43-07:00	Overlapping Channel: Device: HP ProCurve 420: Neighbor within 1 ch...	System
2005-10-11T22:03:43-07:00	Overlapping Channel: Device: HP ProCurve 420: Neighbor within 3 ch...	System
2005-10-10T13:02:48-07:00	Up	System

Cobertura

- Mediciones de campo
  - Distribución de canales para minimizar las interferencias (Carlos Turró UPV)
    - http://www.rediris.es/jt/jt2005/archivo/archivo-jt.es.html

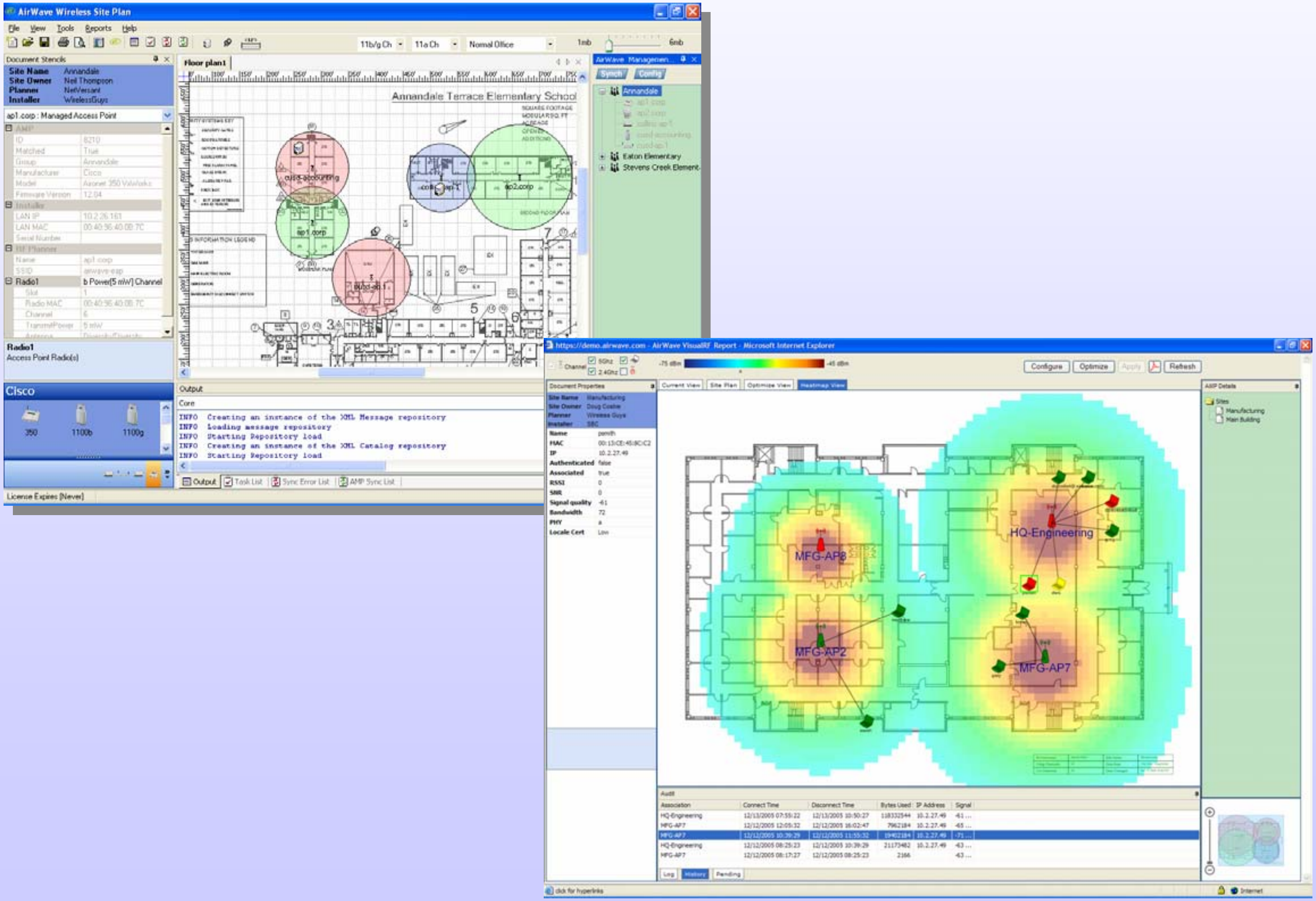


MAC	Ch...	WEP	Type	SSID	Name	Vendor	SNR	SNR+	Latitude	Lon
00022D0F9D21	1		AP	AirWave	Happy Donuts	Agere (Lucent) Orinoco		20		
00601DF02B88	3		AP	AirWave	AirWaveOne	Agere (Lucent) WaveLAN		10		
00022D0FCECB	11		AP	AirWave	AP2 Printer's Inc Mountainview	Agere (Lucent) Orinoco		27		
00601DF05B5C	3, 5		AP	AirWave	AP1 Printer's Inc Mountainview	Agere (Lucent) WaveLAN		46		
0040964429BA	6	Yes	AP	Alan2		Cisco (Aironet)		10	N37.413520	W1
00601D1E1AFE	11		AP	Alpha		Agere (Lucent) WaveLAN		9	N37.332253	W1
00409630E8D8	1		AP	alpha		Cisco (Aironet)		32	N37.412748	W1
004096492BE5	6	Yes	AP	amdwlan		Cisco (Aironet)		8		
00601D22C094	3		AP	Angela's Airport Arena	Angela's Animal Town	Agere (Lucent) WaveLAN		31	N37.442843	W1
00601DF1CC79	5		AP	Angela's Airport Arena	Hitoshi's Hangover Haven	Agere (Lucent) WaveLAN		48	N37.443073	W1
00904B08489D	1		AP	any		Gemtek (D-Link)		13	N37.410712	W1
0030AB0650A6	7	Yes	AP	ANY		Delta Networks		11	N37.333678	W1
00022D0C330C	1	Yes	AP	Apartment		Agere (Lucent) Orinoco		2		
00022D08A6A9	1		AP	Apple Network 08a6a9	Mignot Base Station	Agere (Lucent) Orinoco		13		
00022D1F5DB7	1		AP	Apple Network 1f5db7		Agere (Lucent) Orinoco		5		
00022D1F6538	1		AP	Apple Network 1f6538		Agere (Lucent) Orinoco		-1		

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Cobertura

- Herramientas de monitorización



Document Stencils

Site Name	Annandale
Site Owner	Neil Thompson
Planner	NetVersant
Installer	WirelessGuys

ap1.corp : Managed Access Point

AMP	
ID	8210
Matched	True
Group	Annandale
Manufacturer	Cisco
Model	Aironet 350 VxWorks
Firmware Version	12.04
Installer	
LAN IP	10.2.26.161
LAN MAC	00:40:96:40:08:7C
Serial Number	
RF Planner	
Name	ap1.corp
SSID	airwave-eap
Radio1	b Power[5 mW] Channel
Slot	1
Radio MAC	00:40:96:40:08:7C
Channel	6
TransmitPower	5 mW
Antenna	Diversity/Diversity

Radio1
Access Point Radio(s)

Output
Core

```
INFO  Creating an instance of the XML Message repository
INFO  Loading message repository
INFO  Starting Repository load
INFO  Creating an instance of the XML Catalog repository
INFO  Starting Repository load
```

Document Properties

Site Name	Manufacturing
Site Owner	Doug Coshe
Planner	Wireless Guys
Installer	SBC
Name	psmith
MAC	00:13:CE:45:8C:C2
IP	10.2.27.49
Authenticated	false
Associated	true
RSSI	0
SNR	0
Signal quality	-61
Bandwidth	72
PHY	a
Locale Cert	Low

Audit

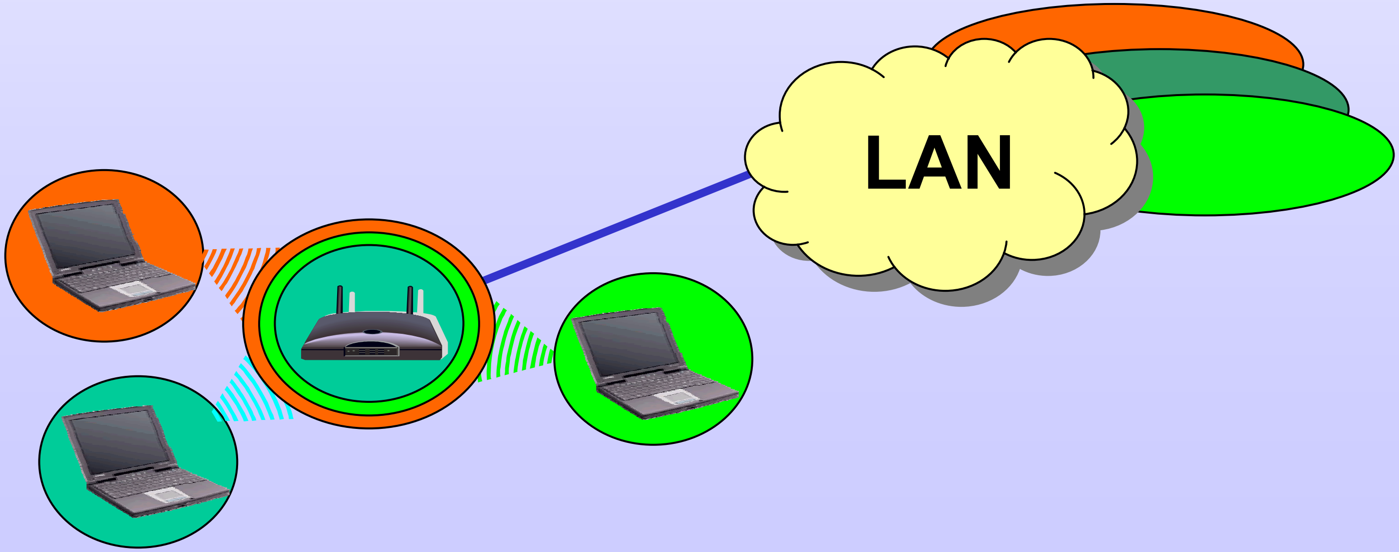
Association	Connect Time	Disconnect Time	Bytes Used	IP Address	Signal
HQ-Engineering	12/13/2005 07:55:22	12/13/2005 10:50:27	118332544	10.2.27.49	-61 ...
MFG-AP7	12/12/2005 12:05:32	12/12/2005 16:02:47	7962184	10.2.27.49	-65 ...
MFG-AP7	12/12/2005 10:39:29	12/12/2005 11:55:32	19402184	10.2.27.49	-71 ...
HQ-Engineering	12/12/2005 08:25:23	12/12/2005 10:39:29	21173482	10.2.27.49	-63 ...
MFG-AP7	12/12/2005 08:17:27	12/12/2005 08:25:23	2166		-63 ...

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

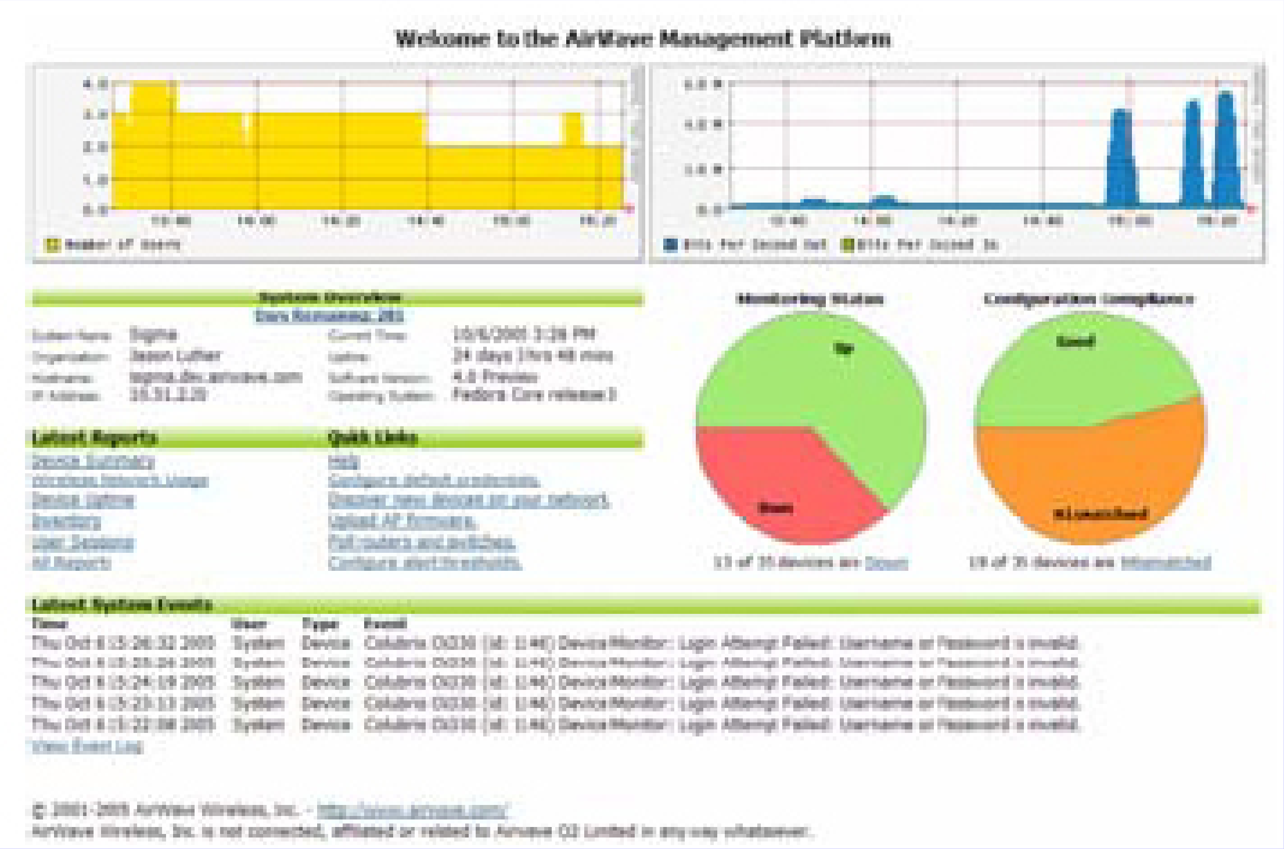
Arquitectura y gestión de red

- Puntos de acceso independientes
  - Recomendable dedicar una VLAN para la gestión
  - Segmentar mediante SSIDs-VLANs
  - Enrutamiento entre VLANs con ACLs
  - Gestión centralizada SNMP, SSH, HTTP,…
    - Como ejemplo: Airwave



Plataforma de gestión

- ¿Cómo está nuestra red wifi?



Welcome to the AirWave Management Platform

System Overview

Days Remaining: 281

System Name	Sigma	Current Time	10/6/2005 3:28 PM
Organization	Jason Luther	Uptime	24 days 1hrs 48 mins
Hostname	sigma.dev.airwave.com	Software Version	4.0 Preview
IP Address	10.51.2.20	Operating System	Fedora Core release 3

Latest Reports

Device Summary
Wireless Network Usage
Device Uptime
Inventory
User Sessions
All Reports

Quick Links

Help
Configure default credentials.
Discover new devices on your network.
Upload AP firmware.
Poll routers and switches.
Configure alert thresholds.

13 of 35 devices are Down

19 of 35 devices are Mismatched

Latest System Events

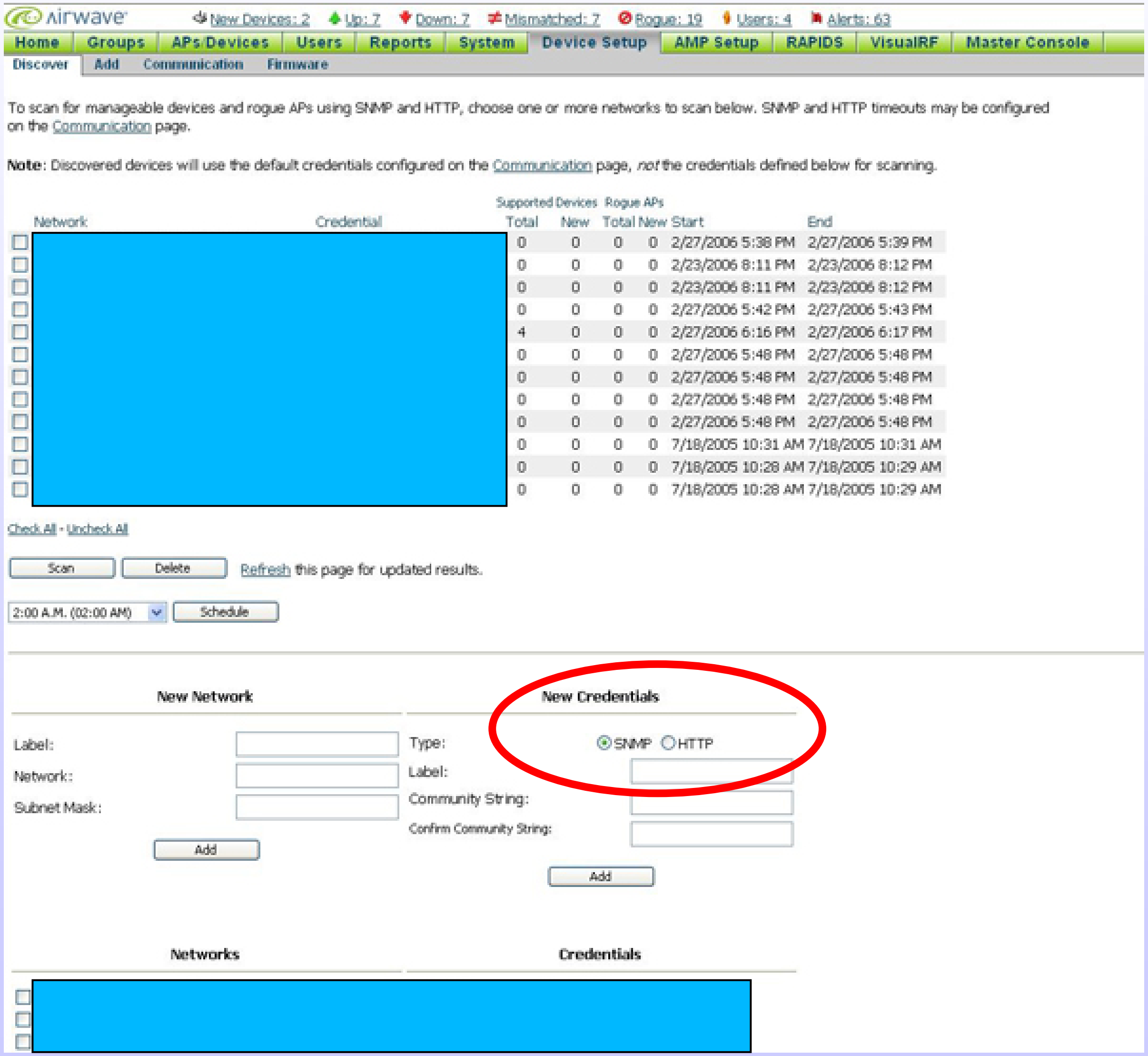
Time	User	Type	Event
Thu Oct 6 15:26:32 2005	System	Device	Colubris CN330 (id: 1146) Device Monitor: Login Attempt Failed: Username or Password is invalid.
Thu Oct 6 15:25:26 2005	System	Device	Colubris CN330 (id: 1146) Device Monitor: Login Attempt Failed: Username or Password is invalid.
Thu Oct 6 15:24:19 2005	System	Device	Colubris CN330 (id: 1146) Device Monitor: Login Attempt Failed: Username or Password is invalid.
Thu Oct 6 15:23:13 2005	System	Device	Colubris CN330 (id: 1146) Device Monitor: Login Attempt Failed: Username or Password is invalid.
Thu Oct 6 15:22:08 2005	System	Device	Colubris CN330 (id: 1146) Device Monitor: Login Attempt Failed: Username or Password is invalid.

View Event Log

© 2001-2005 AirWave Wireless, Inc. - http://www.airwave.com/
AirWave Wireless, Inc. is not connected, affiliated or related to Airwave O2 Limited in any way whatsoever.

Plataforma de gestión

- Descubrimiento de APs



To scan for manageable devices and rogue APs using SNMP and HTTP, choose one or more networks to scan below. SNMP and HTTP timeouts may be configured on the Communication page.

Note: Discovered devices will use the default credentials configured on the Communication page, *not* the credentials defined below for scanning.

			Supported Devices		Rogue APs			
	Network	Credential	Total	New	Total	New	Start	End
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:38 PM	2/27/2006 5:39 PM
□	[redacted]	[redacted]	0	0	0	0	2/23/2006 8:11 PM	2/23/2006 8:12 PM
□	[redacted]	[redacted]	0	0	0	0	2/23/2006 8:11 PM	2/23/2006 8:12 PM
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:42 PM	2/27/2006 5:43 PM
□	[redacted]	[redacted]	4	0	0	0	2/27/2006 6:16 PM	2/27/2006 6:17 PM
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:48 PM	2/27/2006 5:48 PM
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:48 PM	2/27/2006 5:48 PM
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:48 PM	2/27/2006 5:48 PM
□	[redacted]	[redacted]	0	0	0	0	2/27/2006 5:48 PM	2/27/2006 5:48 PM
□	[redacted]	[redacted]	0	0	0	0	7/18/2005 10:31 AM	7/18/2005 10:31 AM
□	[redacted]	[redacted]	0	0	0	0	7/18/2005 10:28 AM	7/18/2005 10:29 AM
□	[redacted]	[redacted]	0	0	0	0	7/18/2005 10:28 AM	7/18/2005 10:29 AM

Check All - Uncheck All

Refresh this page for updated results.

2:00 A.M. (02:00 AM)

New Network

Label:

Network:

Subnet Mask:

New Credentials

Type: ● SNMP ○ HTTP

Label:

Community String:

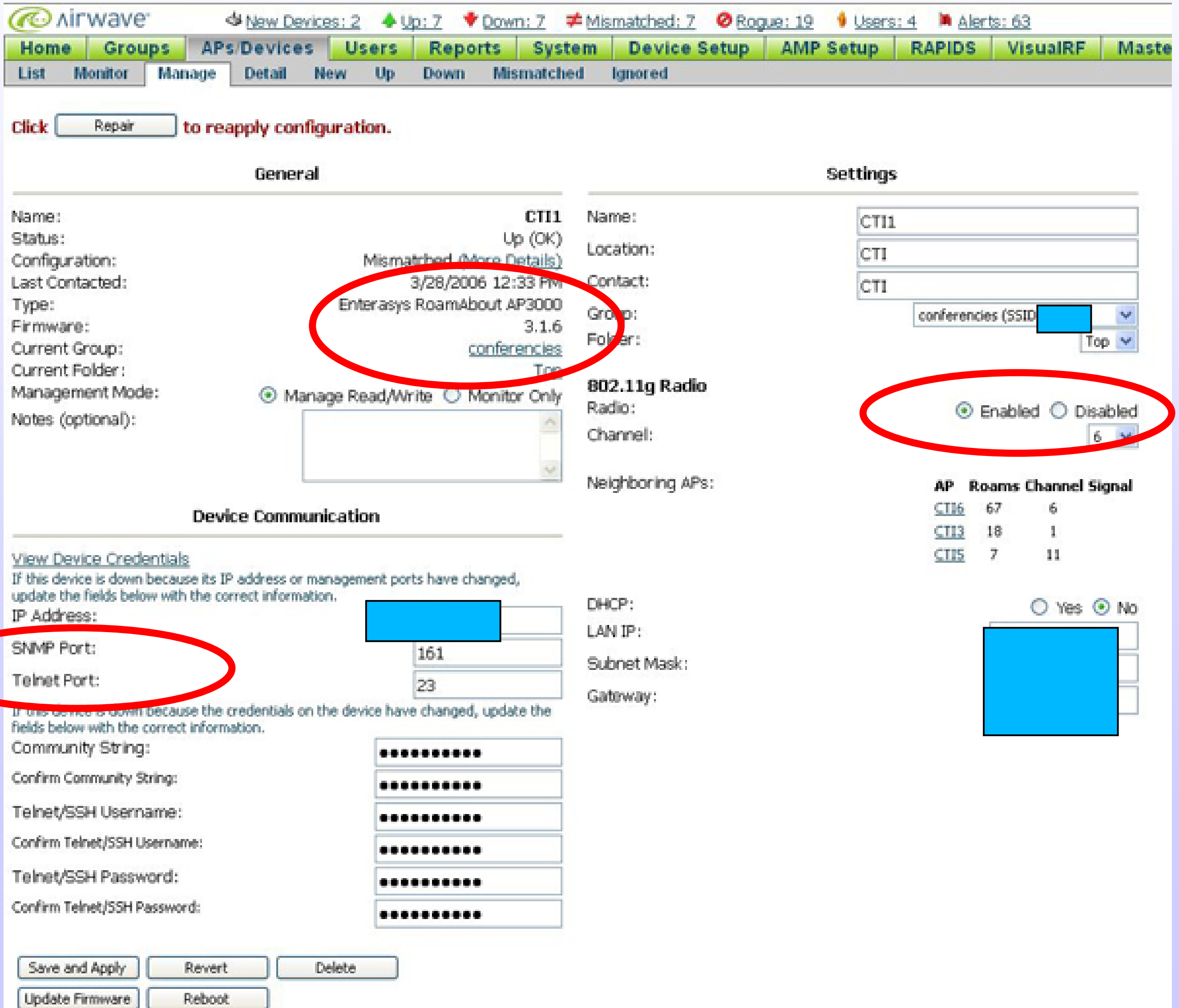
Confirm Community String:

Networks **Credentials**

□ [redacted]
□
□

Plataforma de gestión

- Configuración de un AP



airwave
New Devices: 2 | Up: 7 | Down: 7 | Mismatched: 7 | Rogue: 19 | Users: 4 | Alerts: 63
Home | Groups | APs/Devices | Users | Reports | System | Device Setup | AMP Setup | RAPIDS | VisualRF | Maste
List | Monitor | Manage | Detail | New | Up | Down | Mismatched | Ignored

Click [Repair] to reapply configuration.

General

Name:	CTI1
Status:	Up (OK)
Configuration:	Mismatched (More Details)
Last Contacted:	3/28/2006 12:33 PM
Type:	Enterasys RoamAbout AP3000
Firmware:	3.1.6
Current Group:	conferencies
Current Folder:	Top
Management Mode:	● Manage Read/Write ○ Monitor Only
Notes (optional):	

Settings

Name:	CTI1
Location:	CTI
Contact:	CTI
Group:	conferencies (SSID [redacted]
Folder:	Top

802.11g Radio

Radio:	● Enabled ○ Disabled
Channel:	6

Neighboring APs:

AP	Roams	Channel	Signal
CTI6	67	6	
CTI3	18	1	
CTI5	7	11	

Device Communication

View Device Credentials

If this device is down because its IP address or management ports have changed, update the fields below with the correct information.

IP Address:	[redacted]
SNMP Port:	161
Telnet Port:	23

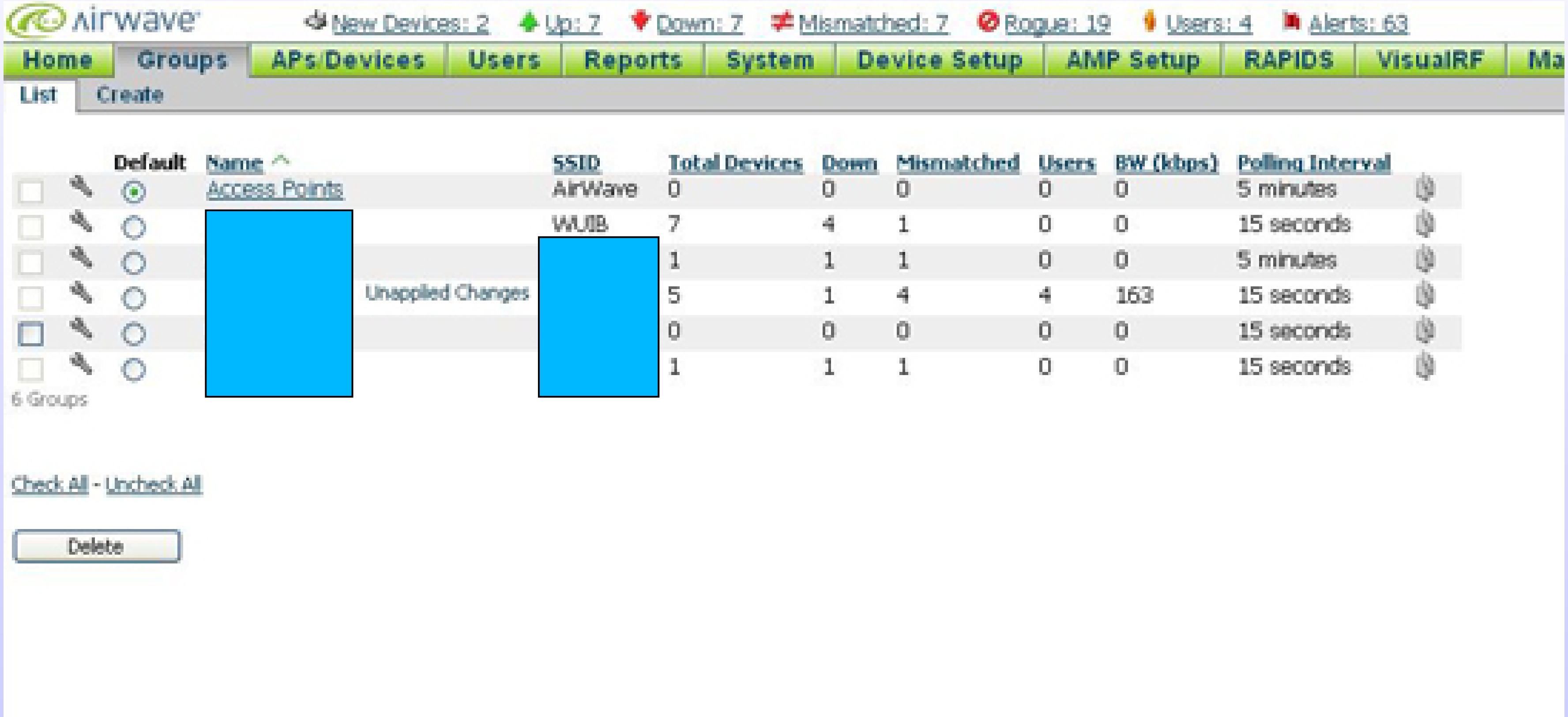
If this device is down because the credentials on the device have changed, update the fields below with the correct information.

Community String:	●●●●●●●●●●●
Confirm Community String:	●●●●●●●●●●●
Telnet/SSH Username:	●●●●●●●●●●●
Confirm Telnet/SSH Username:	●●●●●●●●●●●
Telnet/SSH Password:	●●●●●●●●●●●
Confirm Telnet/SSH Password:	●●●●●●●●●●●

DHCP:	○ Yes ● No
LAN IP:	[redacted]
Subnet Mask:	
Gateway:	

Plataforma de gestión

- Grupos de APs



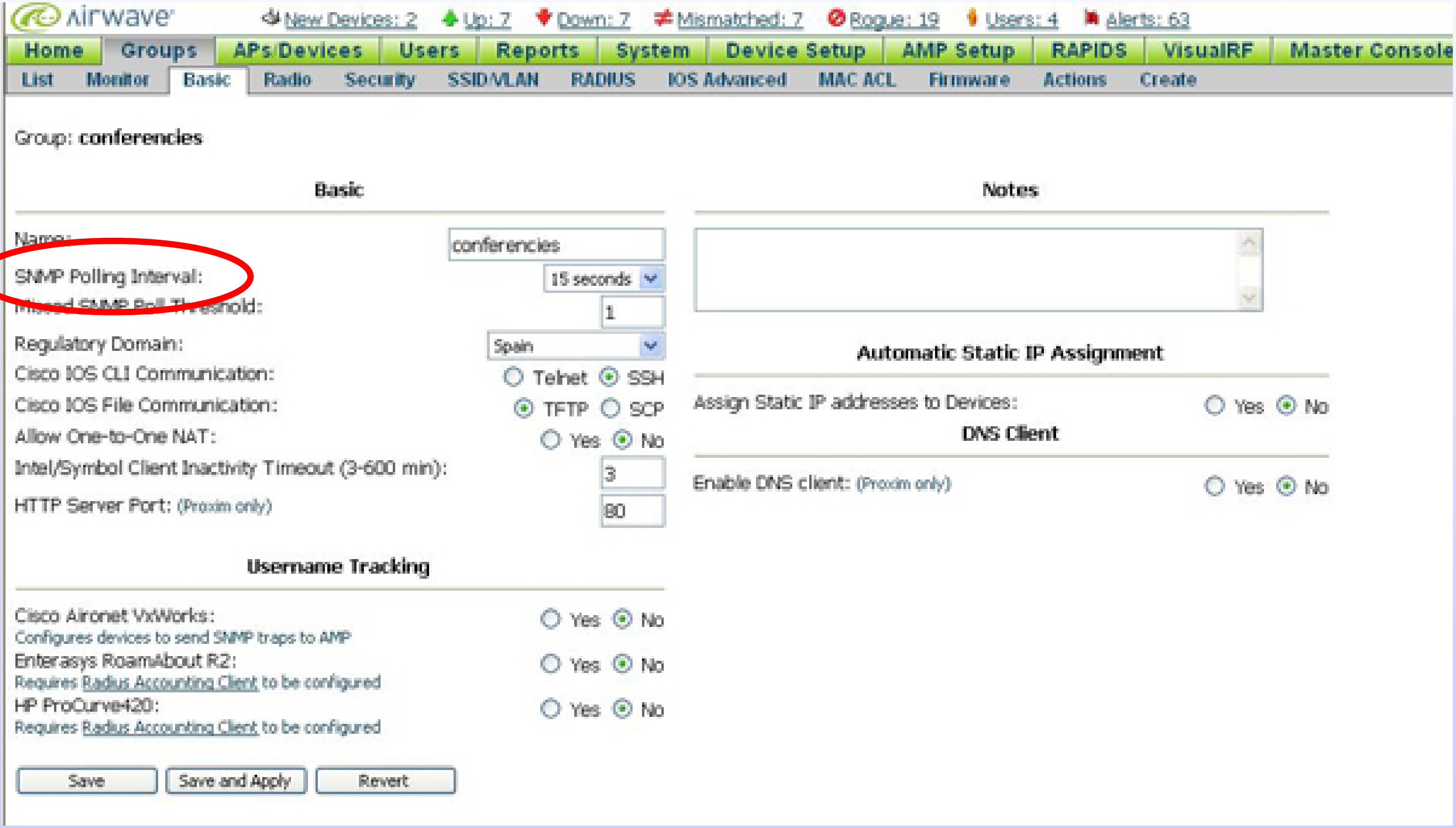
		Default	Name ^		SSID	Total Devices	Down	Mismatched	Users	BW (kbps)	Polling Interval	
□		●	Access Points		AirWave	0	0	0	0	0	5 minutes	
□		○	[redacted]		WUIB	7	4	1	0	0	15 seconds	
□		○	[redacted]		[redacted]	1	1	1	0	0	5 minutes	
□		○	[redacted]	Unapplied Changes	[redacted]	5	1	4	4	163	15 seconds	
□		○	[redacted]		[redacted]	0	0	0	0	0	15 seconds	
□		○	[redacted]		[redacted]	1	1	1	0	0	15 seconds	

6 Groups

Check All - Uncheck All

Plataforma de gestión

- Configuración de un grupo: Basic



Group: **conferencies**

Basic

Name: conferencies

SNMP Polling Interval: 15 seconds

Missed SNMP Poll Threshold: 1

Regulatory Domain: Spain

Cisco IOS CLI Communication: ○ Telnet ● SSH

Cisco IOS File Communication: ● TFTP ○ SCP

Allow One-to-One NAT: ○ Yes ● No

Intel/Symbol Client Inactivity Timeout (3-600 min): 3

HTTP Server Port: (Proxim only) 80

Username Tracking

Cisco Aironet VxWorks: ○ Yes ● No
Configures devices to send SNMP traps to AMP

Enterasys RoamAbout R2: ○ Yes ● No
Requires Radius Accounting Client to be configured

HP ProCurve420: ○ Yes ● No
Requires Radius Accounting Client to be configured

Notes

Automatic Static IP Assignment

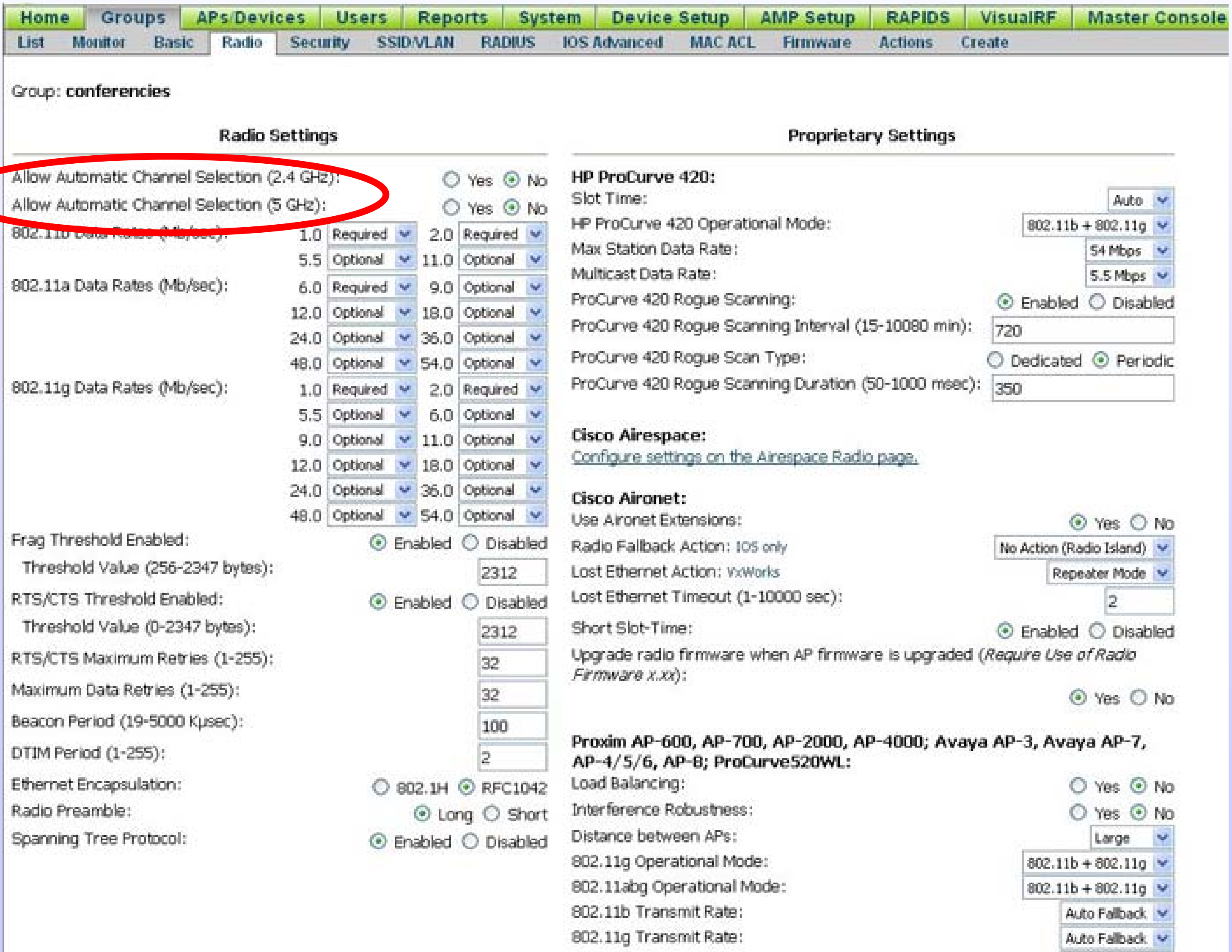
Assign Static IP addresses to Devices: ○ Yes ● No

DNS Client

Enable DNS client: (Proxim only) ○ Yes ● No

Plataforma de gestión

- Configuración de un grupo: Radio


Home | Groups | APs/Devices | Users | Reports | System | Device Setup | AMP Setup | RAPIDS | VisualRF | Master Console
List | Monitor | Basic | Radio | Security | SSID/VLAN | RADIUS | IOS Advanced | MAC ACL | Firmware | Actions | Create

Group: **conferencies**

Radio Settings

Allow Automatic Channel Selection (2.4 GHz): ○ Yes ● No
Allow Automatic Channel Selection (5 GHz): ○ Yes ● No
802.11b Data Rates (Mb/sec): 1.0 Required, 2.0 Required, 5.5 Optional, 11.0 Optional
802.11a Data Rates (Mb/sec): 6.0 Required, 9.0 Optional, 12.0 Optional, 18.0 Optional, 24.0 Optional, 36.0 Optional, 48.0 Optional, 54.0 Optional
802.11g Data Rates (Mb/sec): 1.0 Required, 2.0 Required, 5.5 Optional, 6.0 Optional, 9.0 Optional, 11.0 Optional, 12.0 Optional, 18.0 Optional, 24.0 Optional, 36.0 Optional, 48.0 Optional, 54.0 Optional
Frag Threshold Enabled: ● Enabled ○ Disabled
Threshold Value (256-2347 bytes): 2312
RTS/CTS Threshold Enabled: ● Enabled ○ Disabled
Threshold Value (0-2347 bytes): 2312
RTS/CTS Maximum Retries (1-255): 32
Maximum Data Retries (1-255): 32
Beacon Period (19-5000 Kμsec): 100
DTIM Period (1-255): 2
Ethernet Encapsulation: ○ 802.1H ● RFC1042
Radio Preamble: ● Long ○ Short
Spanning Tree Protocol: ● Enabled ○ Disabled

Proprietary Settings

HP ProCurve 420:
Slot Time: Auto
HP ProCurve 420 Operational Mode: 802.11b + 802.11g
Max Station Data Rate: 54 Mbps
Multicast Data Rate: 5.5 Mbps
ProCurve 420 Rogue Scanning: ● Enabled ○ Disabled
ProCurve 420 Rogue Scanning Interval (15-10080 min): 720
ProCurve 420 Rogue Scan Type: ○ Dedicated ● Periodic
ProCurve 420 Rogue Scanning Duration (50-1000 msec): 350

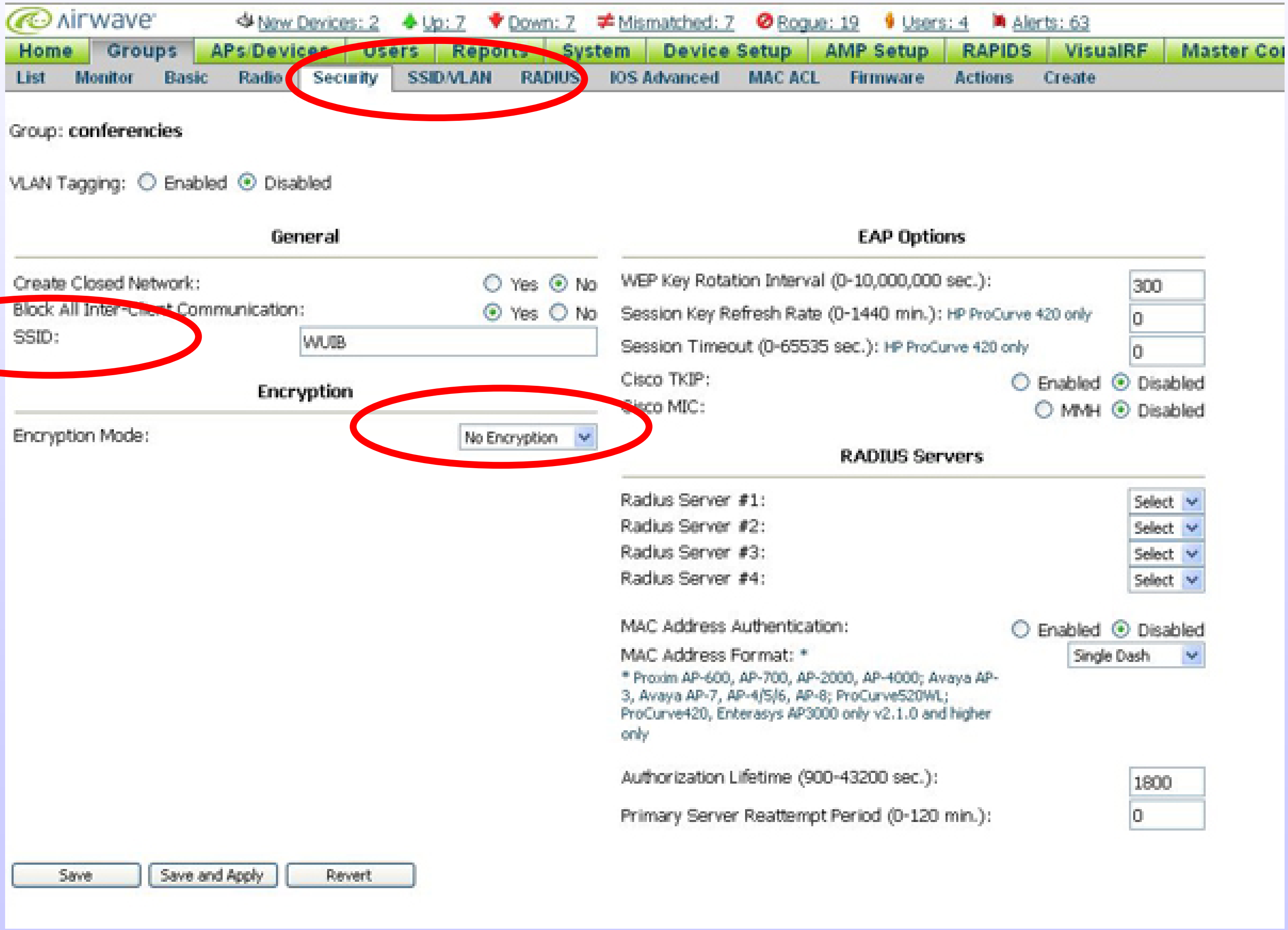
Cisco Airespace:
Configure settings on the Airespace Radio page.

Cisco Aironet:
Use Aironet Extensions: ● Yes ○ No
Radio Fallback Action: IOS only — No Action (Radio Island)
Lost Ethernet Action: VxWorks — Repeater Mode
Lost Ethernet Timeout (1-10000 sec): 2
Short Slot-Time: ● Enabled ○ Disabled
Upgrade radio firmware when AP firmware is upgraded (*Require Use of Radio Firmware x.xx*): ● Yes ○ No

Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL:
Load Balancing: ○ Yes ● No
Interference Robustness: ○ Yes ● No
Distance between APs: Large
802.11g Operational Mode: 802.11b + 802.11g
802.11abg Operational Mode: 802.11b + 802.11g
802.11b Transmit Rate: Auto Fallback
802.11g Transmit Rate: Auto Fallback

Plataforma de gestión

- Parámetros de seguridad del grupo



Group: **conferencies**

VLAN Tagging: ○ Enabled ● Disabled

General

Create Closed Network: ○ Yes ● No

Block All Inter-Client Communication: ● Yes ○ No

SSID: WUIB

Encryption

Encryption Mode: No Encryption

EAP Options

WEP Key Rotation Interval (0-10,000,000 sec.): 300

Session Key Refresh Rate (0-1440 min.): HP ProCurve 420 only 0

Session Timeout (0-65535 sec.): HP ProCurve 420 only 0

Cisco TKIP: ○ Enabled ● Disabled

Cisco MIC: ○ MMH ● Disabled

RADIUS Servers

Radius Server #1: Select

Radius Server #2: Select

Radius Server #3: Select

Radius Server #4: Select

MAC Address Authentication: ○ Enabled ● Disabled

MAC Address Format: * Single Dash

* Proxim AP-600, AP-700, AP-2000, AP-4000; Avaya AP-3, Avaya AP-7, AP-4/5/6, AP-8; ProCurve520WL; ProCurve420, Enterasys AP3000 only v2.1.0 and higher only

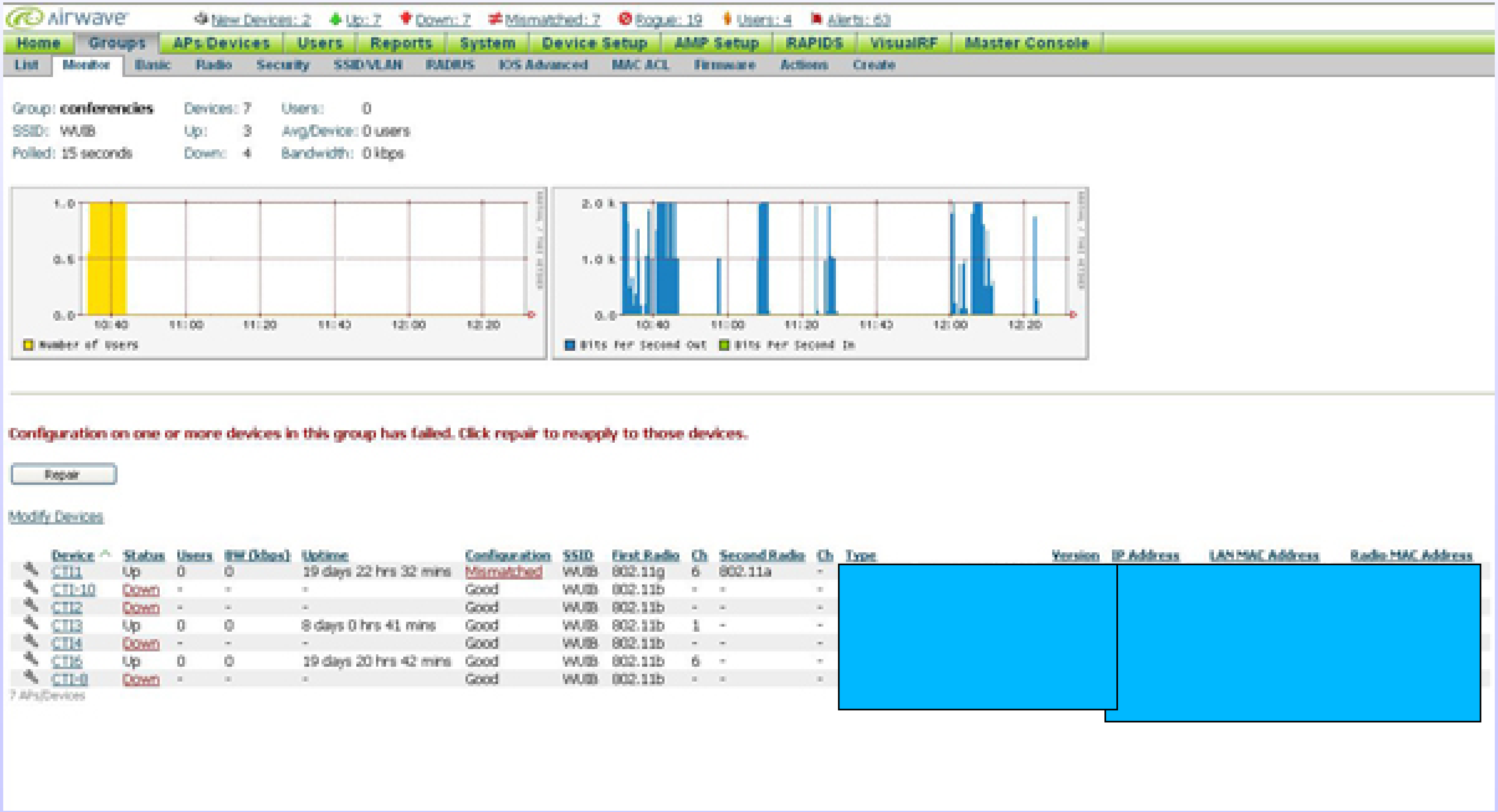
Authorization Lifetime (900-43200 sec.): 1800

Primary Server Reattempt Period (0-120 min.): 0

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Plataforma de gestión

- Monitorizando un grupo



Group: **conferencies**	Devices: 7	Users: 0
SSID: WUIB	Up: 3	Avg/Device: 0 users
Polled: 15 seconds	Down: 4	Bandwidth: 0 kbps

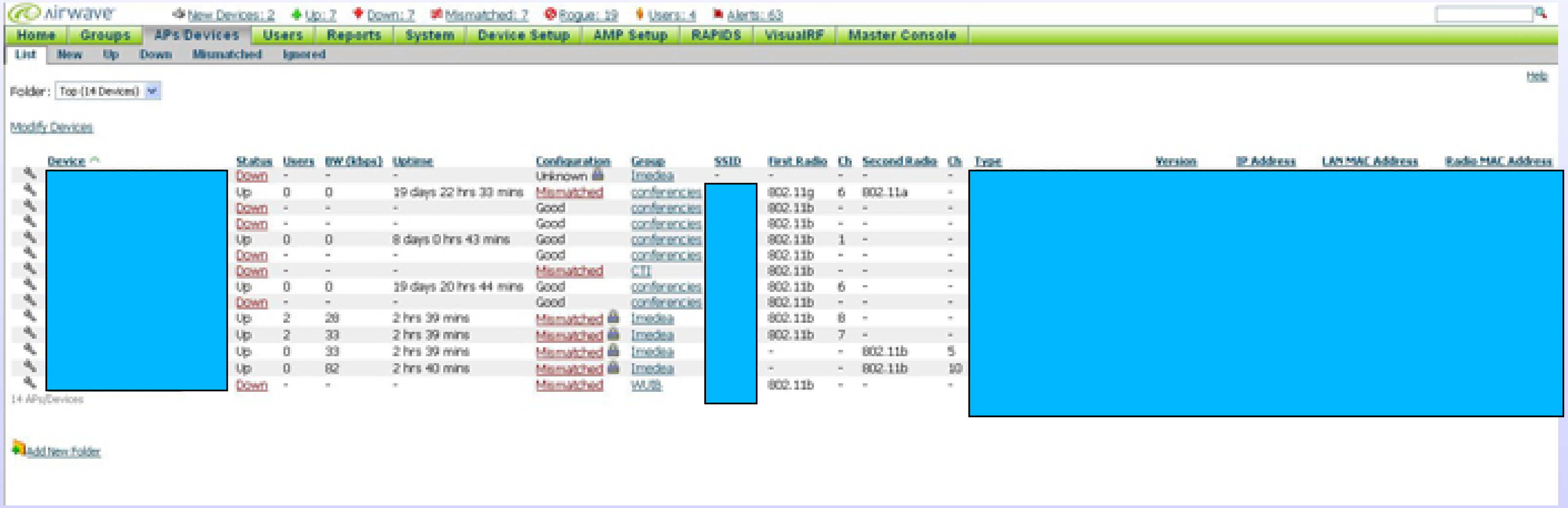
Configuration on one or more devices in this group has failed. Click repair to reapply to those devices.

Device	Status	Users	BW (kbps)	Uptime	Configuration	SSID	First Radio	Ch	Second Radio	Ch	Type	Version	IP Address	LAN MAC Address	Radio MAC Address
CTI1	Up	0	0	19 days 22 hrs 32 mins	Mismatched	WUIB	802.11g	6	802.11a	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI-10	Down	-	-	-	Good	WUIB	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI2	Down	-	-	-	Good	WUIB	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI3	Up	0	0	8 days 0 hrs 41 mins	Good	WUIB	802.11b	1	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI4	Down	-	-	-	Good	WUIB	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI6	Up	0	0	19 days 20 hrs 42 mins	Good	WUIB	802.11b	6	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
CTI-8	Down	-	-	-	Good	WUIB	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

7 APs/Devices

Plataforma de gestión

- Listado de APs: Verificando su configuración!!
  - Asignación de grupos según las necesidades

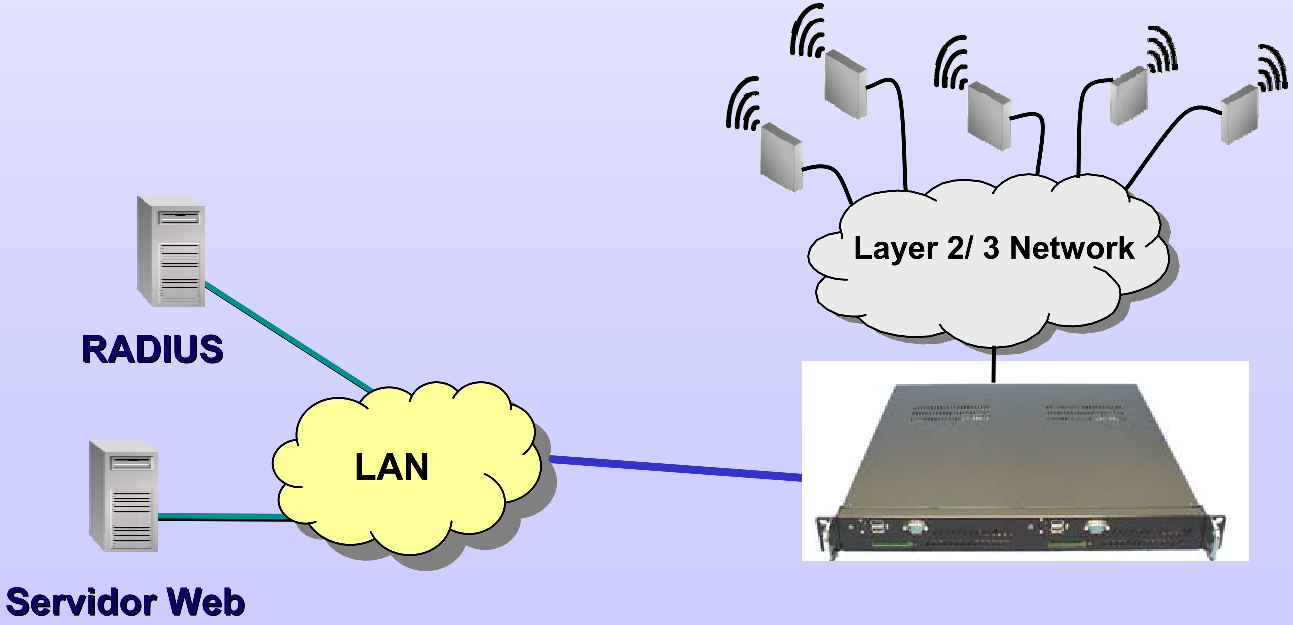


Device	Status	Users	BW (kbps)	Uptime	Configuration	Group	SSID	First Radio	Ch	Second Radio	Ch	Type	Version	IP Address	LAN MAC Address	Radio MAC Address
[redacted]	Down	-	-	-	Unknown 🔒	Imedea	-	-	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	0	0	19 days 22 hrs 33 mins	Mismatched	conferencies	[redacted]	802.11g	6	802.11a	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Good	conferencies	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Good	conferencies	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	0	0	8 days 0 hrs 43 mins	Good	conferencies	[redacted]	802.11b	1	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Good	conferencies	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Mismatched	CTI	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	0	0	19 days 20 hrs 44 mins	Good	conferencies	[redacted]	802.11b	6	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Good	conferencies	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	2	28	2 hrs 39 mins	Mismatched 🔒	Imedea	[redacted]	802.11b	8	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	2	33	2 hrs 39 mins	Mismatched 🔒	Imedea	[redacted]	802.11b	7	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	0	33	2 hrs 39 mins	Mismatched 🔒	Imedea	[redacted]	-	-	802.11b	5	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Up	0	82	2 hrs 40 mins	Mismatched 🔒	Imedea	[redacted]	-	-	802.11b	10	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	Down	-	-	-	Mismatched	WLIB	[redacted]	802.11b	-	-	-	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

14 APs/Devices

Arquitectura y gestión de red

- Controlador de puntos de accesos
  - Nivel: Físico, VLAN, IP
  - Automatización: Configuración, asignación de canales, balanceo de carga, etc…
  - <u>Soporte para productos de otros fabricantes???</u>

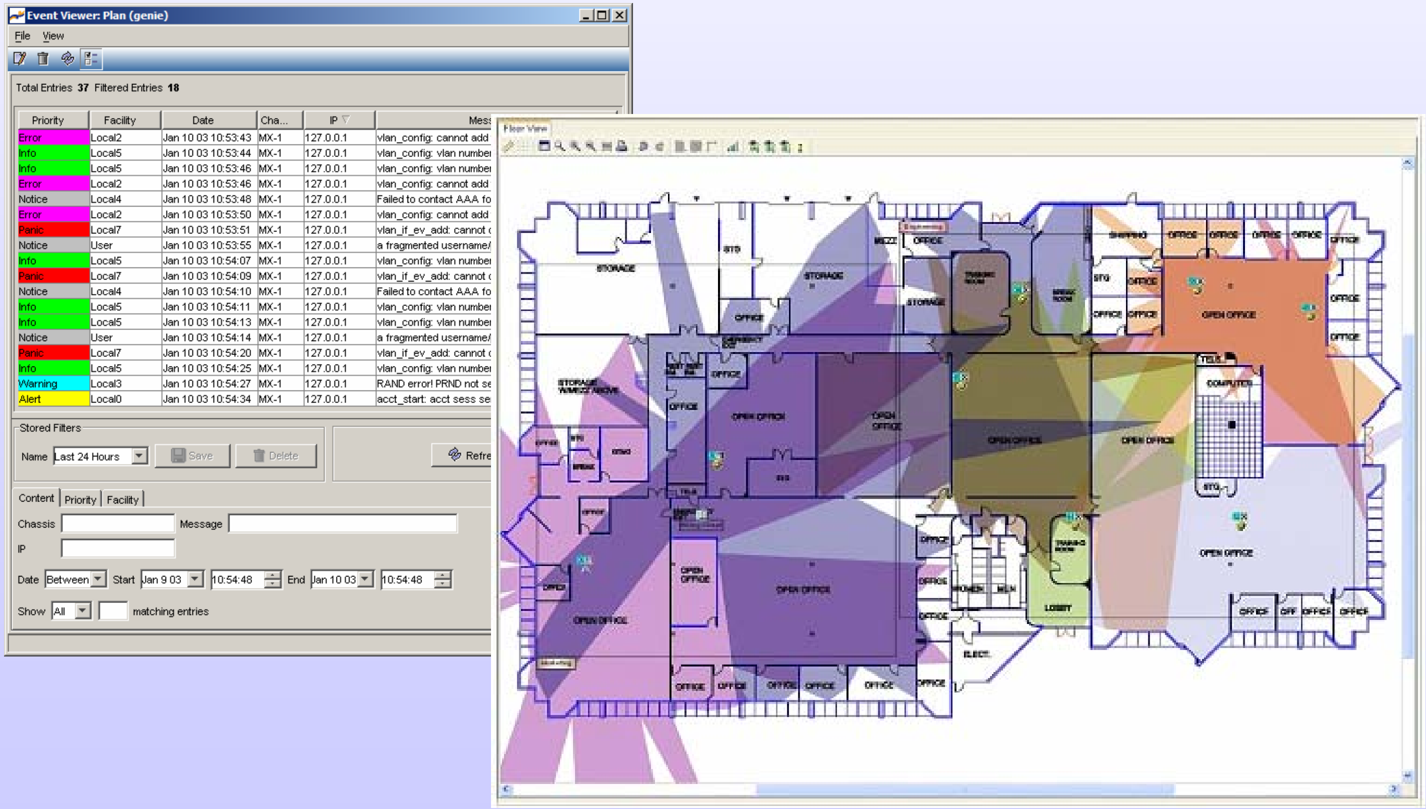


Controlador de APs

- Producto
  - Configuración Plug&Play
    - Indicando el número de serie y MAC...
    - Soporte para otros fabricantes...
  - Gestión centralizada (= Airwave)
  - Funcionalidades muy integradas
    - Al ser todo un mismo producto!!!
  - APs económicos!!!

Controlador de APs

- Funcionalidades integradas:
  - Alarmas, Coberturas, Localización de usuarios,...



Total Entries **37** Filtered Entries **18**

Priority	Facility	Date	Cha...	IP	Mess
Error	Local2	Jan 10 03 10:53:43	MX-1	127.0.0.1	vlan_config: cannot add
Info	Local5	Jan 10 03 10:53:44	MX-1	127.0.0.1	vlan_config: vlan number
Info	Local5	Jan 10 03 10:53:46	MX-1	127.0.0.1	vlan_config: vlan number
Error	Local2	Jan 10 03 10:53:46	MX-1	127.0.0.1	vlan_config: cannot add
Notice	Local4	Jan 10 03 10:53:48	MX-1	127.0.0.1	Failed to contact AAA fo
Error	Local2	Jan 10 03 10:53:50	MX-1	127.0.0.1	vlan_config: cannot add
Panic	Local7	Jan 10 03 10:53:51	MX-1	127.0.0.1	vlan_if_ev_add: cannot
Notice	User	Jan 10 03 10:53:55	MX-1	127.0.0.1	a fragmented username/
Info	Local5	Jan 10 03 10:54:07	MX-1	127.0.0.1	vlan_config: vlan number
Panic	Local7	Jan 10 03 10:54:09	MX-1	127.0.0.1	vlan_if_ev_add: cannot
Notice	Local4	Jan 10 03 10:54:10	MX-1	127.0.0.1	Failed to contact AAA fo
Info	Local5	Jan 10 03 10:54:11	MX-1	127.0.0.1	vlan_config: vlan number
Info	Local5	Jan 10 03 10:54:13	MX-1	127.0.0.1	vlan_config: vlan number
Notice	User	Jan 10 03 10:54:14	MX-1	127.0.0.1	a fragmented username/
Panic	Local7	Jan 10 03 10:54:20	MX-1	127.0.0.1	vlan_if_ev_add: cannot
Info	Local5	Jan 10 03 10:54:25	MX-1	127.0.0.1	vlan_config: vlan number
Warning	Local3	Jan 10 03 10:54:27	MX-1	127.0.0.1	RAND error! PRND not se
Alert	Local0	Jan 10 03 10:54:34	MX-1	127.0.0.1	acct_start: acct sess se

Stored Filters

Name: Last 24 Hours ▾ Save Delete Refre

Content | Priority | Facility

Chassis: Message:

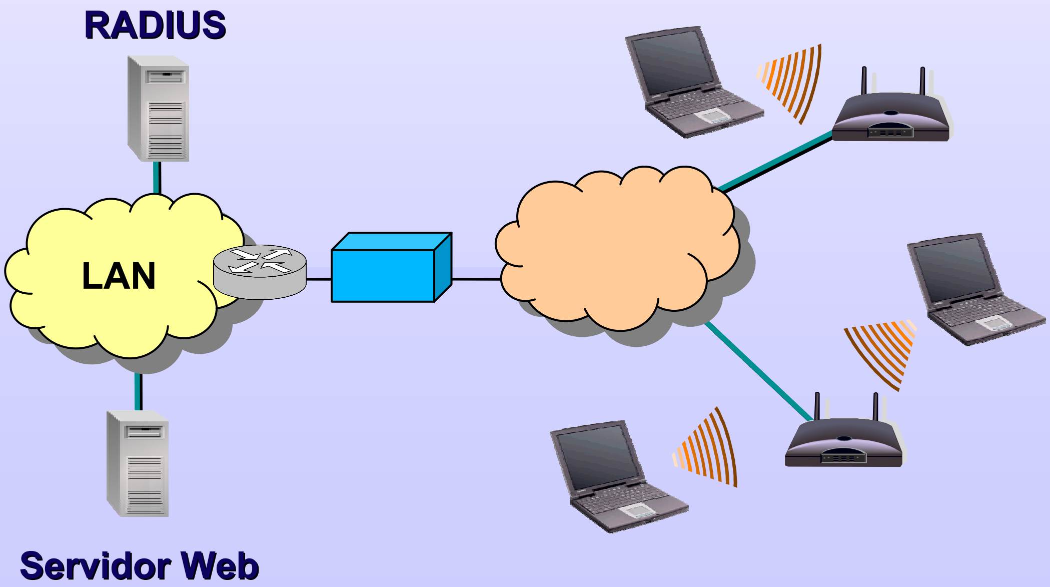
IP:

Date: Between ▾ Start: Jan 9 03 ▾ 10:54:48 End: Jan 10 03 ▾ 10:54:48

Show: All ▾ matching entries

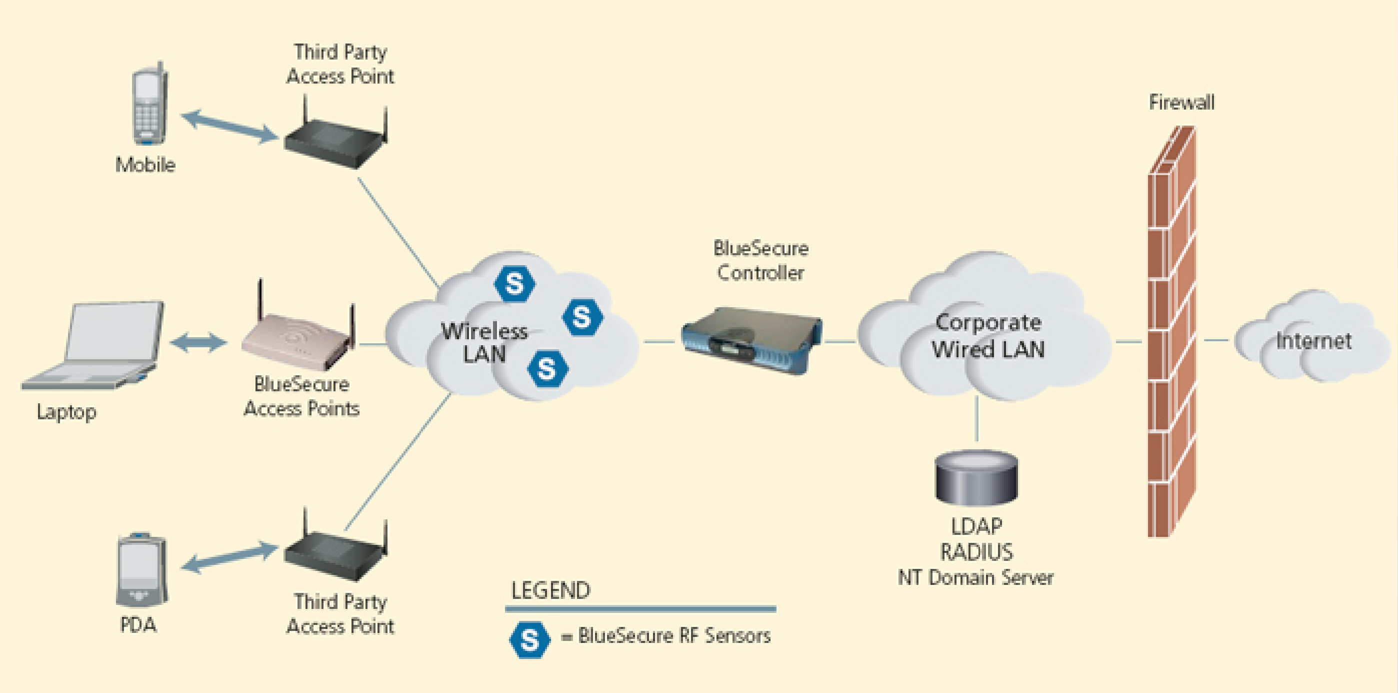
Arquitectura y gestión de red

- La caja negra...
  - Pueden controlar APs
  - Servicios: DHCP, 802.1x, VPN, Portal-Web, LDAP-Radius interno, etc...
  - IDS-IDP y Control de admisión



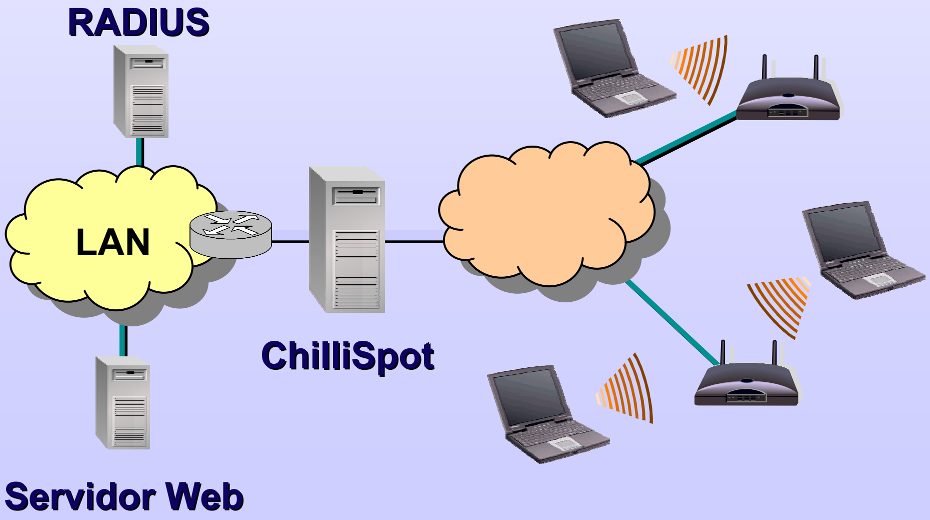
Bluesocket

- Así lo presenta la empresa...
  - Características mas adelante...



Wireless Gateway: CHILLISPOT

- www.chillispot.org
  - OpenSource



Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Cifrado

- WEP
  - RC4 y el vector de inicialización en claro … problemas!!
- WEP+
  - Evitando vectores de inicialización débiles
- WPA
  - Upgrade software de los productos WEP→ RC4
  - Claves TKIP: PSK (secreto), PMK(master), PTK (temporal), PGK (grupo),…
  - Anti-replay
- WPA2
  - Upgrade hardware para soportar AES

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Control de acceso

- Características propias
  - MAC, VLAN, …
- Secreto compartido
  - WEP, WPA-PSK, Kerberos, …
- Token en posesión
  - Certificado digital, tarjeta inteligente, e-token USB, …
- Biometría

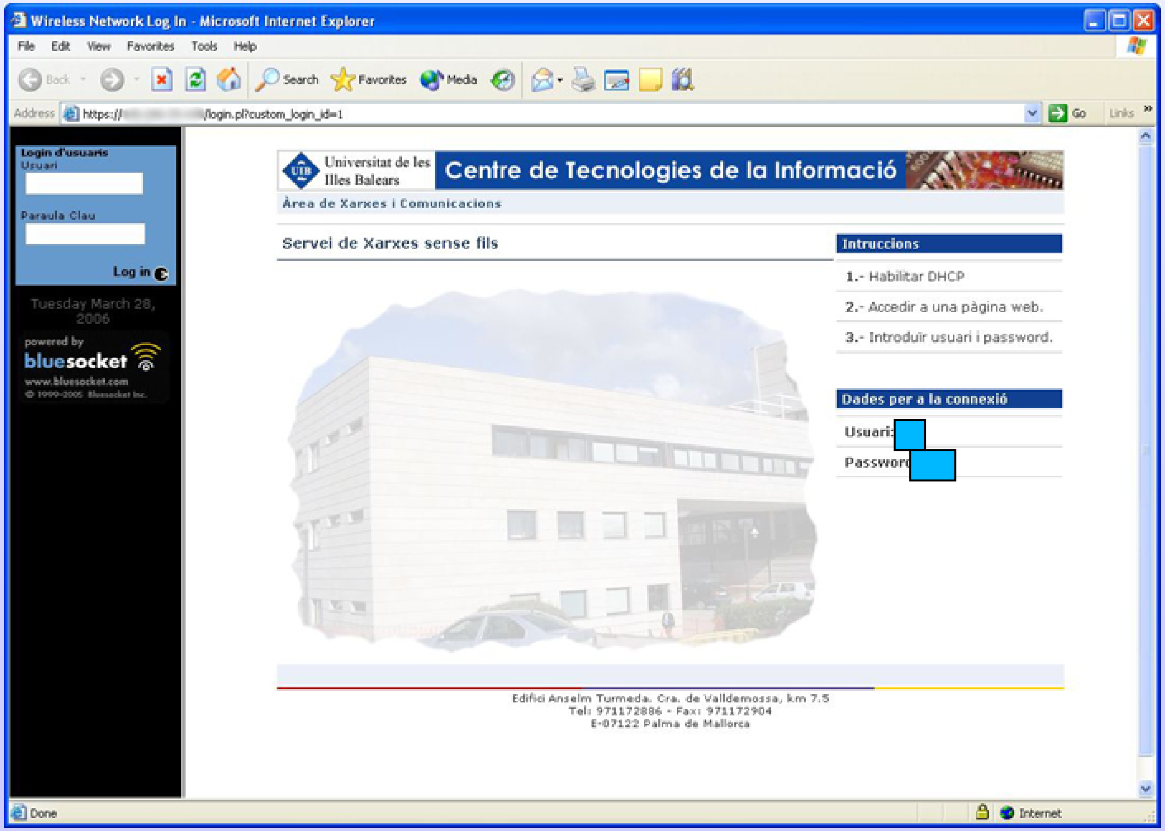
IV Foro de Seguridad de RedIRIS

Diseño, implantación y securización de redes wifi

UIB Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Control de acceso

- Portal web
  - Web que se ofrece al usuario para realizar la autenticación
  - Previa petición de una url...



https://[redacted]/login.pl?custom_login_id=1

Login d'usuaris
Usuari
Paraula Clau
Log in

Tuesday March 28, 2006

powered by bluesocket
www.bluesocket.com
© 1999-2005 Bluesocket Inc.

Universitat de les Illes Balears
Centre de Tecnologies de la Informació
Àrea de Xarxes i Comunicacions

Servei de Xarxes sense fils

Intruccions

1.- Habilitar DHCP
2.- Accedir a una pàgina web.
3.- Introduïr usuari i password.

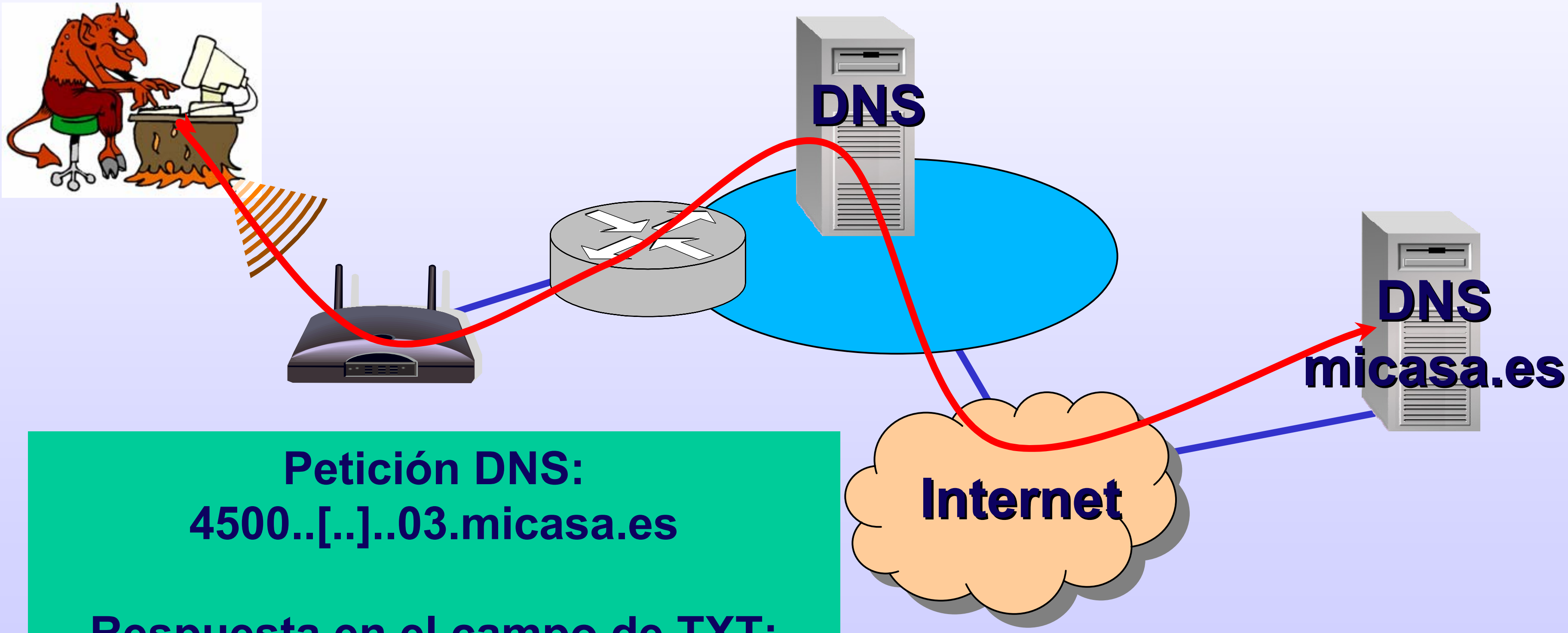
Dades per a la connexió

Usuari: [redacted]
Passwor[redacted]

Edifici Anselm Turmeda. Cra. de Valldemossa, km 7.5
Tel: 971172886 - Fax: 971172904
E-07122 Palma de Mallorca

DNS-Tunneling

- OJO!! DNS-Tunneling



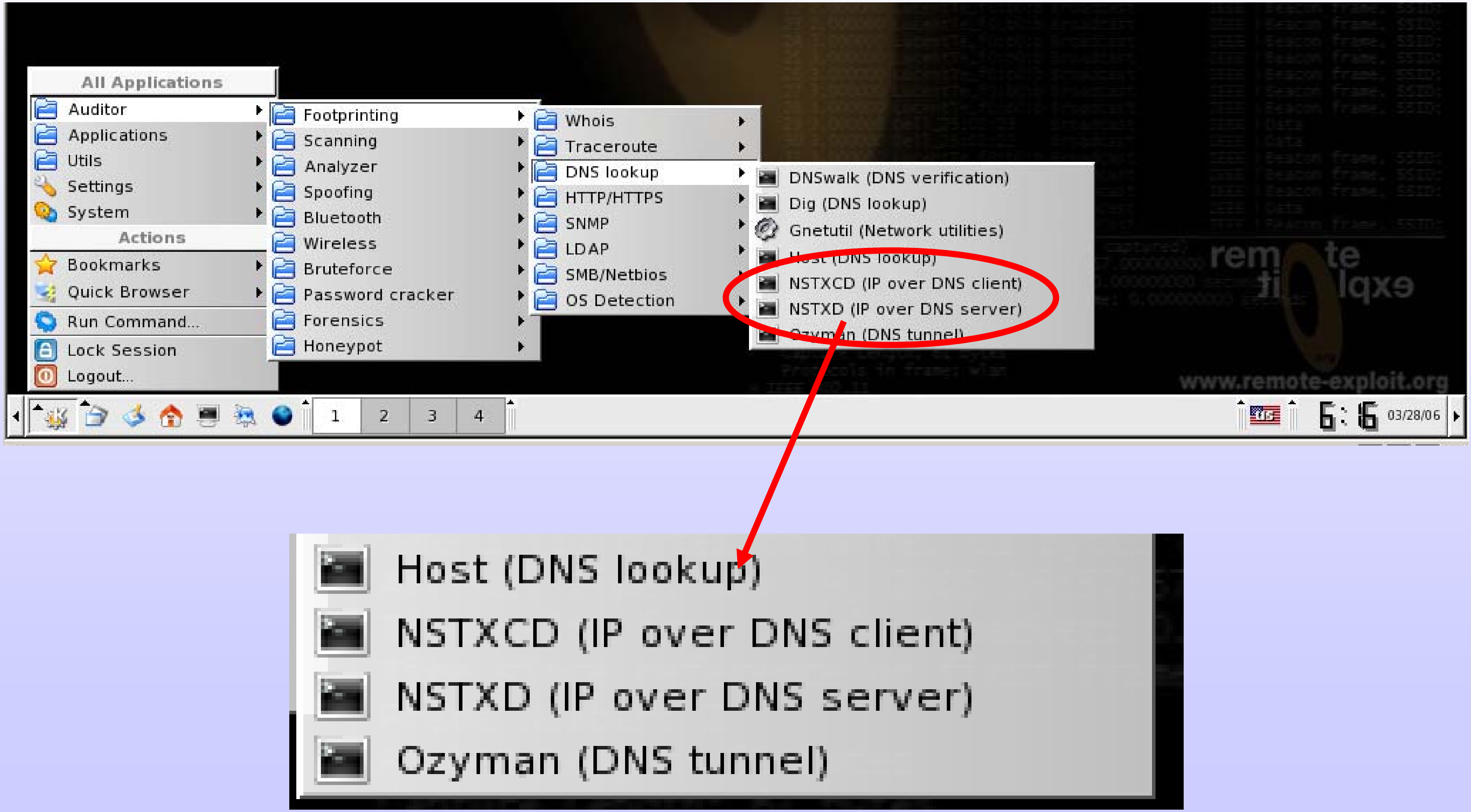
Petición DNS:
4500..[..]..03.micasa.es

Respuesta en el campo de TXT:
“45000...[..]..e6e5”

Paquetes IP!!!

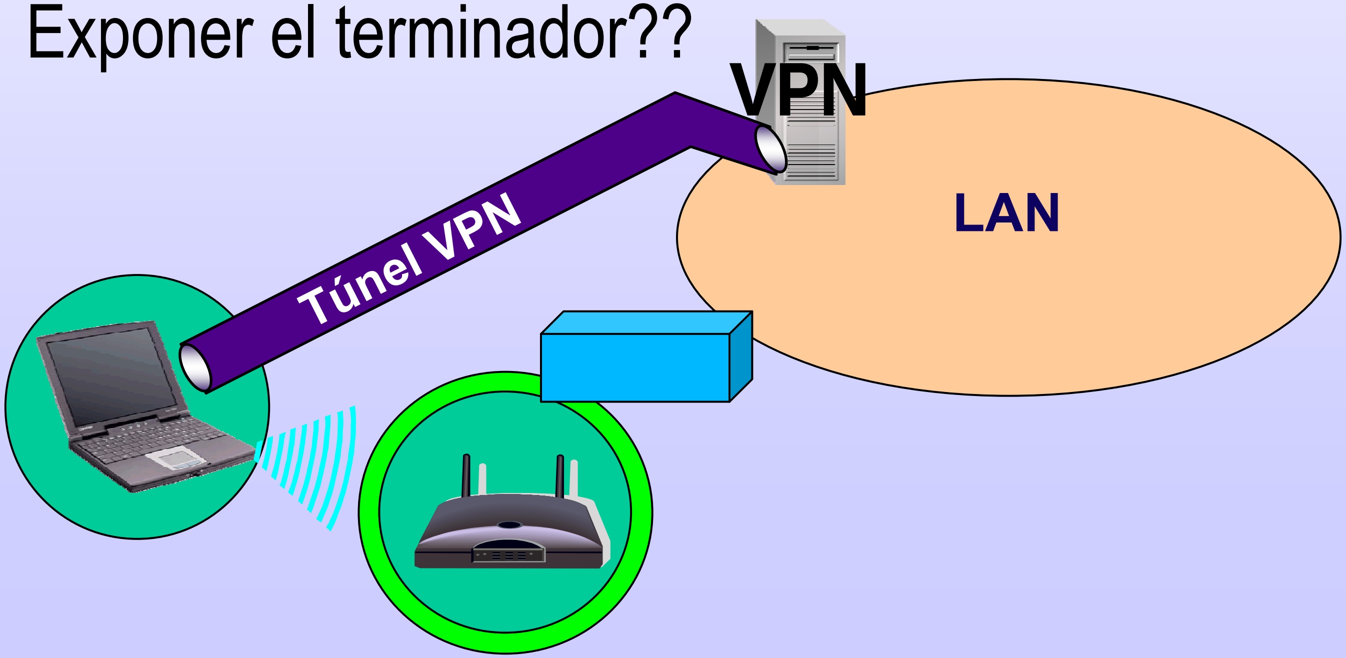
DNS-Tunneling

- ¿Crear túneles sobre DNS?... Complicado!!



Control de acceso

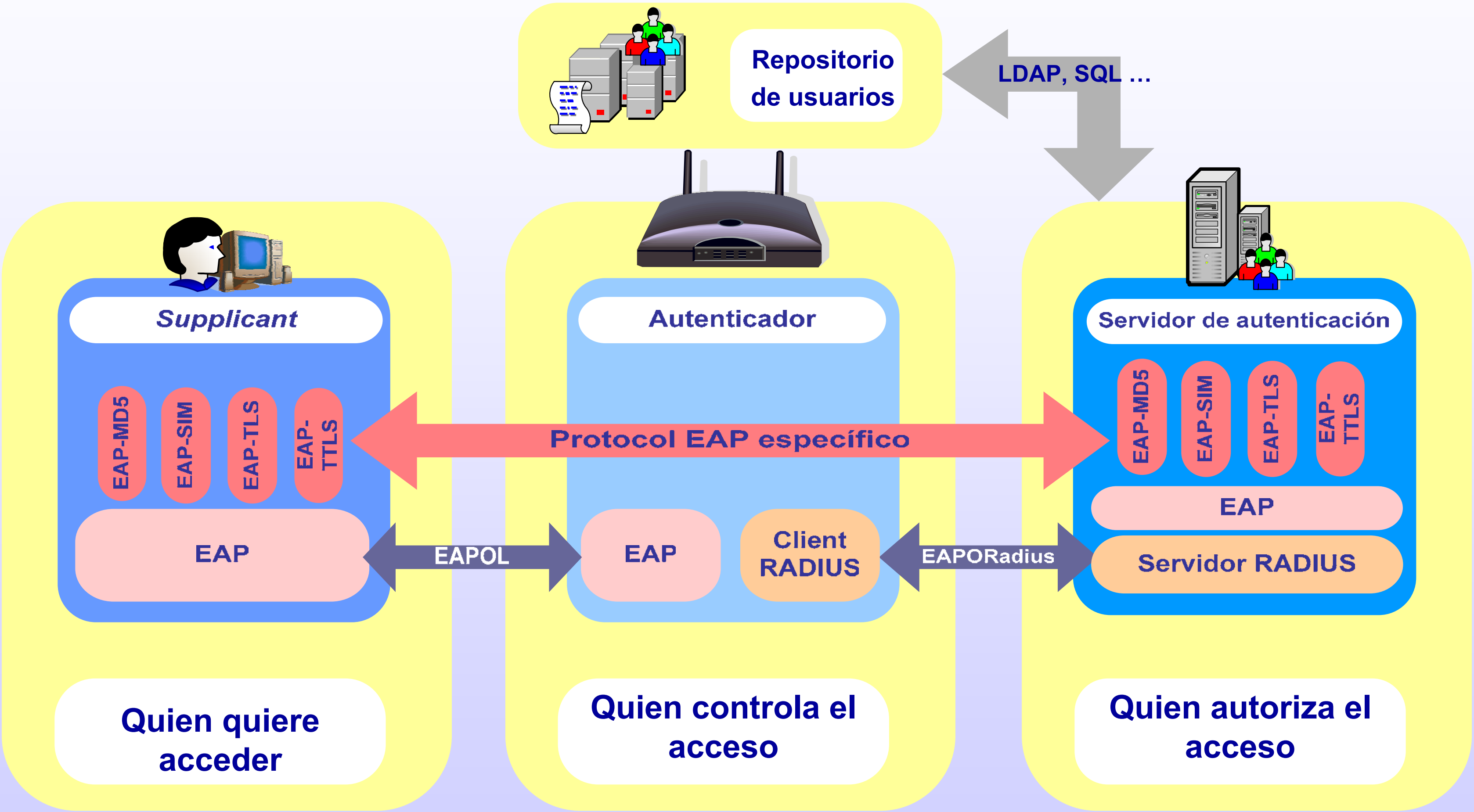
- Soluciones VPN
  - Protocolos VPN: PPTP vs. IPSec
  - ISAKMP (Main vs. Aggressive Mode)
  - AH vs ESP (256bits AES con integridad SHA1)
  - Clientes VPN
  - Exponer el terminador??



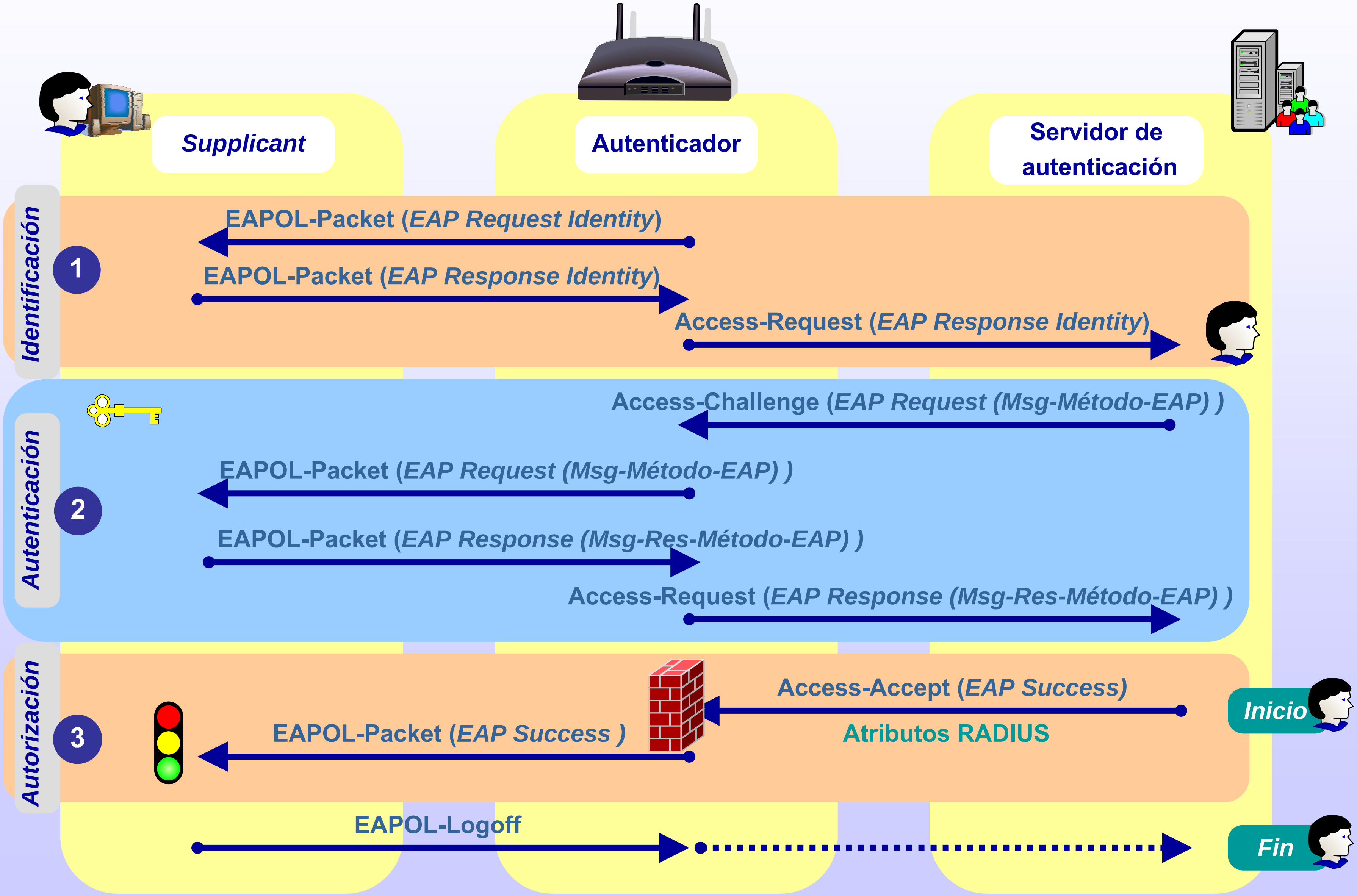
Control de acceso

- 802.1X
  - Proporciona una estructura para la autenticación
  - Métodos EAP
    - EAP-PEAP: usuario/password (puede utilizar TTLS para cifrar)
    - EAP/TLS: que tal vuestra PKI??
  - Atributos Radius
    - Distribución de claves WEP y WPA
    - Asignación de políticas
  - Accounting
  - Eduroam: “Requisito 802.1x y cifrado WPA”

802.1x


Repositorio de usuarios
LDAP, SQL …
Supplicant
EAP-MD5
EAP-SIM
EAP-TLS
EAP-TTLS
EAP
Autenticador
Protocol EAP específico
EAPOL
EAP
Client RADIUS
EAPORadius
Servidor de autenticación
EAP-MD5
EAP-SIM
EAP-TLS
EAP-TTLS
EAP
Servidor RADIUS
Quien quiere acceder
Quien controla el acceso
Quien autoriza el acceso

802.1x



Supplicant

Autenticador

Servidor de autenticación

1 Identificación

EAPOL-Packet (*EAP Request Identity*)

EAPOL-Packet (*EAP Response Identity*)

Access-Request (*EAP Response Identity*)

2 Autenticación

Access-Challenge (*EAP Request (Msg-Método-EAP))*

EAPOL-Packet (*EAP Request (Msg-Método-EAP))*

EAPOL-Packet (*EAP Response (Msg-Res-Método-EAP))*

Access-Request (*EAP Response (Msg-Res-Método-EAP))*

3 Autorización

Access-Accept (*EAP Success)*

Atributos RADIUS

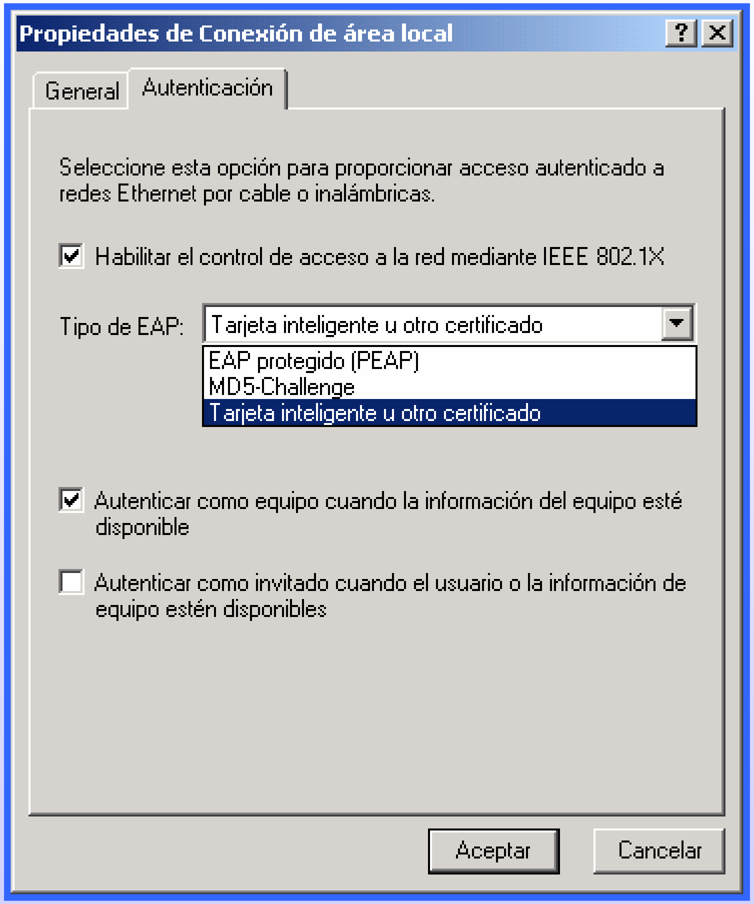
EAPOL-Packet (*EAP Success)*

Inicio

EAPOL-Logoff

Fin

Cliente 802.1x



Propiedades de Conexión de área local

Seleccione esta opción para proporcionar acceso autenticado a redes Ethernet por cable o inalámbricas.

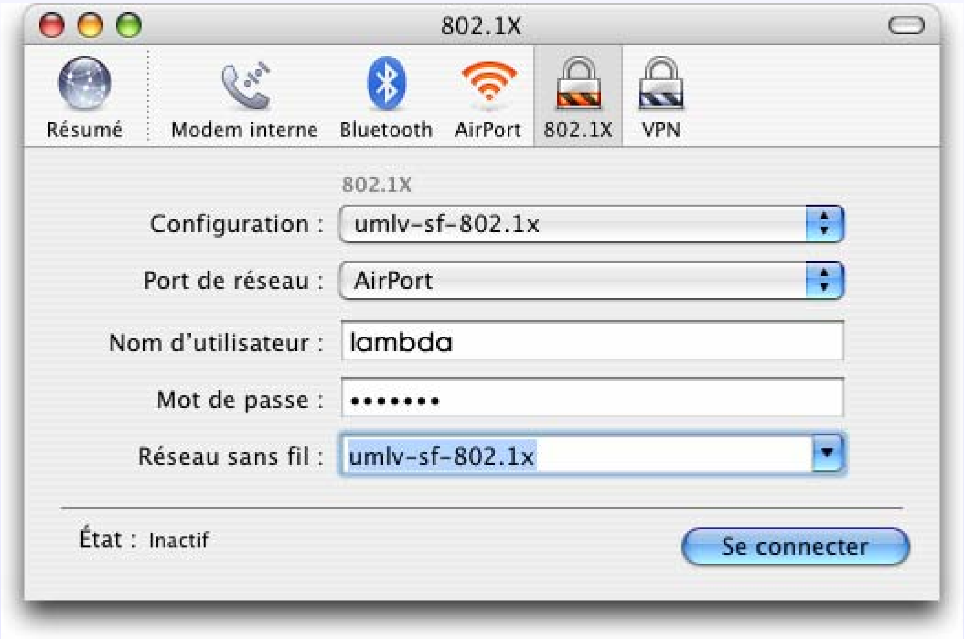
☑ Habilitar el control de acceso a la red mediante IEEE 802.1X

Tipo de EAP: Tarjeta inteligente u otro certificado

- EAP protegido (PEAP)
- MD5-Challenge
- Tarjeta inteligente u otro certificado

☑ Autenticar como equipo cuando la información del equipo esté disponible

☐ Autenticar como invitado cuando el usuario o la información de equipo estén disponibles



802.1X

802.1X

Configuration : umlv-sf-802.1x

Port de réseau : AirPort

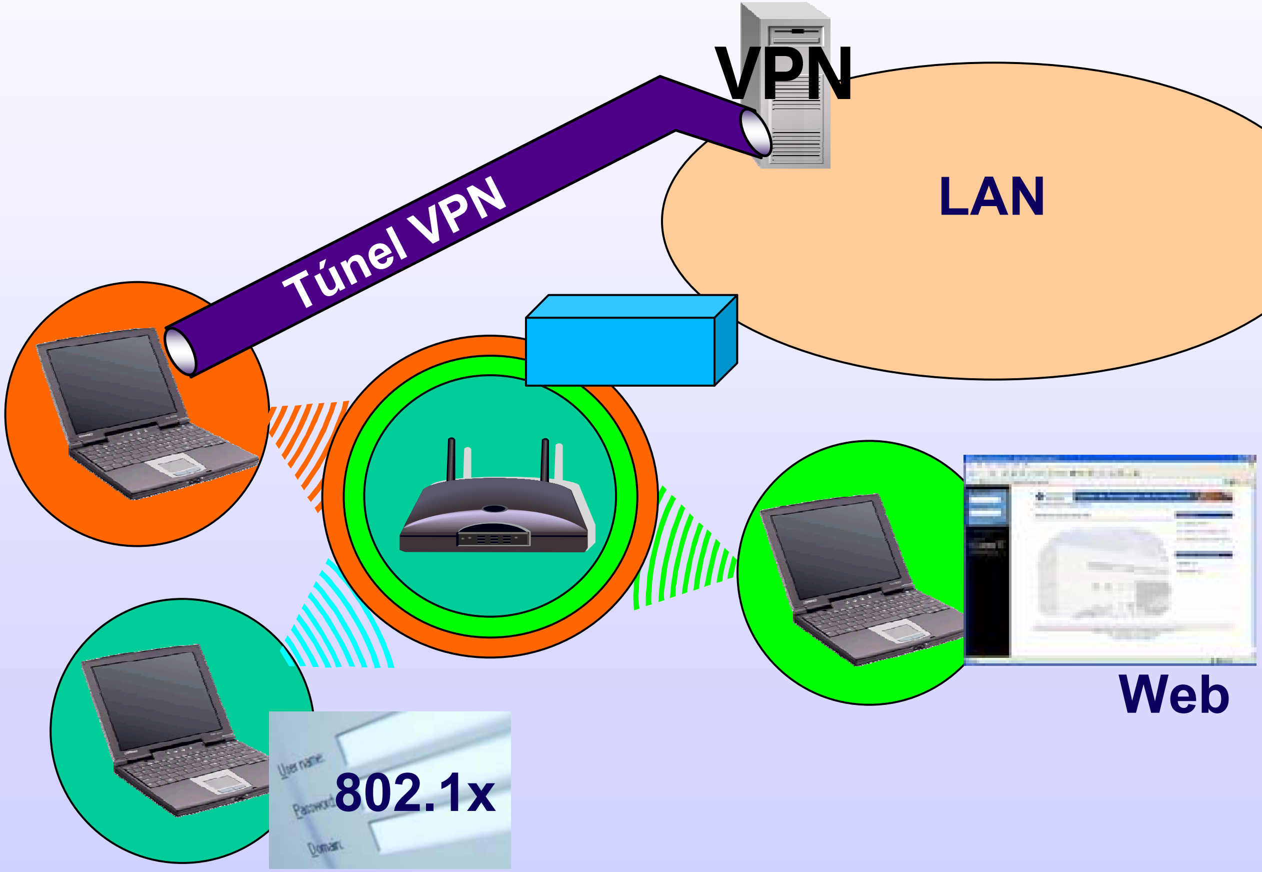
Nom d'utilisateur : lambda

Mot de passe : •••••••

Réseau sans fil : umlv-sf-802.1x

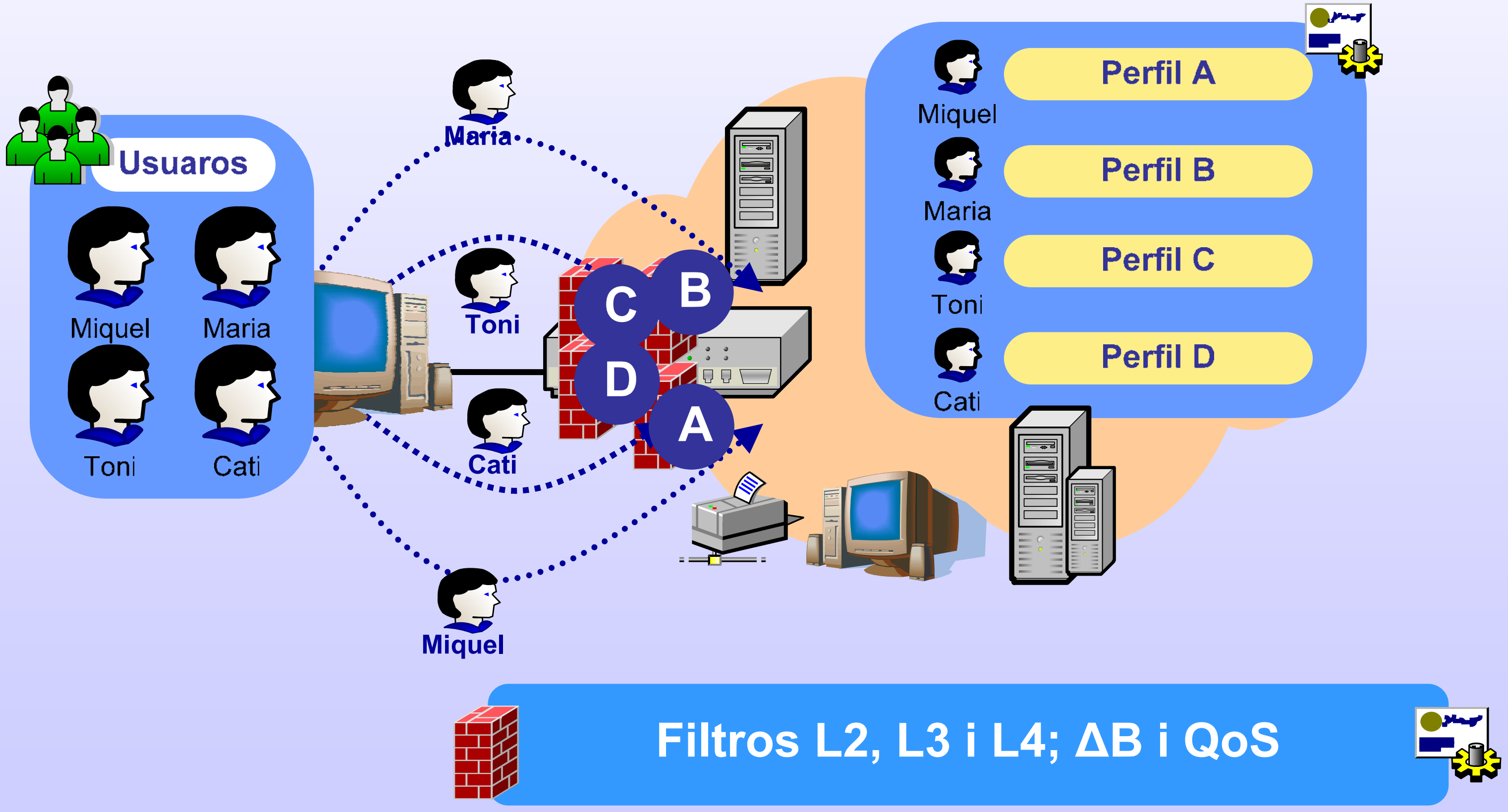
État : Inactif

Múltiples métodos de control de acceso



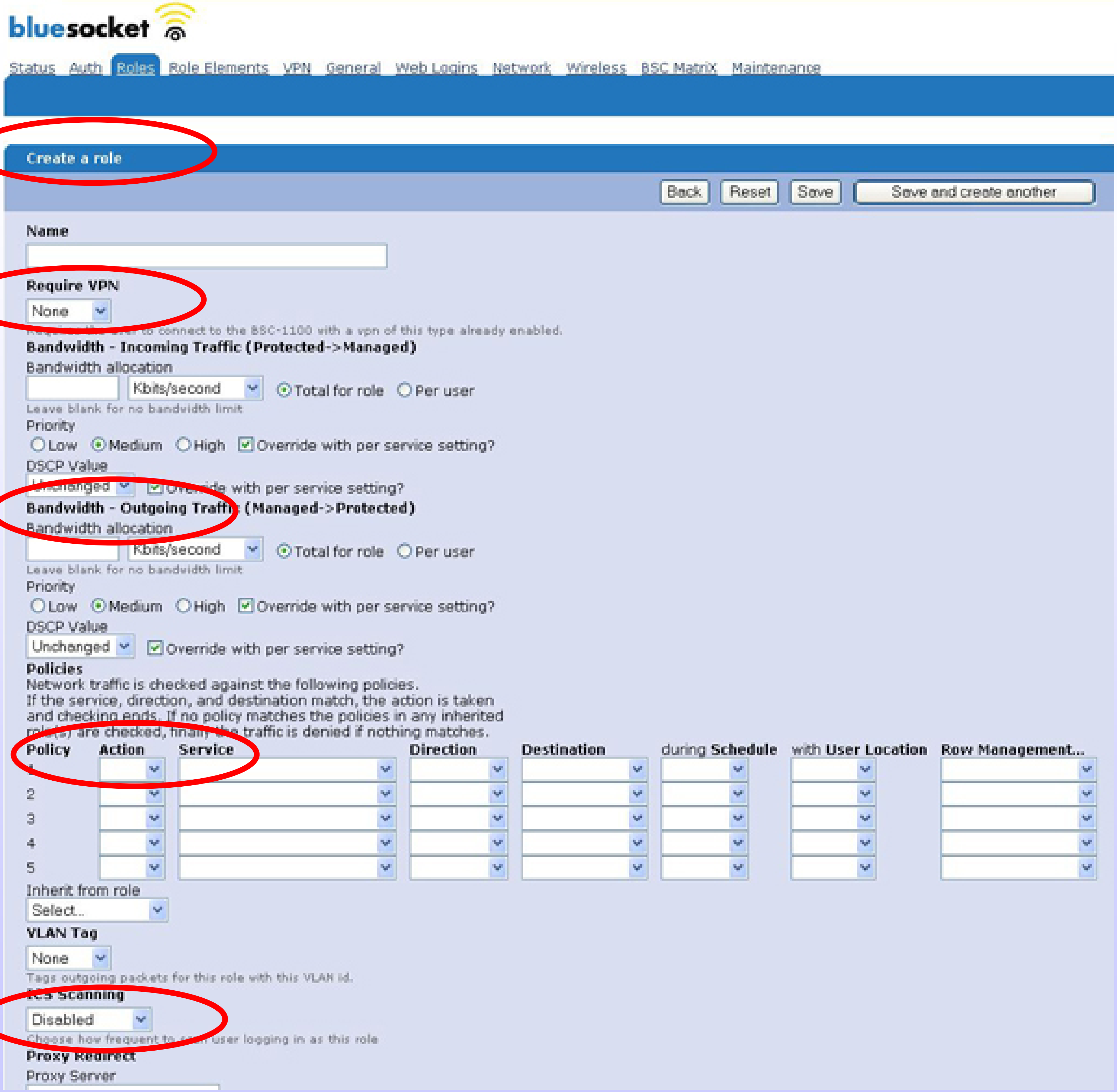
Políticas de acceso

- El objetivo...



Políticas de acceso

- Definir grupos de usuarios
- Definir el perfil para cada grupo
- Elementos de un perfil
  - Filtros de nivel 2: MAC, VLAN origen
  - Filtros de nivel 3-4: IP, TCP, UDP
  - Filtros de nivel 7: a nivel de aplicación!!
  - Control de ancho de banda



Create a role

Name

Require VPN

None

Requires the user to connect to the BSC-1100 with a vpn of this type already enabled.

Bandwidth - Incoming Traffic (Protected->Managed)

Bandwidth allocation

Kbits/second ● Total for role ○ Per user

Leave blank for no bandwidth limit

Priority

○ Low ● Medium ○ High ☑ Override with per service setting?

DSCP Value

Unchanged ☑ Override with per service setting?

Bandwidth - Outgoing Traffic (Managed->Protected)

Bandwidth allocation

Kbits/second ● Total for role ○ Per user

Leave blank for no bandwidth limit

Priority

○ Low ● Medium ○ High ☑ Override with per service setting?

DSCP Value

Unchanged ☑ Override with per service setting?

Policies

Network traffic is checked against the following policies. If the service, direction, and destination match, the action is taken and checking ends. If no policy matches the policies in any inherited role(s) are checked, finally the traffic is denied if nothing matches.

Policy	Action	Service	Direction	Destination	during Schedule	with User Location	Row Management...
1							
2							
3							
4							
5							

Inherit from role

Select..

VLAN Tag

None

Tags outgoing packets for this role with this VLAN id.

ICS Scanning

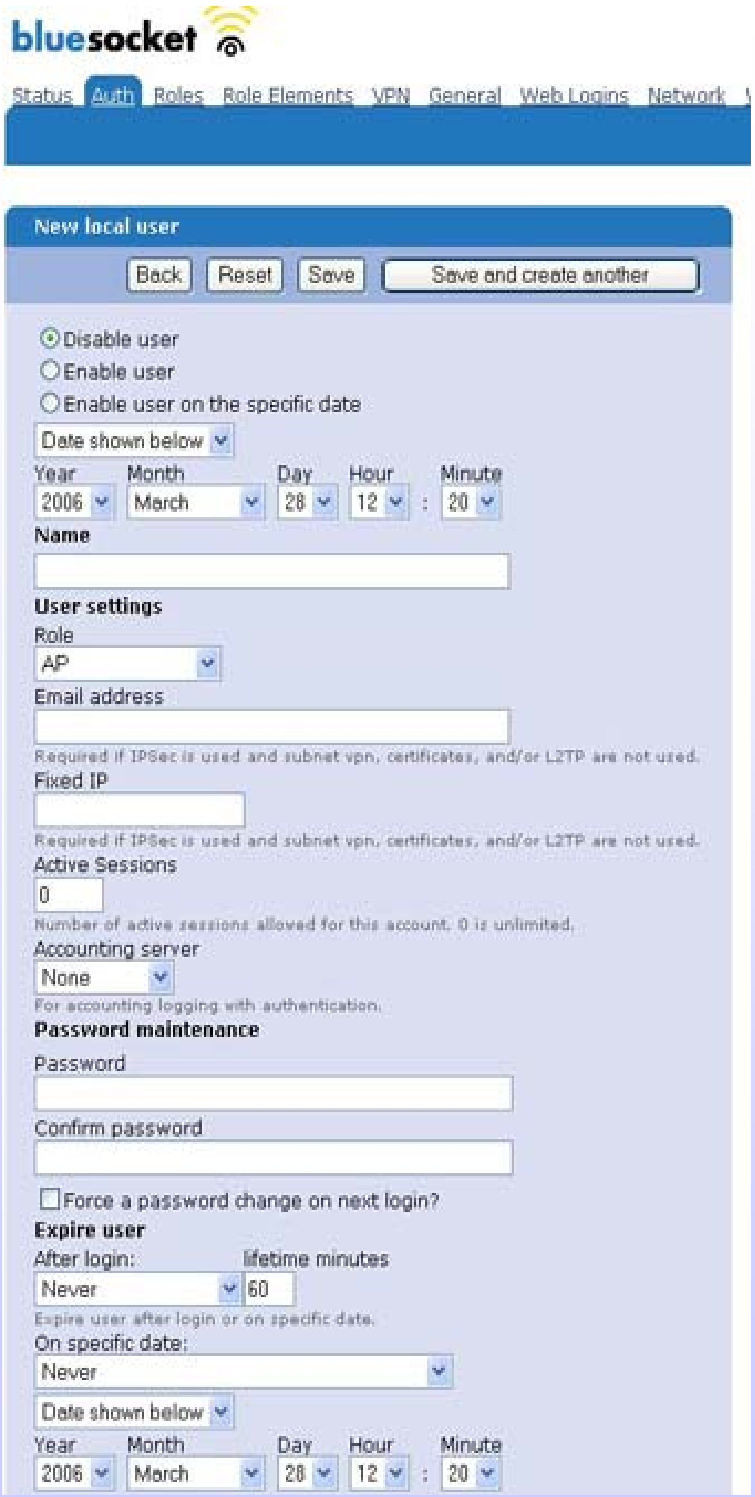
Disabled

Choose how frequent to scan user logging in as this role

Proxy Redirect

Proxy Server

- Alta de usuarios
  - Asignar perfil
  - Fecha de habilitación
  - Fecha de caducidad
  - Accounting



New local user

● Disable user
○ Enable user
○ Enable user on the specific date

Date shown below

Year	Month	Day	Hour	Minute
2006	March	28	12	20

Name

User settings

Role: AP

Email address

Required if IPSec is used and subnet vpn, certificates, and/or L2TP are not used.

Fixed IP

Required if IPSec is used and subnet vpn, certificates, and/or L2TP are not used.

Active Sessions: 0

Number of active sessions allowed for this account. 0 is unlimited.

Accounting server: None

For accounting logging with authentication.

Password maintenance

Password

Confirm password

□ Force a password change on next login?

Expire user

After login: Never — lifetime minutes: 60

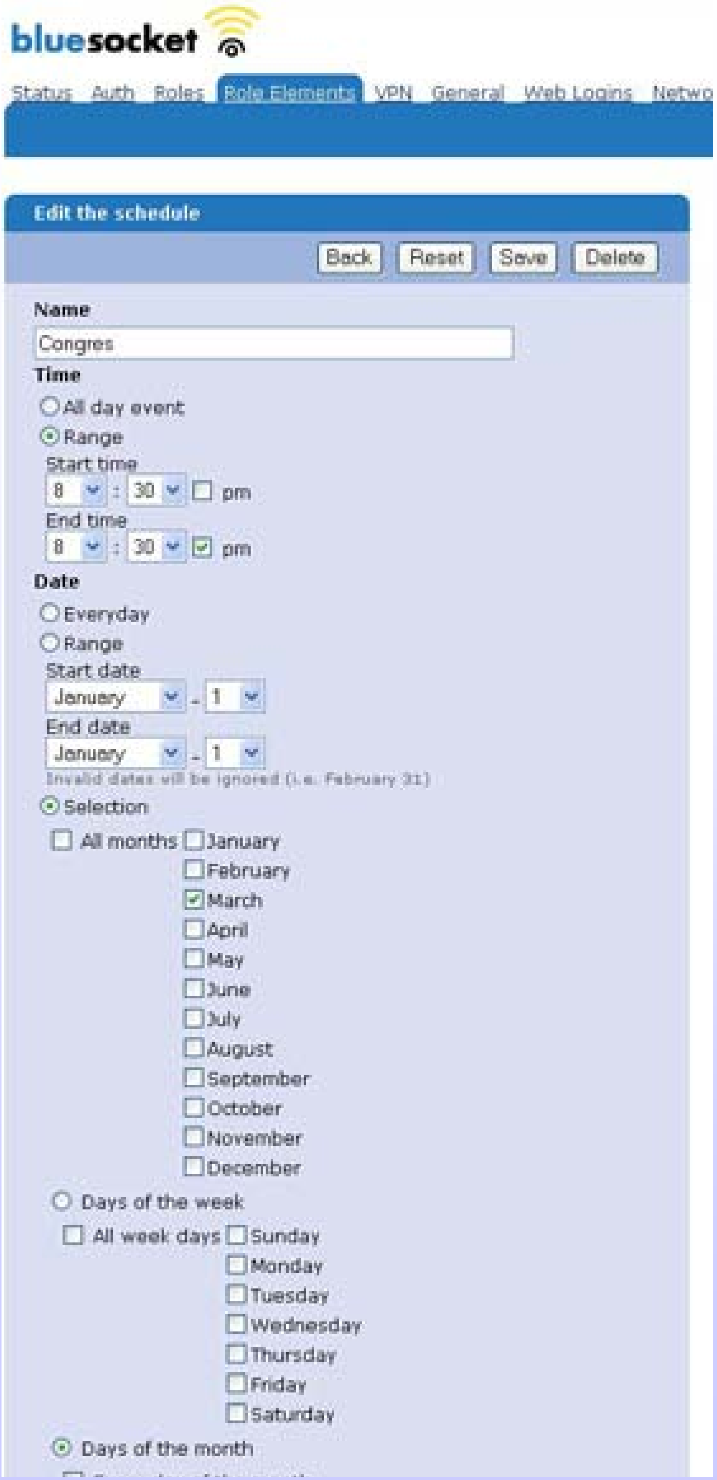
Expire user after login or on specific date.

On specific date: Never

Date shown below

Year	Month	Day	Hour	Minute
2006	March	28	12	20

- Control horario
  - Horas, día, meses,...
  - Asignado a perfil
  - Asignado a usuario



bluesocket
Status Auth Roles Role Elements VPN General Web Logins Netwo
Edit the schedule
Back Reset Save Delete

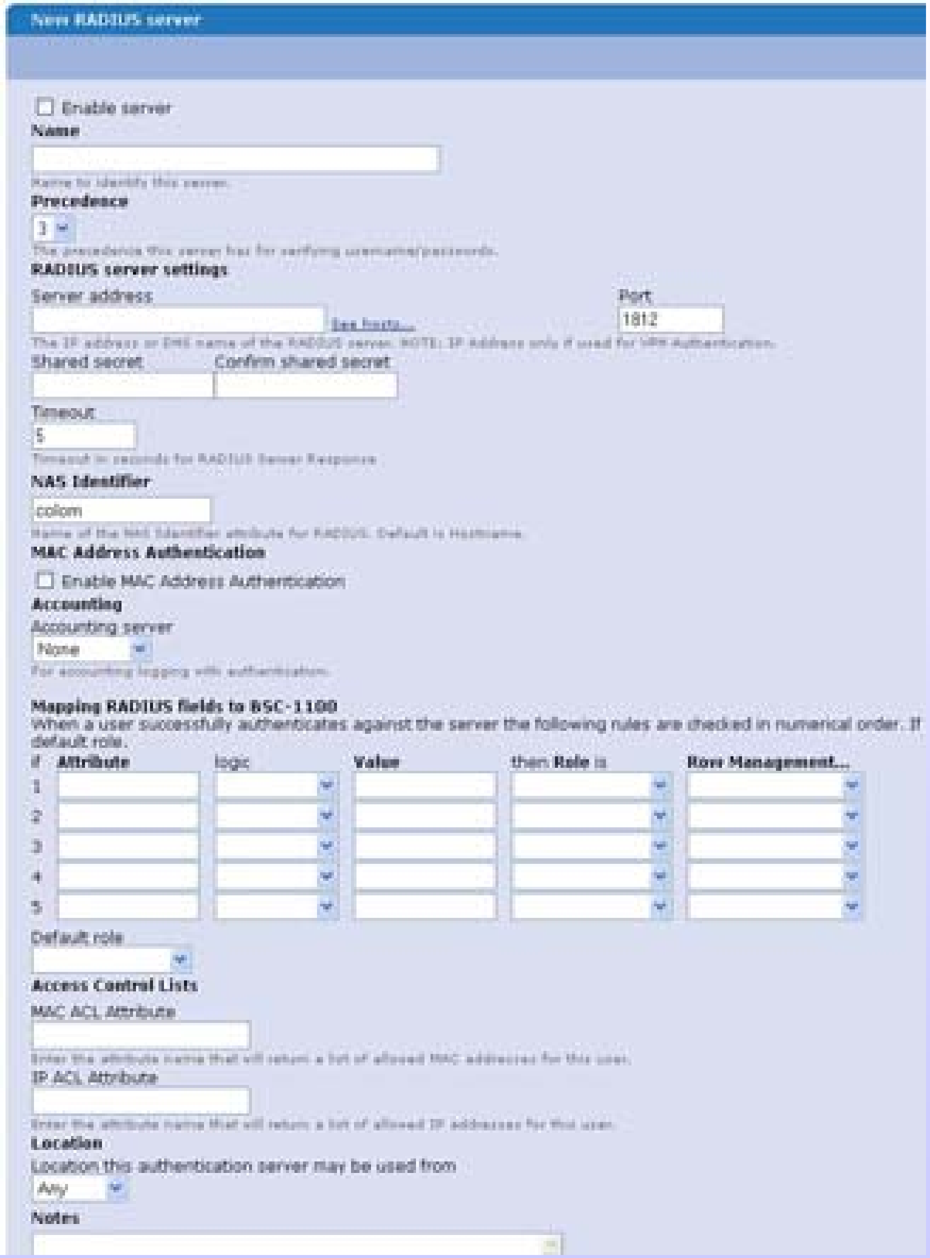
Name
Congres

Time
○ All day event
● Range
Start time
8 : 30 □ pm
End time
8 : 30 ☑ pm

Date
○ Everyday
○ Range
Start date
January - 1
End date
January - 1
Invalid dates will be ignored (i.e. February 31)
● Selection
□ All months □ January
□ February
☑ March
□ April
□ May
□ June
□ July
□ August
□ September
□ October
□ November
□ December
○ Days of the week
□ All week days □ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
● Days of the month

Servidores de autenticación

- Radius:
  - Asignación de perfiles
    - Según atributos
  - Atributos para WEP,WPA
    - 802.1x



New RADIUS server

□ Enable server

Name

Name to identify this server.

Precedence

3

The precedence this server has for verifying usernames/passwords.

RADIUS server settings

Server address — See hosts... — Port: 1812

The IP address or DNS name of the RADIUS server. NOTE: IP Address only if used for VPN Authentication.

Shared secret — Confirm shared secret

Timeout: 5

Timeout in seconds for RADIUS Server Response

NAS Identifier

colom

Name of the NAS Identifier attribute for RADIUS. Default is Hostname.

MAC Address Authentication

□ Enable MAC Address Authentication

Accounting

Accounting server: None

For accounting logging with authentication.

Mapping RADIUS fields to BSC-1100

When a user successfully authenticates against the server the following rules are checked in numerical order. If default role.

#	**Attribute**	logic	**Value**	then **Role** is	**Row Management...**
1					
2					
3					
4					
5					

Default role

Access Control Lists

MAC ACL Attribute

Enter the attribute name that will return a list of allowed MAC addresses for this user.

IP ACL Attribute

Enter the attribute name that will return a list of allowed IP addresses for this user.

Location

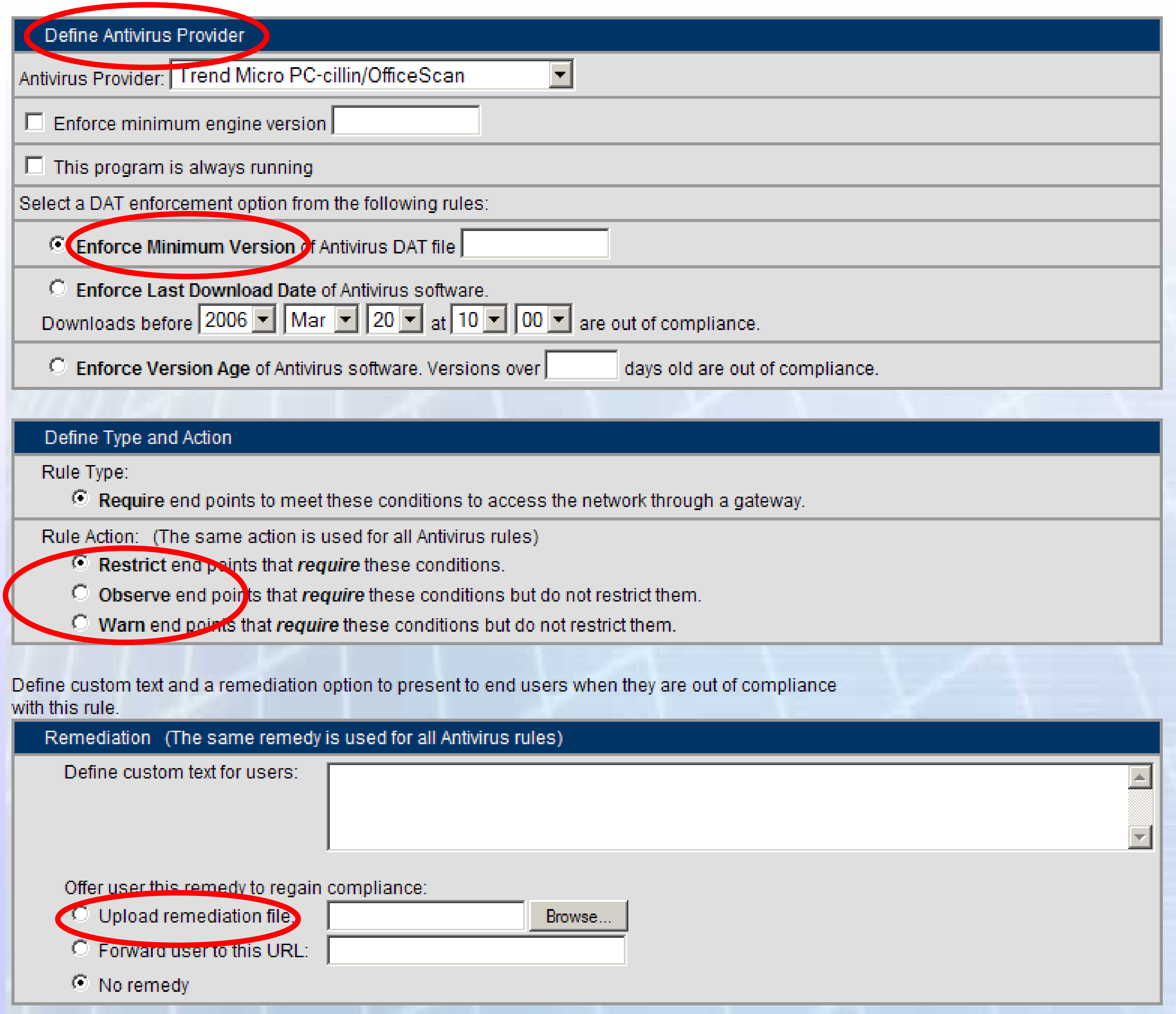
Location this authentication server may be used from: Any

Notes

Control de admisión

- Realizar un control de “calidad” de los usuarios
  - Verificar que tienen el antivirus instalado
    - Ofrecerle la actualización
  - Actualizaciones de windows
    - Permitirle acceso a windows update
  - Virus, troyanos, dialers, adware,...
    - Bloquearle o informarle sobre su problema
  - Realizar búsquedas en el registro de windows
    - Localizar registros y realizar comparaciones
  - Localizar ficheros o ejecutables

- La configuración del sistema...



Define Antivirus Provider

Antivirus Provider: Trend Micro PC-cillin/OfficeScan

☐ Enforce minimum engine version

☐ This program is always running

Select a DAT enforcement option from the following rules:

● **Enforce Minimum Version** of Antivirus DAT file

○ **Enforce Last Download Date** of Antivirus software.
Downloads before 2006 Mar 20 at 10 00 are out of compliance.

○ **Enforce Version Age** of Antivirus software. Versions over days old are out of compliance.

Define Type and Action

Rule Type:

● **Require** end points to meet these conditions to access the network through a gateway.

Rule Action: (The same action is used for all Antivirus rules)

● **Restrict** end points that ***require*** these conditions.

○ **Observe** end points that ***require*** these conditions but do not restrict them.

○ **Warn** end points that ***require*** these conditions but do not restrict them.

Define custom text and a remediation option to present to end users when they are out of compliance with this rule.

Remediation (The same remedy is used for all Antivirus rules)

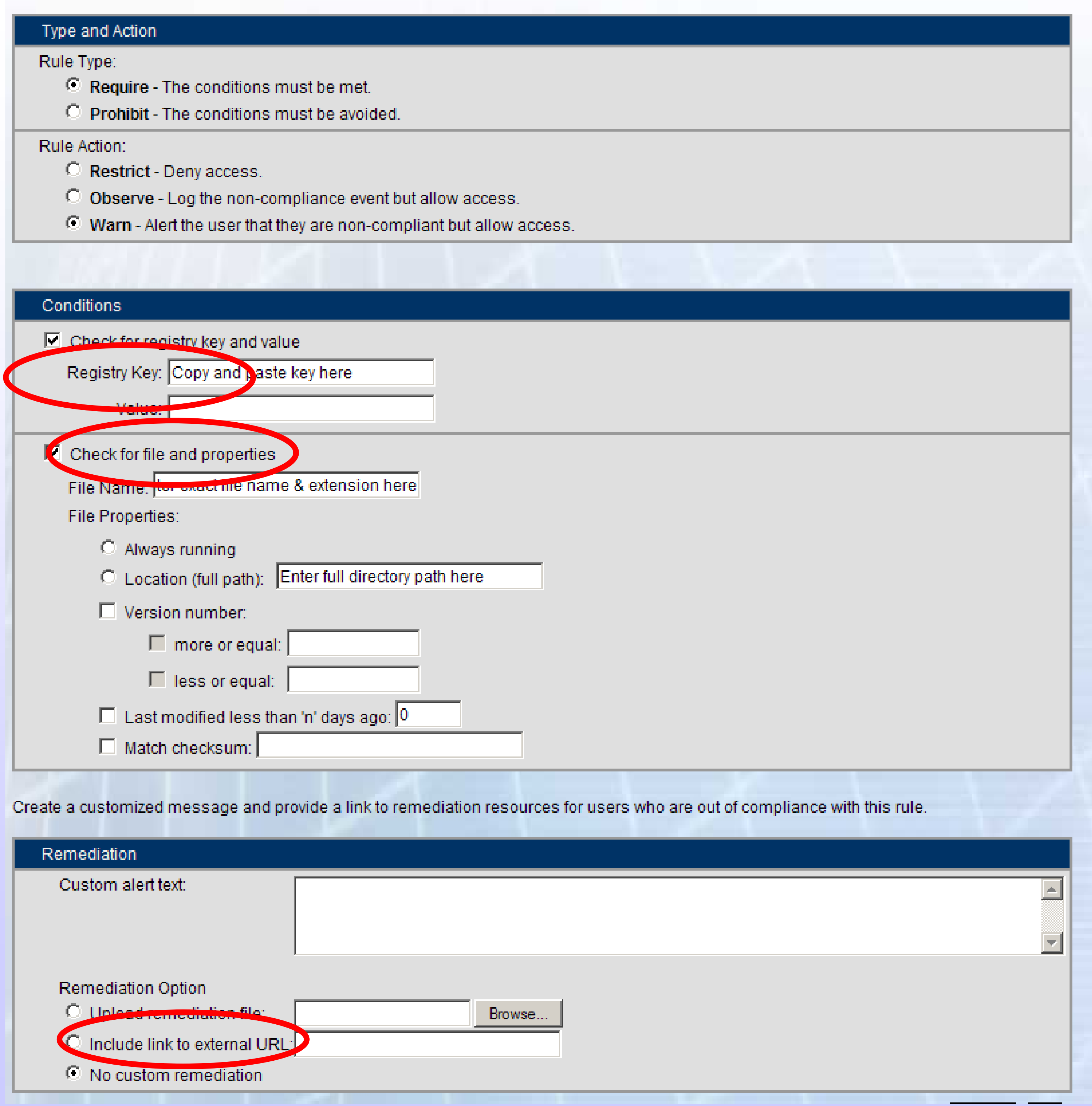
Define custom text for users:

Offer user this remedy to regain compliance:

○ Upload remediation file Browse...

○ Forward user to this URL:

● No remedy



Type and Action

Rule Type:

● **Require** - The conditions must be met.

○ **Prohibit** - The conditions must be avoided.

Rule Action:

○ **Restrict** - Deny access.

○ **Observe** - Log the non-compliance event but allow access.

● **Warn** - Alert the user that they are non-compliant but allow access.

Conditions

☑ Check for registry key and value

Registry Key: Copy and paste key here

Value:

☑ Check for file and properties

File Name: ter exact file name & extension here

File Properties:

○ Always running

○ Location (full path): Enter full directory path here

□ Version number:

□ more or equal:

□ less or equal:

□ Last modified less than 'n' days ago: 0

□ Match checksum:

Create a customized message and provide a link to remediation resources for users who are out of compliance with this rule.

Remediation

Custom alert text:

Remediation Option

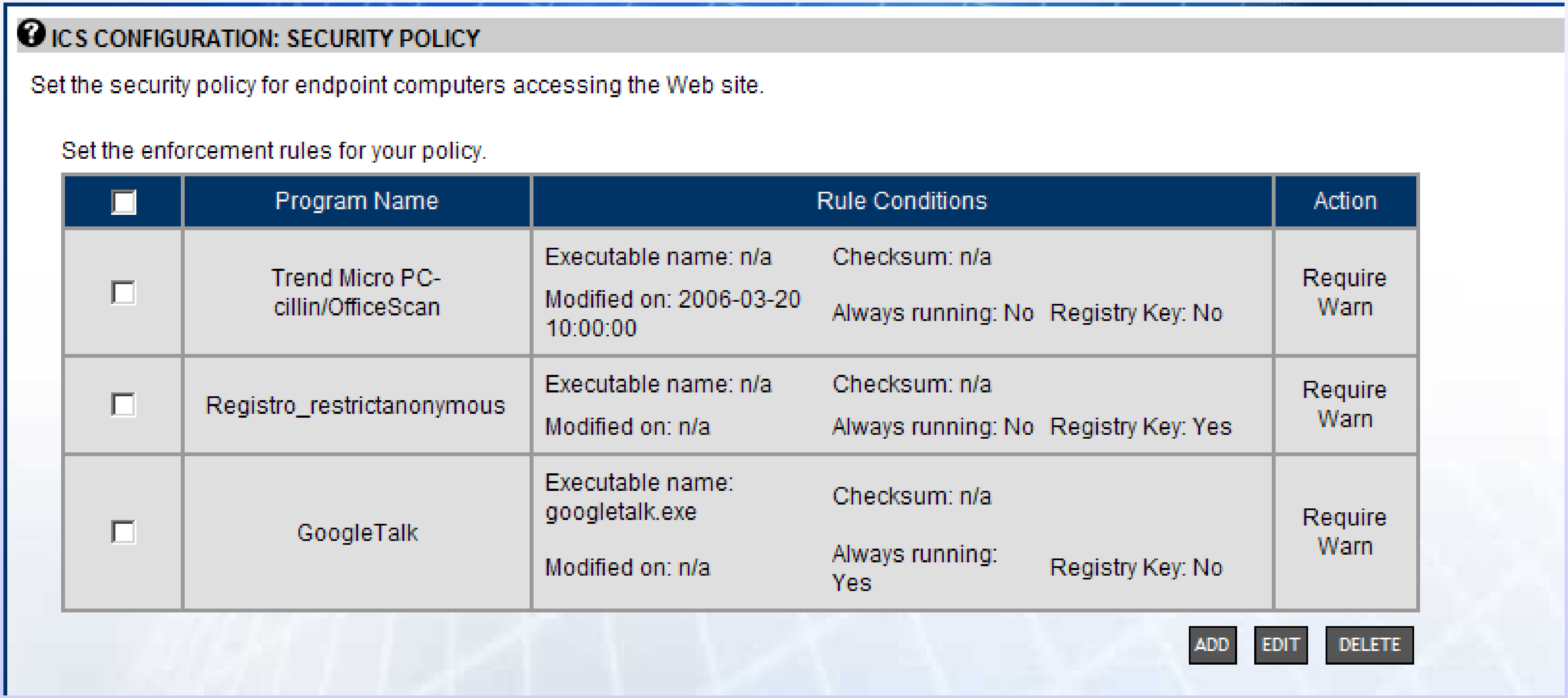
○ Upload remediation file: Browse...

○ Include link to external URL:

● No custom remediation

Control de admisión

- Reglas específicas: Bloquear, informar o ignorar...



ICS CONFIGURATION: SECURITY POLICY

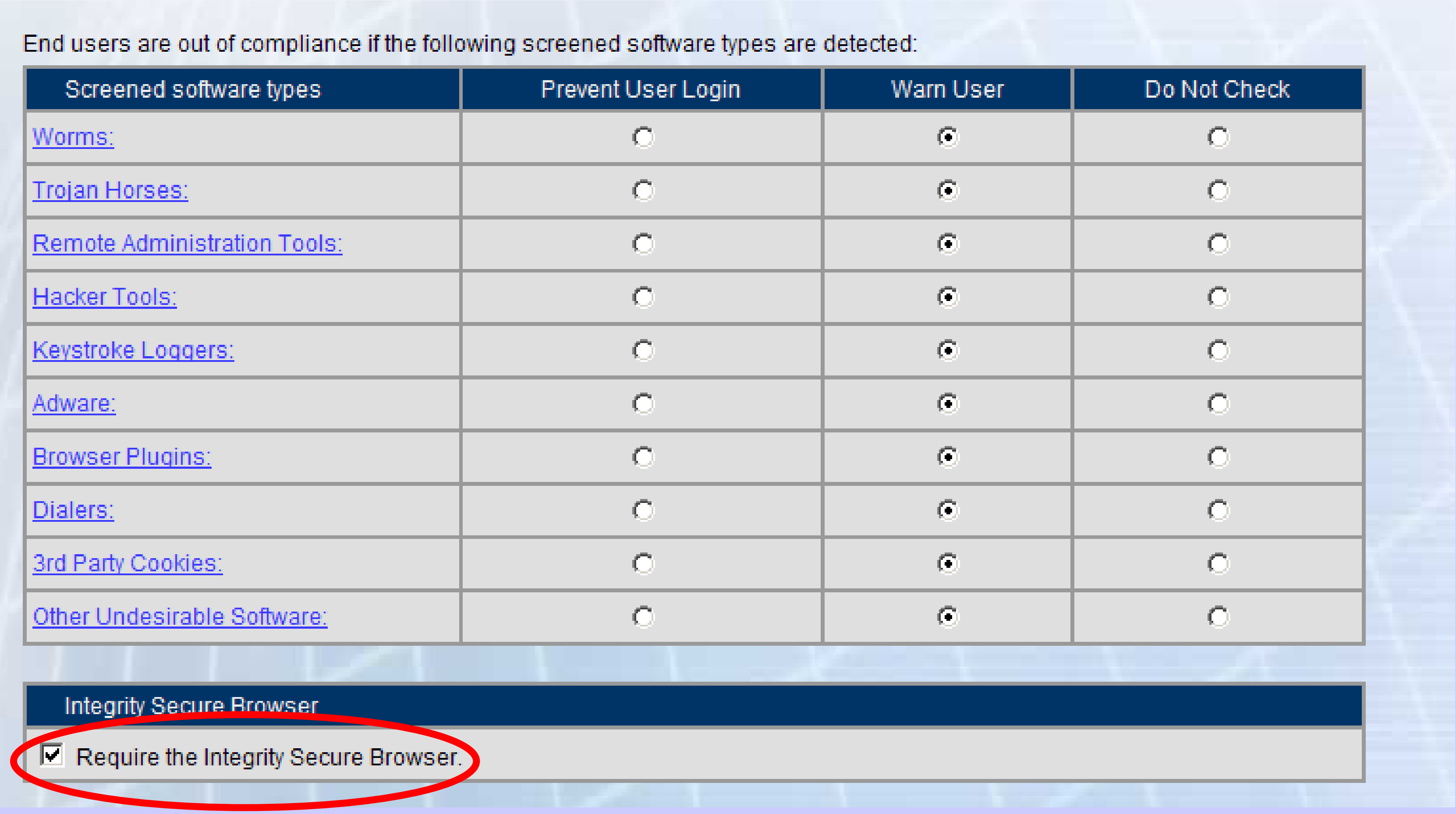
Set the security policy for endpoint computers accessing the Web site.

Set the enforcement rules for your policy.

□	Program Name	Rule Conditions	Action
□	Trend Micro PC-cillin/OfficeScan	Executable name: n/a Checksum: n/a Modified on: 2006-03-20 10:00:00 Always running: No Registry Key: No	Require Warn
□	Registro_restrictanonymous	Executable name: n/a Checksum: n/a Modified on: n/a Always running: No Registry Key: Yes	Require Warn
□	GoogleTalk	Executable name: googletalk.exe Checksum: n/a Modified on: n/a Always running: Yes Registry Key: No	Require Warn

Control de admisión

- Virus, troyanos, dialers, etc...
- Integrity Secure Browser



End users are out of compliance if the following screened software types are detected:

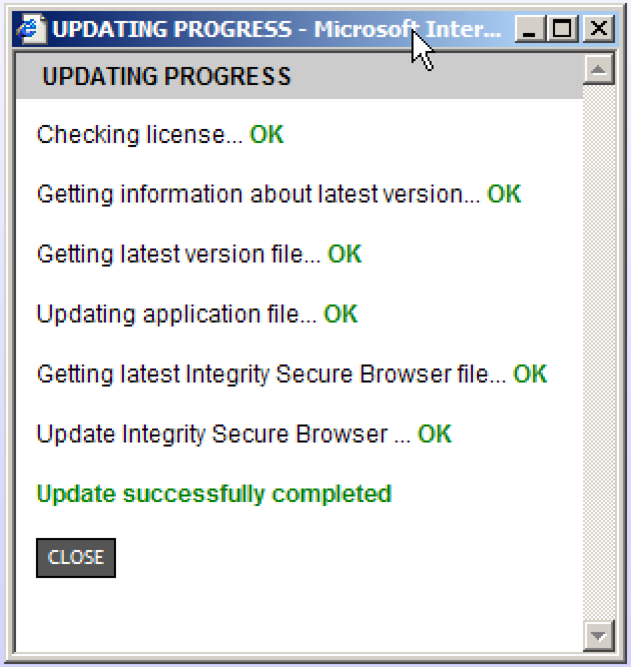
Screened software types	Prevent User Login	Warn User	Do Not Check
Worms:	○	●	○
Trojan Horses:	○	●	○
Remote Administration Tools:	○	●	○
Hacker Tools:	○	●	○
Keystroke Loggers:	○	●	○
Adware:	○	●	○
Browser Plugins:	○	●	○
Dialers:	○	●	○
3rd Party Cookies:	○	●	○
Other Undesirable Software:	○	●	○

Integrity Secure Browser

☑ Require the Integrity Secure Browser.

Control de admisión

- Políticas y firmas actualizadas!!!



UPDATING PROGRESS

Checking license... OK

Getting information about latest version... OK

Getting latest version file... OK

Updating application file... OK

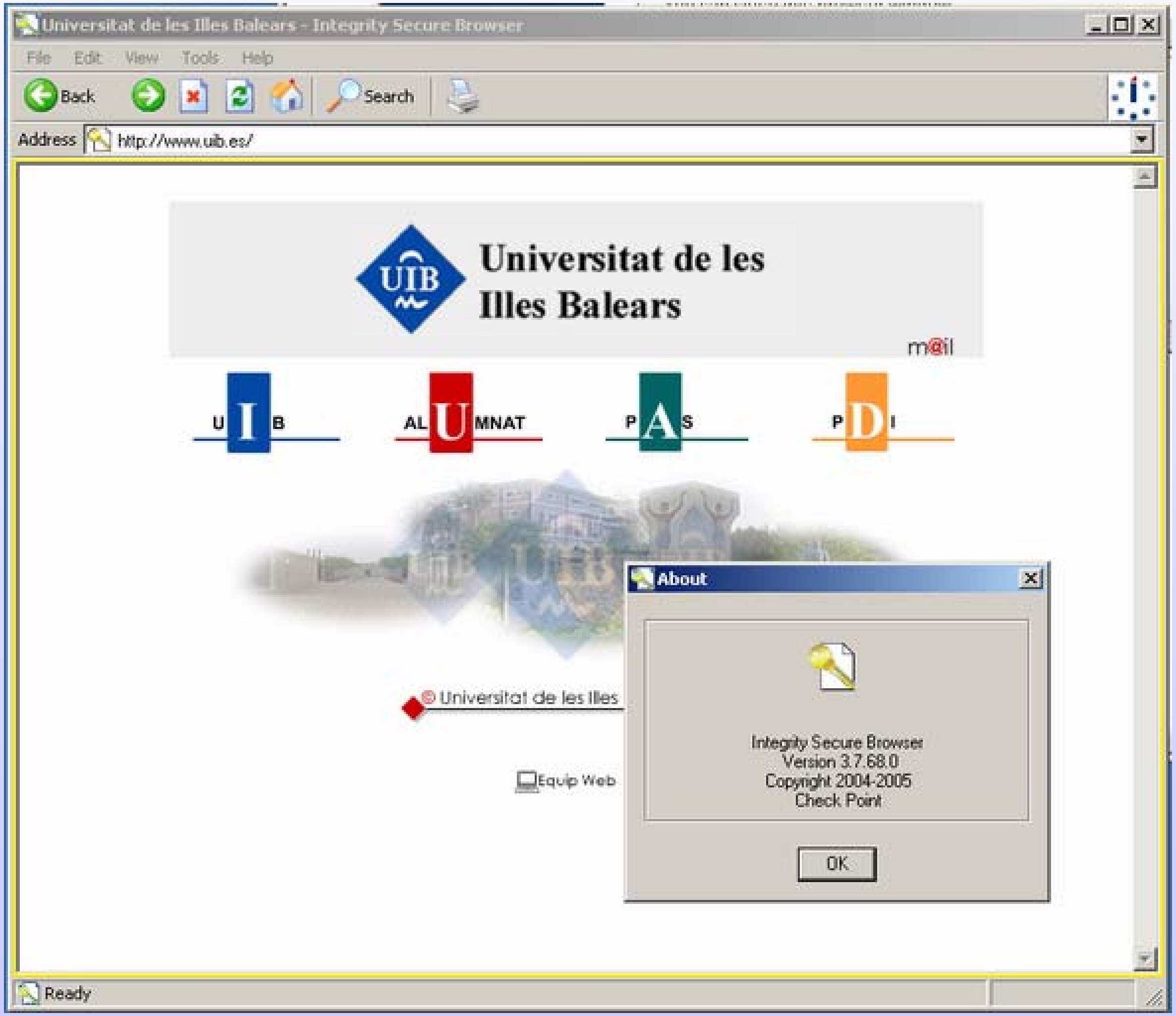
Getting latest Integrity Secure Browser file... OK

Update Integrity Secure Browser ... OK

Update successfully completed

Control de admisión

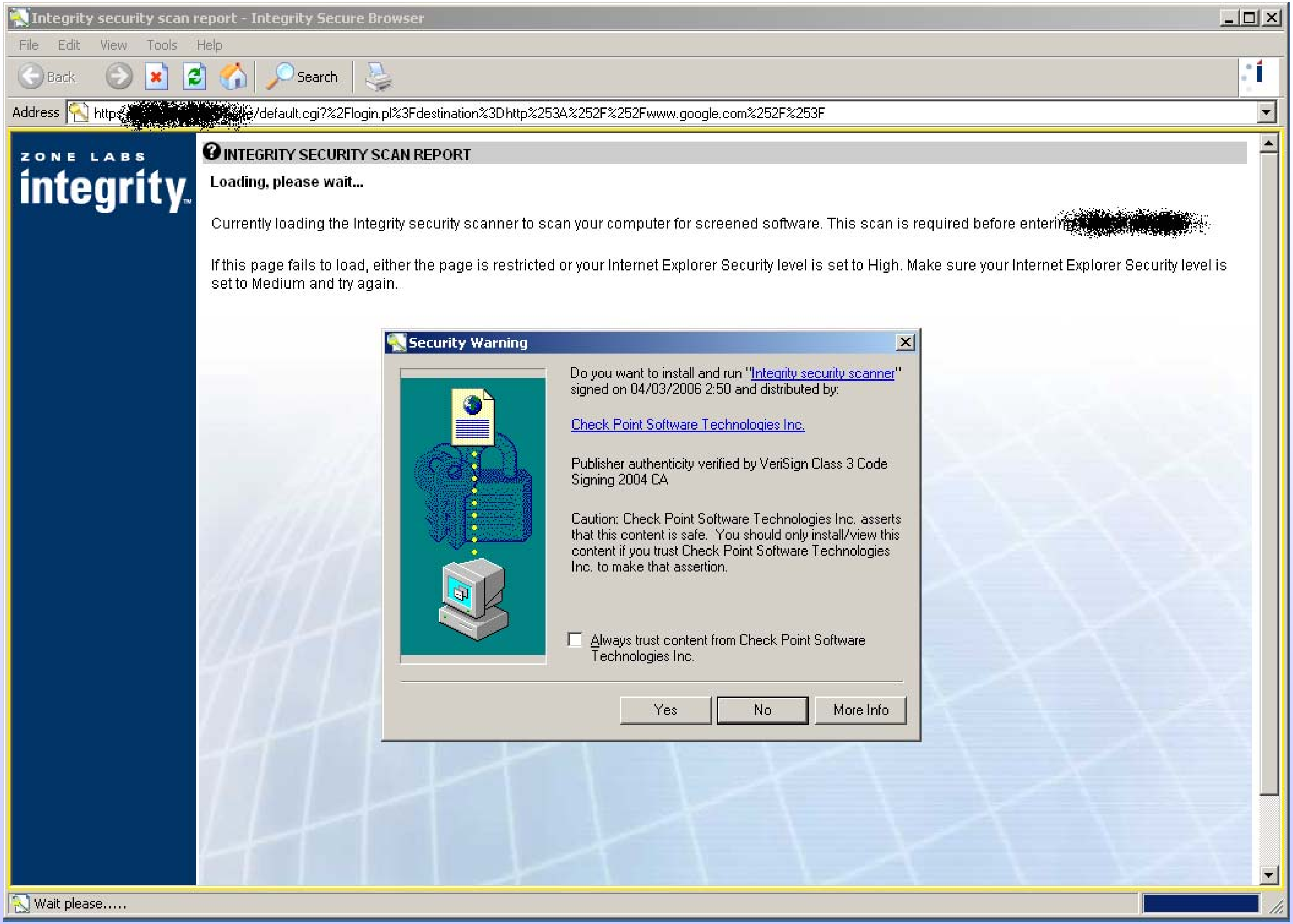
- ¿Qué percibe el usuario?



Universitat de les Illes Balears - Integrity Secure Browser

Address http://www.uib.es/

Integrity Secure Browser
Version 3.7.68.0
Copyright 2004-2005
Check Point


Integrity security scan report - Integrity Secure Browser
File Edit View Tools Help
Back
Search
Address
ZONE LABS
integrity

http[redacted]/default.cgi?%2Flogin.pl%3Fdestination%3Dhttp%253A%252F%252Fwww.google.com%252F%253F

INTEGRITY SECURITY SCAN REPORT

Loading, please wait...

Currently loading the Integrity security scanner to scan your computer for screened software. This scan is required before enterin[redacted]

If this page fails to load, either the page is restricted or your Internet Explorer Security level is set to High. Make sure your Internet Explorer Security level is set to Medium and try again.

Security Warning

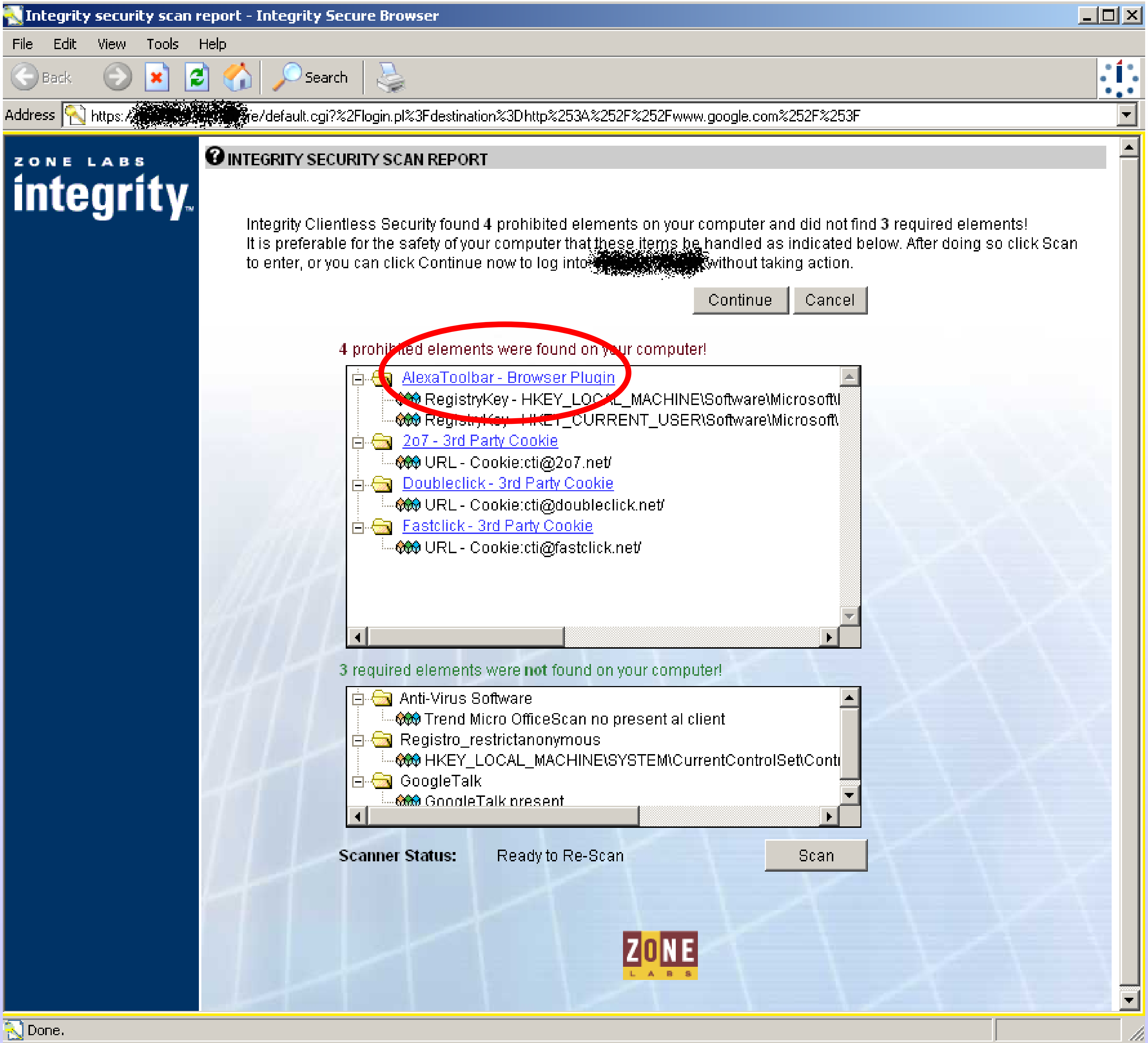
Do you want to install and run "Integrity security scanner" signed on 04/03/2006 2:50 and distributed by:

Check Point Software Technologies Inc.

Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA

Caution: Check Point Software Technologies Inc. asserts that this content is safe. You should only install/view this content if you trust Check Point Software Technologies Inc. to make that assertion.

□ Always trust content from Check Point Software Technologies Inc.


Integrity security scan report - Integrity Secure Browser
File Edit View Tools Help
Back
Search
Address
ZONE LABS
integrity
Continue
Cancel
Scan
ZONE LABS
Done.

https:/[redacted]re/default.cgi?%2Flogin.pl%3Fdestination%3Dhttp%253A%252F%252Fwww.google.com%252F%253F

INTEGRITY SECURITY SCAN REPORT

Integrity Clientless Security found **4** prohibited elements on your computer and did not find **3** required elements!
It is preferable for the safety of your computer that these items be handled as indicated below. After doing so click Scan to enter, or you can click Continue now to log into [redacted] without taking action.

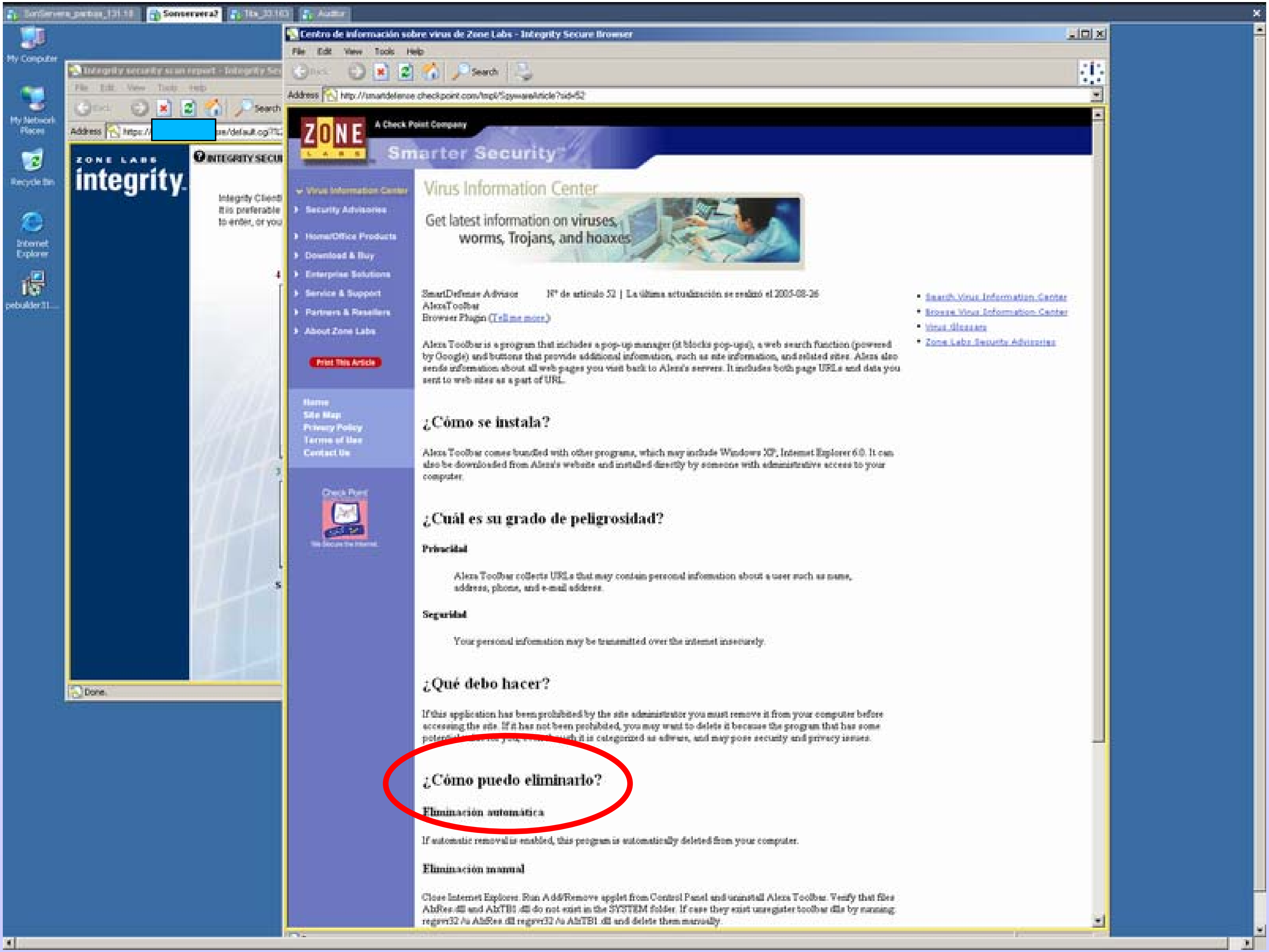
4 prohibited elements were found on your computer!

- AlexaToolbar - Browser Plugin
  - RegistryKey - HKEY_LOCAL_MACHINE\Software\Microsoft\I
  - RegistryKey - HKEY_CURRENT_USER\Software\Microsoft\
- 2o7 - 3rd Party Cookie
  - URL - Cookie:cti@2o7.net/
- Doubleclick - 3rd Party Cookie
  - URL - Cookie:cti@doubleclick.net/
- Fastclick - 3rd Party Cookie
  - URL - Cookie:cti@fastclick.net/

3 required elements were **not** found on your computer!

- Anti-Virus Software
  - Trend Micro OfficeScan no present al client
- Registro_restrictanonymous
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Conti
- GoogleTalk
  - GoogleTalk present

Scanner Status: Ready to Re-Scan



Virus Information Center

Get latest information on viruses, worms, Trojans, and hoaxes

SmartDefense Advisor N° de artículo 52 | La última actualización se realizó el 2005-08-26
AlexaToolbar
Browser Plugin (Tell me more)

- Search Virus Information Center
- Browse Virus Information Center
- Virus Glossary
- Zone Labs Security Advisories

Alexa Toolbar is a program that includes a pop-up manager (it blocks pop-ups), a web search function (powered by Google) and buttons that provide additional information, such as site information, and related sites. Alexa also sends information about all web pages you visit back to Alexa's servers. It includes both page URLs and data you sent to web sites as a part of URL.

¿Cómo se instala?

Alexa Toolbar comes bundled with other programs, which may include Windows XP, Internet Explorer 6.0. It can also be downloaded from Alexa's website and installed directly by someone with administrative access to your computer.

¿Cuál es su grado de peligrosidad?

Privacidad

Alexa Toolbar collects URLs that may contain personal information about a user such as name, address, phone, and e-mail address.

Seguridad

Your personal information may be transmitted over the internet insecurely.

¿Qué debo hacer?

If this application has been prohibited by the site administrator you must remove it from your computer before accessing the site. If it has not been prohibited, you may want to delete it because the program that has some potential [illegible] you, [illegible] it is categorized as adware, and may pose security and privacy issues.

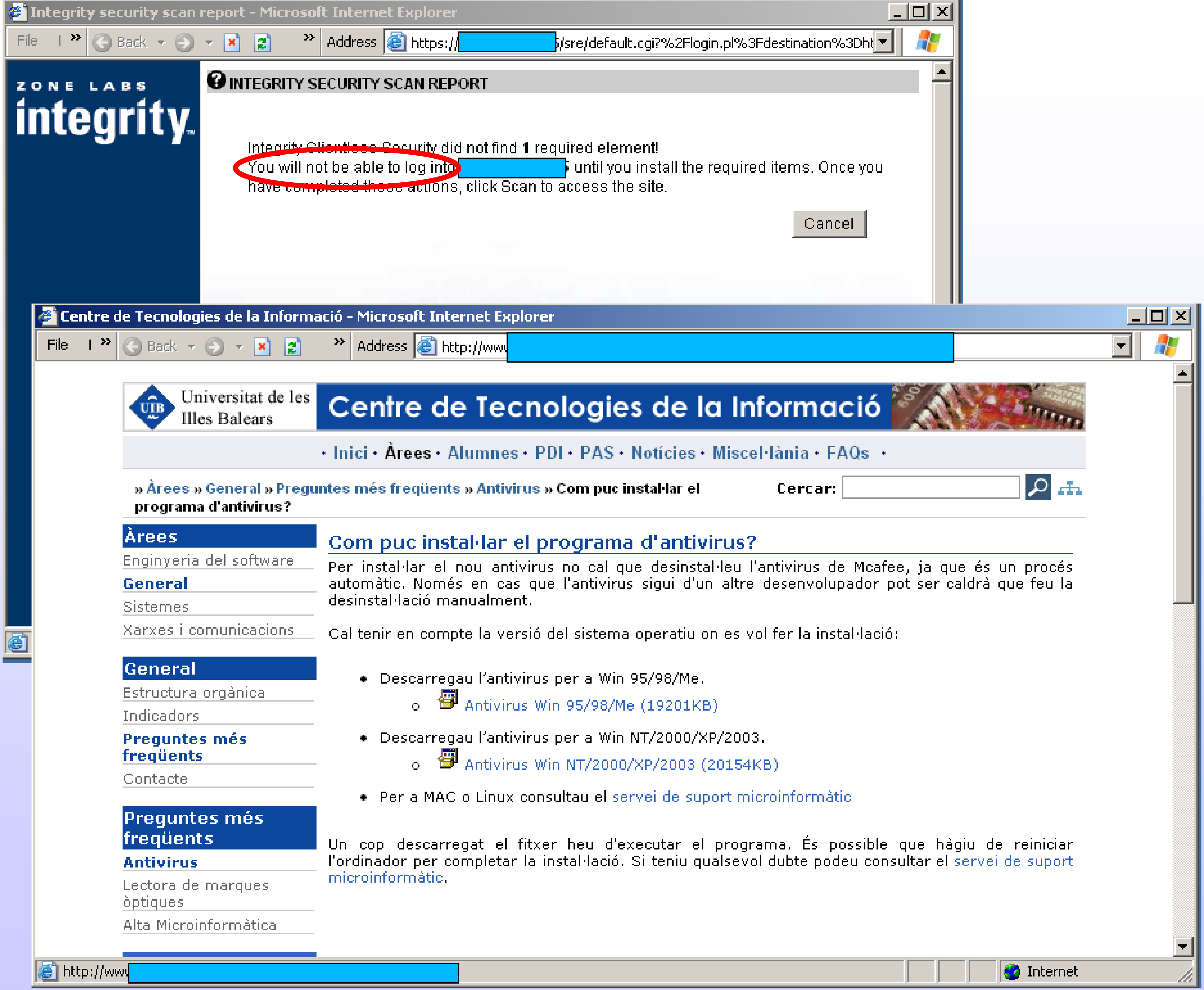
¿Cómo puedo eliminarlo?

Eliminación automática

If automatic removal is enabled, this program is automatically deleted from your computer.

Eliminación manual

Close Internet Explorer. Run Add/Remove applet from Control Panel and uninstall Alexa Toolbar. Verify that files AlxRes.dll and AlxTB1.dll do not exist in the SYSTEM folder. If case they exist unregister toolbar dlls by running regsvr32 /u AlxRes.dll regsvr32 /u AlxTB1.dll and delete them manually.



Integrity security scan report - Microsoft Internet Explorer
File
Back
Address

https://[redacted]/sre/default.cgi?%2Flogin.pl%3Fdestination%3Dht

INTEGRITY SECURITY SCAN REPORT

Integrity Clientless Security did not find 1 required element!
You will not be able to log into [redacted] until you install the required items. Once you have completed these actions, click Scan to access the site.

Cancel

Centre de Tecnologies de la Informació - Microsoft Internet Explorer
File
Back
Address

http://www[redacted]

UIB
Universitat de les Illes Balears

Centre de Tecnologies de la Informació

• Inici • Àrees • Alumnes • PDI • PAS • Notícies • Miscel·lània • FAQs •

» Àrees » General » Preguntes més freqüents » Antivirus » Com puc instal·lar el programa d'antivirus?

Cercar:

Àrees
Enginyeria del software
General
Sistemes
Xarxes i comunicacions

General
Estructura orgànica
Indicadors
Preguntes més freqüents
Contacte

Preguntes més freqüents
Antivirus
Lectora de marques òptiques
Alta Microinformàtica

Com puc instal·lar el programa d'antivirus?

Per instal·lar el nou antivirus no cal que desinstal·leu l'antivirus de Mcafee, ja que és un procés automàtic. Només en cas que l'antivirus sigui d'un altre desenvolupador pot ser caldrà que feu la desinstal·lació manualment.

Cal tenir en compte la versió del sistema operatiu on es vol fer la instal·lació:

- Descarregau l'antivirus per a Win 95/98/Me.
  - Antivirus Win 95/98/Me (19201KB)
- Descarregau l'antivirus per a Win NT/2000/XP/2003.
  - Antivirus Win NT/2000/XP/2003 (20154KB)
- Per a MAC o Linux consultau el servei de suport microinformàtic

Un cop descarregat el fitxer heu d'executar el programa. És possible que hàgiu de reiniciar l'ordinador per completar la instal·lació. Si teniu qualsevol dubte podeu consultar el servei de suport microinformàtic.

http://www[redacted]

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Mantenimiento de la red

- ¿Funciona la wifi en todos los edificios?
  - Localización de usuarios activos
  - Robots APs: Linksys con Linux
    - http://www.linksysinfo.org/index.php
    - http://toys.lerdorf.com/archives/20-Kismet-on-the-Linksys-WRT54G.html
    - Monitorización de una red Wi-Fi autenticada mediante robots
      - Ramón Bayán (UOC) , Logroño JT2005
- ¿Están bien configurados mis APs?
  - Automatización de configuraciones para eventos
  - Comparación de configuraciones según plantillas

Mantenimiento

- ¿Están actualizados todos mis elementos de red?
- Bugs y workarounds… impresionantes!!
  - El control de ancho de banda aplicada sobre el perfil de usuario "no registrado" se aplica también a los usuarios autenticados mediante VPN-PPTP
  - Si un usuario bloqueado por el IDS deja de enviar el tráfico malicioso durante un tiempo, la gestión del equipo indica que está liberado pero realmente sigue bloqueado
  - Todos los servidores Radius definidos en el AP comparten la misma shared-secret
  - La longitud de la shared-secret = 16carácteres sino se envia un texto aleatorio...

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

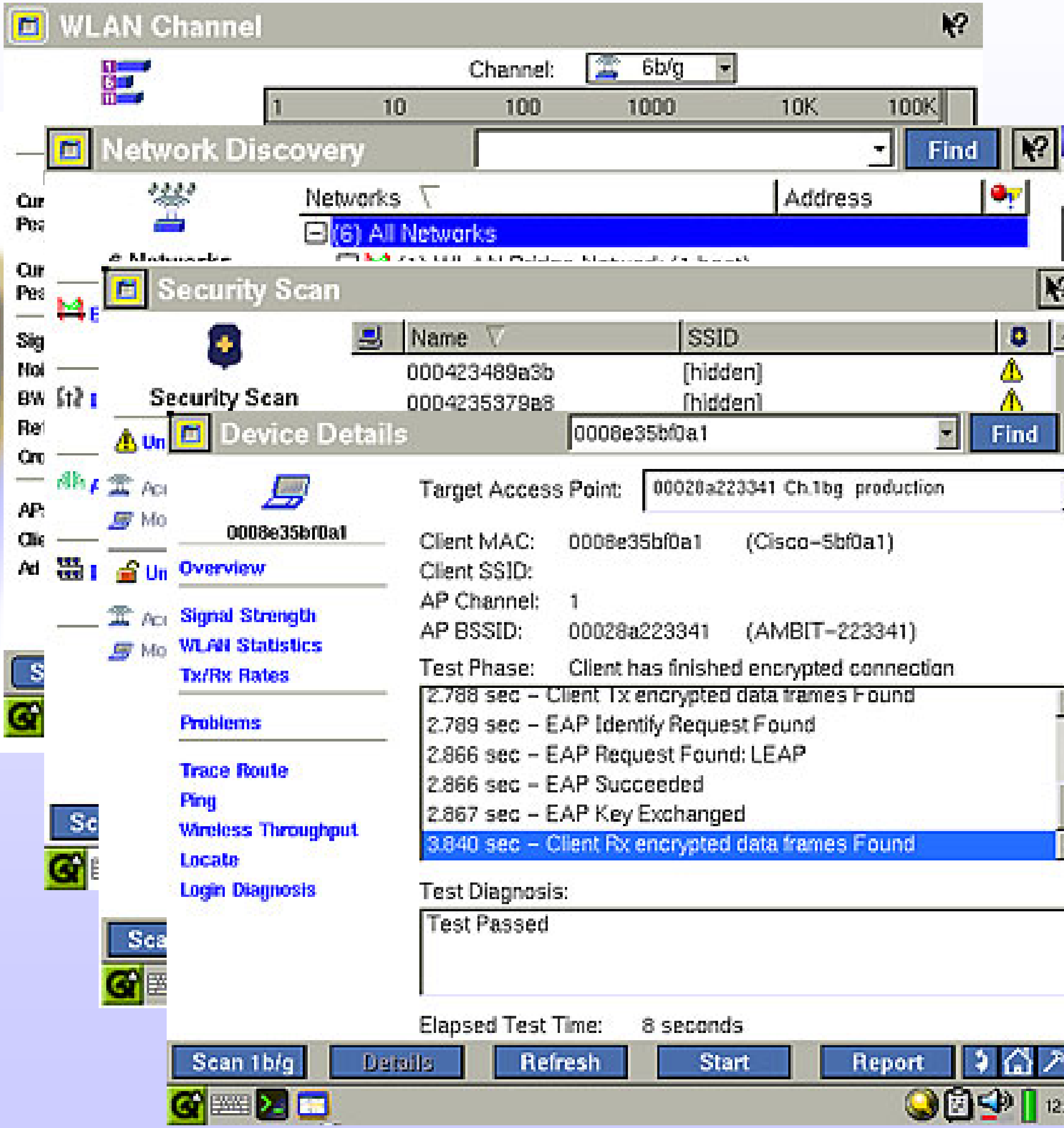
Monitorización y securización

- ¿Qué está pasando en mi red wifi?
  - Capturar en modo monitor/pasivo
- Puntos de acceso Rogue
  - Usuarios bien intencionados: Que baratos son los APs!!
  - Usuarios maliciosos: Suplantación de SSID y servicios.

Agenda

- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Fluke



Channel: 6b/g

1 10 100 1000 10K 100K

Name	SSID
000423489a3b	[hidden]
0004235379a8	[hidden]

0008e35bf0a1

Target Access Point: 00028a223341 Ch.1bg production

Client MAC: 0008e35bf0a1 (Cisco-5bf0a1)
Client SSID:
AP Channel: 1
AP BSSID: 00028a223341 (AMBIT-223341)
Test Phase: Client has finished encrypted connection

```
2.788 sec – Client Tx encrypted data frames Found
2.789 sec – EAP Identify Request Found
2.866 sec – EAP Request Found: LEAP
2.866 sec – EAP Succeeded
2.867 sec – EAP Key Exchanged
3.840 sec – Client Rx encrypted data frames Found
```

Test Diagnosis:
Test Passed

Elapsed Test Time: 8 seconds

Herramientas

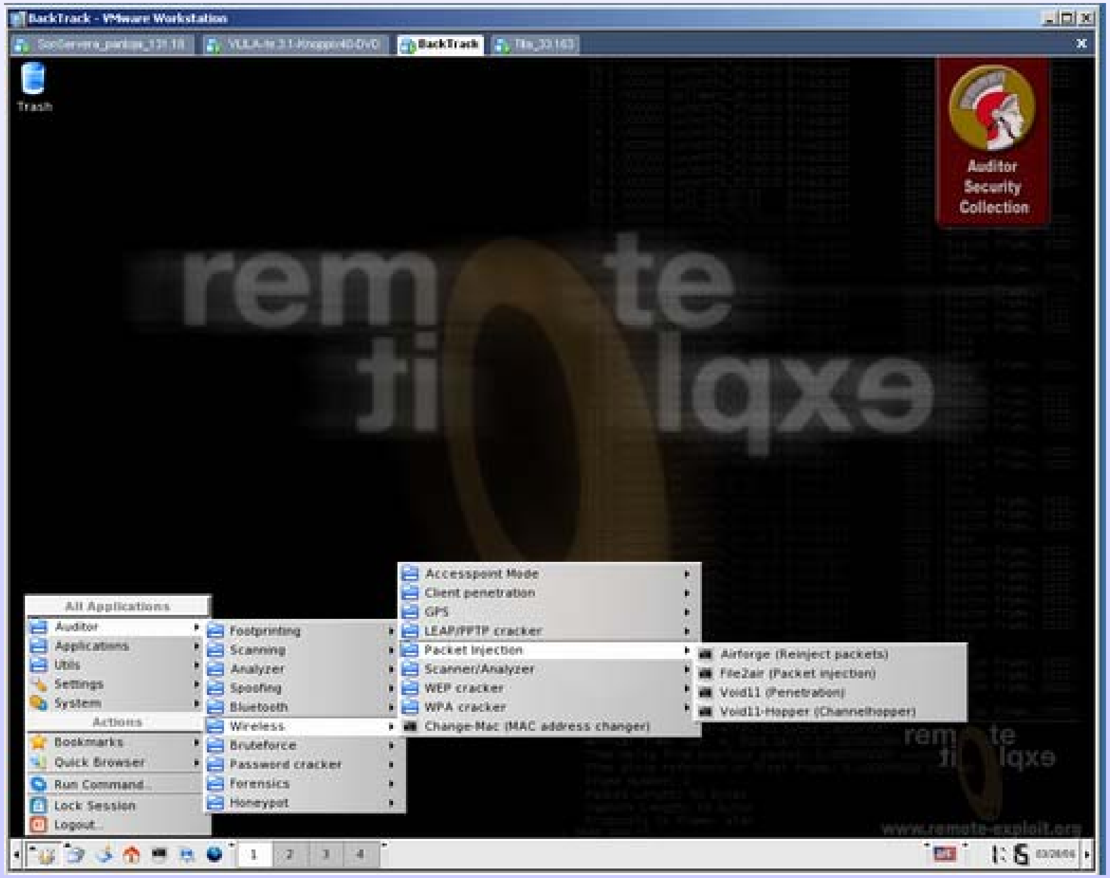
- Sistemas Linux: la importancia del RFMon
  - Live CDs
  - Iwconfig
  - Ethereal
  - Kismet y gpsmap
  - Nessus
- Sistemas Windows: RFMon el problema…
  - Netstumbler
  - Airopeek

Knoppix

- http://www.knoppix.org/
  - Debian
  - 8 GB de software instalado (DVD 4 GB)

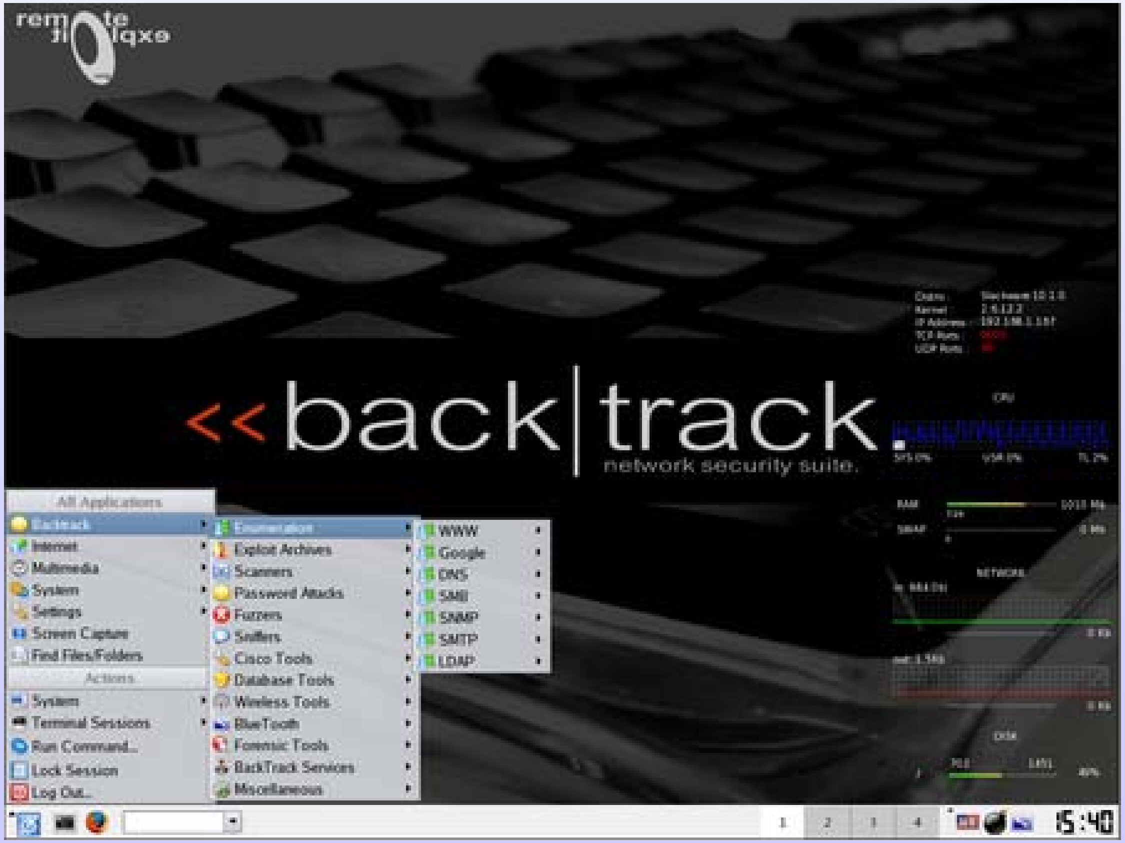
Auditor

- http://www.remote-exploit.org/index.php/Auditor_main
  - Basado en Knoppix
  - Herramientas de seguridad



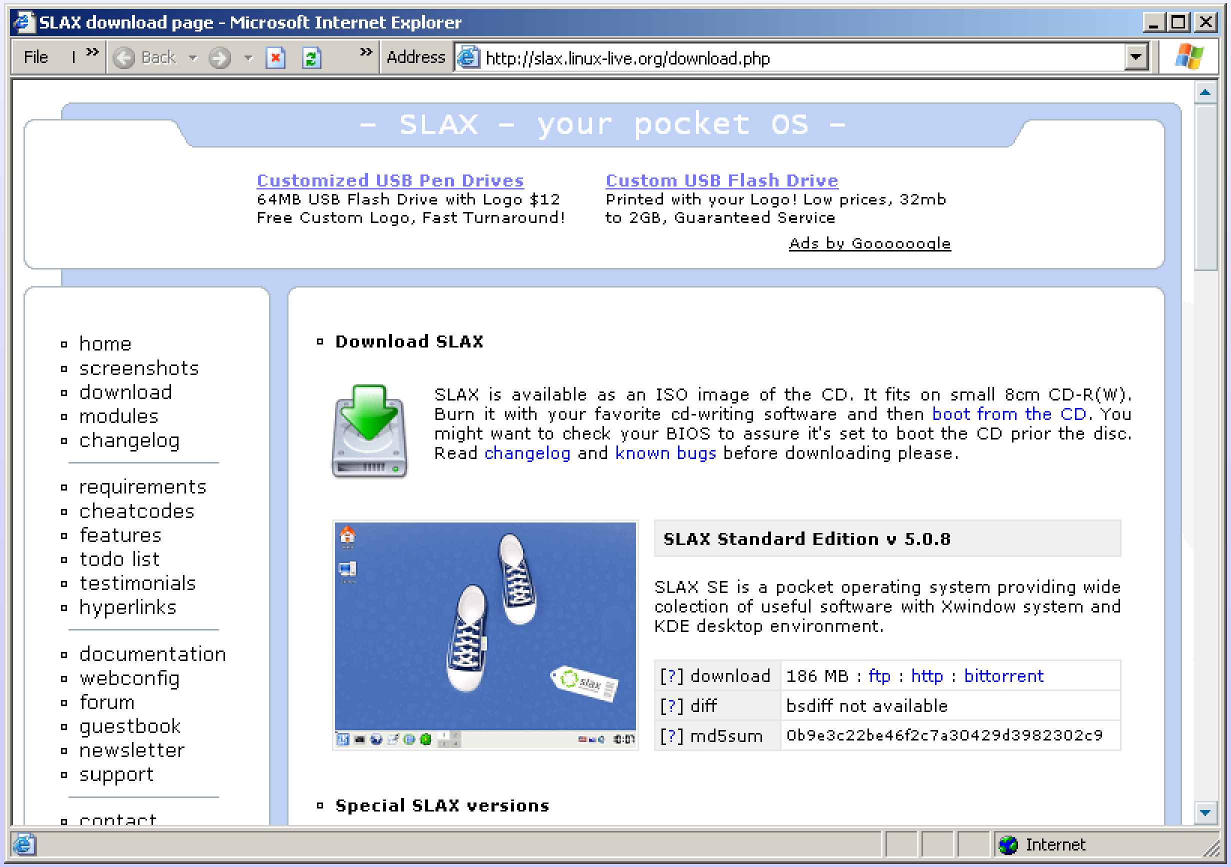
BackTrack

- http://www.remote-exploit.org/index.php/BackTrack
  - Basada en SLAX



SLAX

- http://slax.linux-live.org
  - Basado en Slackware
  - Crear tu propia live cd...


SLAX download page - Microsoft Internet Explorer
File
Back
Address
http://slax.linux-live.org/download.php
Internet

- SLAX - your pocket OS -

Customized USB Pen Drives
64MB USB Flash Drive with Logo $12
Free Custom Logo, Fast Turnaround!

Custom USB Flash Drive
Printed with your Logo! Low prices, 32mb
to 2GB, Guaranteed Service

Ads by Goooooogle

- home
- screenshots
- download
- modules
- changelog
- requirements
- cheatcodes
- features
- todo list
- testimonials
- hyperlinks
- documentation
- webconfig
- forum
- guestbook
- newsletter
- support
- contact

Download SLAX

SLAX is available as an ISO image of the CD. It fits on small 8cm CD-R(W). Burn it with your favorite cd-writing software and then boot from the CD. You might want to check your BIOS to assure it's set to boot the CD prior the disc. Read changelog and known bugs before downloading please.

SLAX Standard Edition v 5.0.8

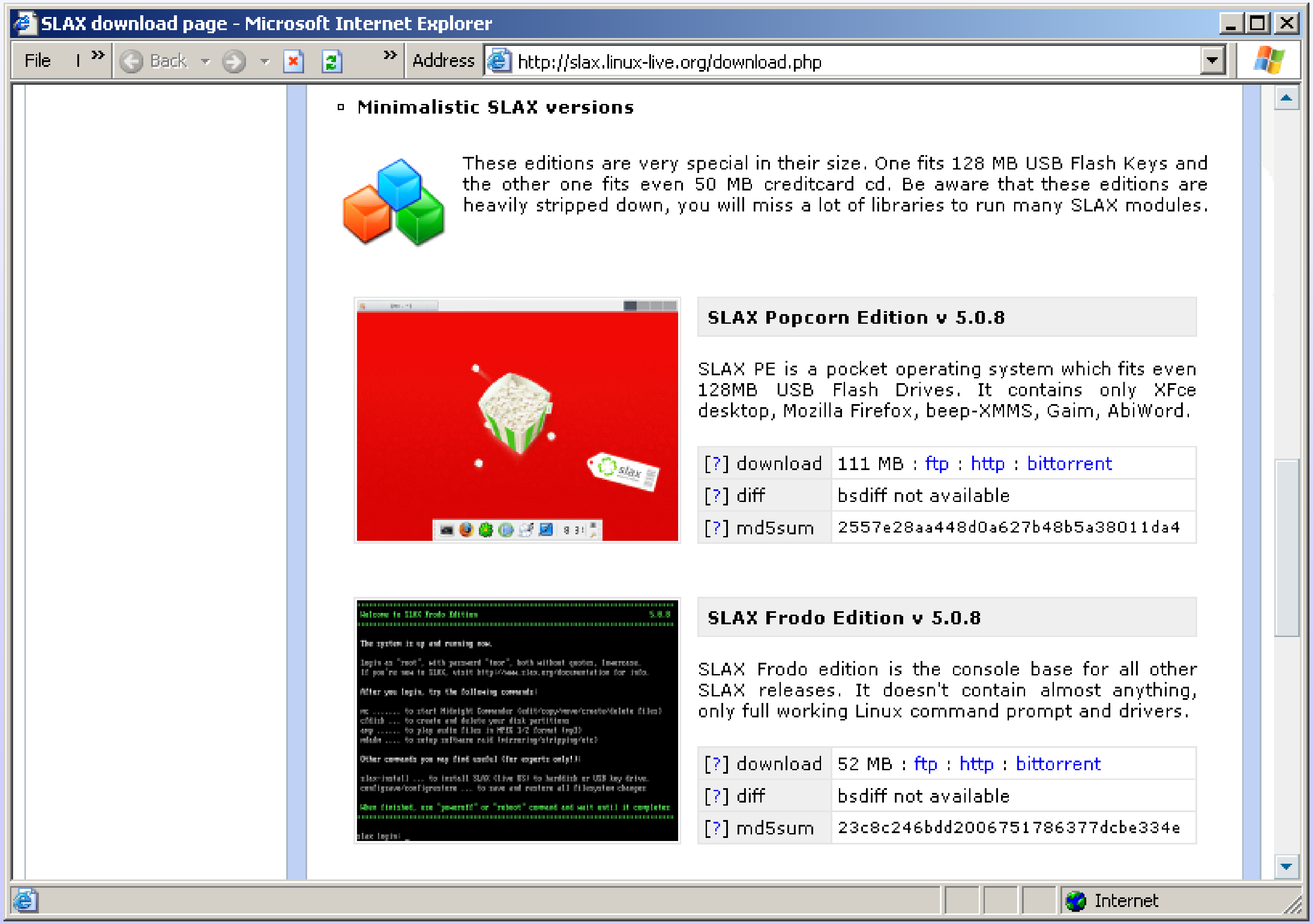
SLAX SE is a pocket operating system providing wide colection of useful software with Xwindow system and KDE desktop environment.

[?] download	186 MB : ftp : http : bittorrent
[?] diff	bsdiff not available
[?] md5sum	0b9e3c22be46f2c7a30429d3982302c9

Special SLAX versions

SLAX

- Versiones básicas: 111MB y 52MB



SLAX download page - Microsoft Internet Explorer

- Minimalistic SLAX versions

These editions are very special in their size. One fits 128 MB USB Flash Keys and the other one fits even 50 MB creditcard cd. Be aware that these editions are heavily stripped down, you will miss a lot of libraries to run many SLAX modules.

SLAX Popcorn Edition v 5.0.8

SLAX PE is a pocket operating system which fits even 128MB USB Flash Drives. It contains only XFce desktop, Mozilla Firefox, beep-XMMS, Gaim, AbiWord.

[?] download	111 MB : ftp : http : bittorrent
[?] diff	bsdiff not available
[?] md5sum	2557e28aa448d0a627b48b5a38011da4

SLAX Frodo Edition v 5.0.8

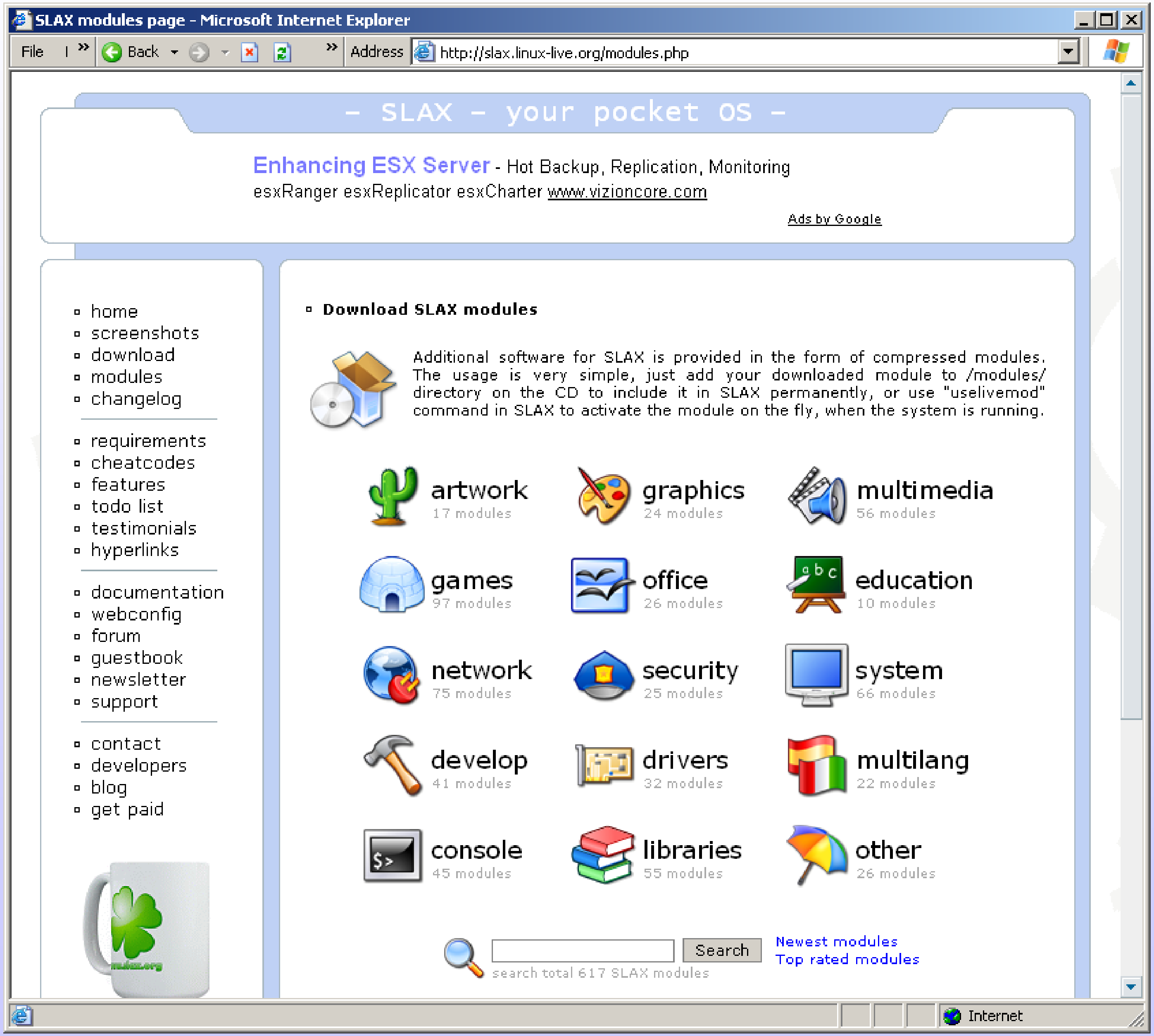
```
Welcome to SLAX Frodo Edition                                    5.0.8

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.
If you're new to SLAX, visit http://www.slax.org/documentation for info.

After you login, try the following commands:

mc ........ to start Midnight Commander (edit/copy/move/create/delete files)
cfdisk .... to create and delete your disk partitions
amp ....... to play audio files in MPEG 1/2 format (mp3)
mdadm ..... to setup software raid (mirroring/stripping/etc)

Other commands you may find useful (for experts only!):

slax-install ... to install SLAX (Live OS) to harddisk or USB key drive.
configsave/configrestore ... to save and restore all filesystem changes

When finished, use "poweroff" or "reboot" command and wait until it completes

slax login: _
```

SLAX Frodo edition is the console base for all other SLAX releases. It doesn't contain almost anything, only full working Linux command prompt and drivers.

[?] download	52 MB : ftp : http : bittorrent
[?] diff	bsdiff not available
[?] md5sum	23c8c246bdd2006751786377dcbe334e

SLAX

- Módulos


SLAX modules page - Microsoft Internet Explorer
File
Back
Address
http://slax.linux-live.org/modules.php
Internet

- SLAX - your pocket OS -

- home
- screenshots
- download
- modules
- changelog

- requirements
- cheatcodes
- features
- todo list
- testimonials
- hyperlinks

- documentation
- webconfig
- forum
- guestbook
- newsletter
- support

- contact
- developers
- blog
- get paid

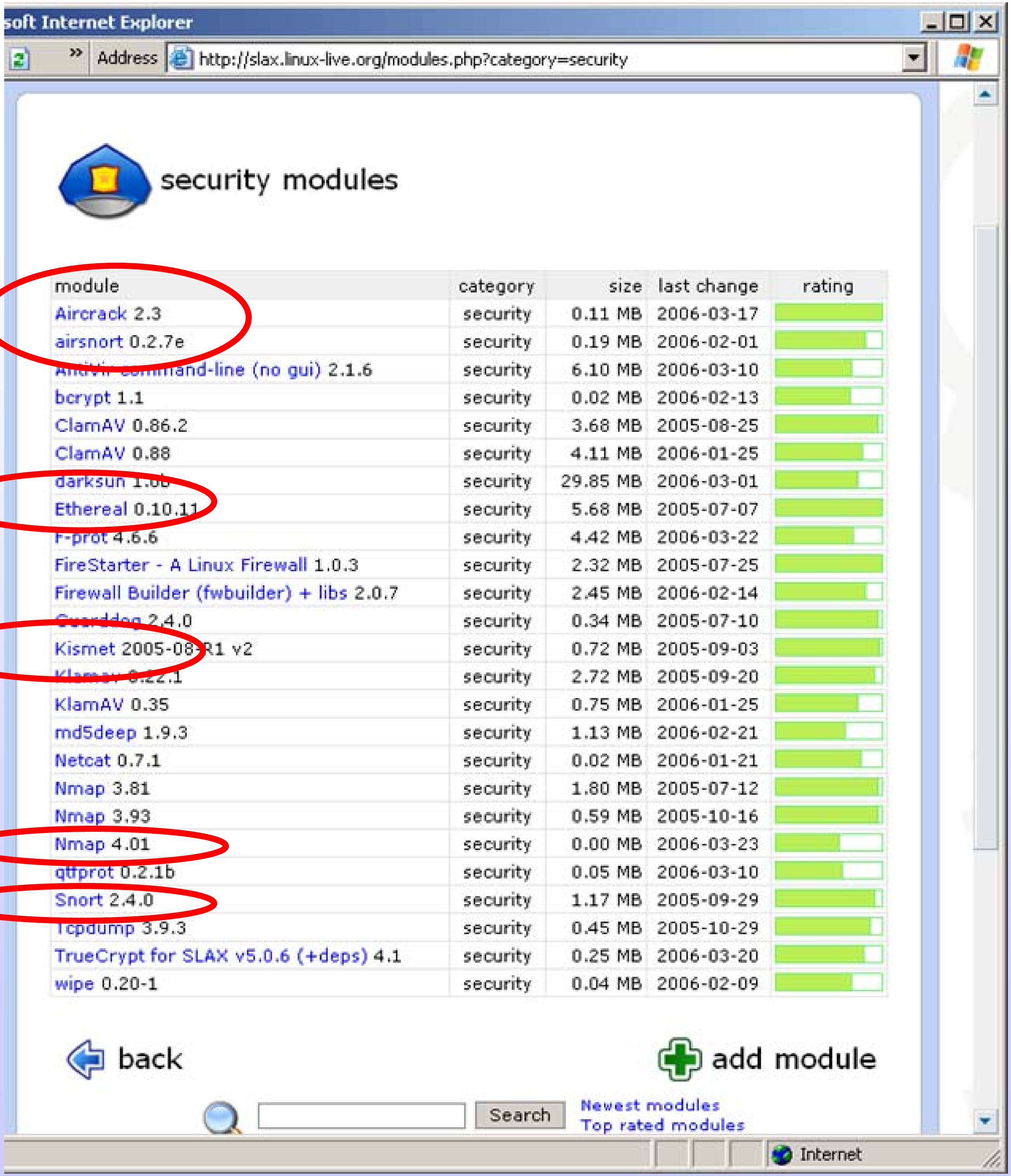
- **Download SLAX modules**

Additional software for SLAX is provided in the form of compressed modules. The usage is very simple, just add your downloaded module to /modules/ directory on the CD to include it in SLAX permanently, or use "uselivemod" command in SLAX to activate the module on the fly, when the system is running.

artwork 17 modules	graphics 24 modules	multimedia 56 modules
games 97 modules	office 26 modules	education 10 modules
network 75 modules	security 25 modules	system 66 modules
develop 41 modules	drivers 32 modules	multilang 22 modules
console 45 modules	libraries 55 modules	other 26 modules

Search
search total 617 SLAX modules
Newest modules
Top rated modules

- Seguridad

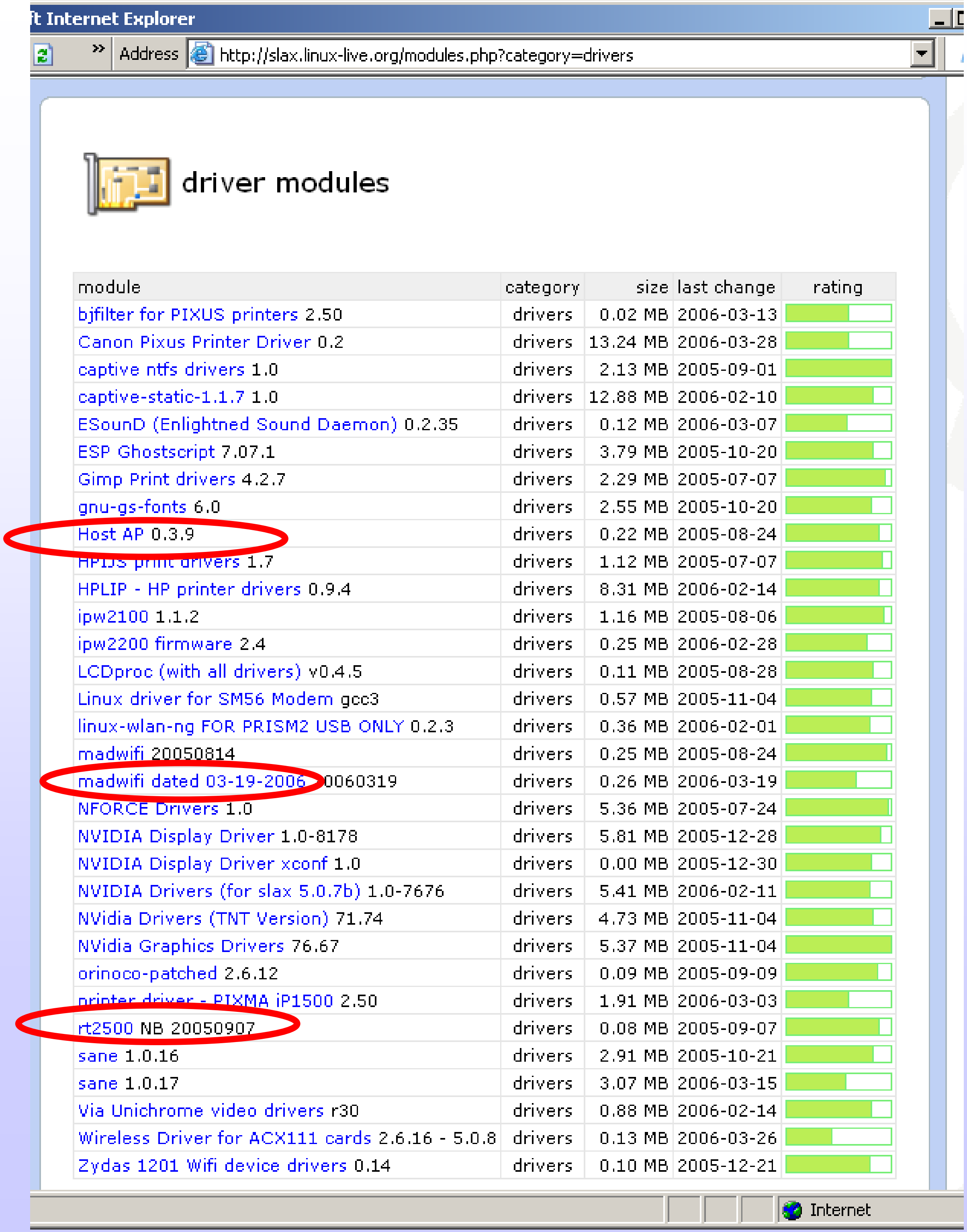


soft Internet Explorer
Address http://slax.linux-live.org/modules.php?category=security

security modules

module	category	size	last change	rating
Aircrack 2.3	security	0.11 MB	2006-03-17	🟩
airsnort 0.2.7e	security	0.19 MB	2006-02-01	🟩
AntiVir command-line (no gui) 2.1.6	security	6.10 MB	2006-03-10	🟩
bcrypt 1.1	security	0.02 MB	2006-02-13	🟩
ClamAV 0.86.2	security	3.68 MB	2005-08-25	🟩
ClamAV 0.88	security	4.11 MB	2006-01-25	🟩
darksun 1.0b	security	29.85 MB	2006-03-01	🟩
Ethereal 0.10.11	security	5.68 MB	2005-07-07	🟩
F-prot 4.6.6	security	4.42 MB	2006-03-22	🟩
FireStarter - A Linux Firewall 1.0.3	security	2.32 MB	2005-07-25	🟩
Firewall Builder (fwbuilder) + libs 2.0.7	security	2.45 MB	2006-02-14	🟩
Guarddog 2.4.0	security	0.34 MB	2005-07-10	🟩
Kismet 2005-08-R1 v2	security	0.72 MB	2005-09-03	🟩
Klamav 0.22.1	security	2.72 MB	2005-09-20	🟩
KlamAV 0.35	security	0.75 MB	2006-01-25	🟩
md5deep 1.9.3	security	1.13 MB	2006-02-21	🟩
Netcat 0.7.1	security	0.02 MB	2006-01-21	🟩
Nmap 3.81	security	1.80 MB	2005-07-12	🟩
Nmap 3.93	security	0.59 MB	2005-10-16	🟩
Nmap 4.01	security	0.00 MB	2006-03-23	🟩
qtfprot 0.2.1b	security	0.05 MB	2006-03-10	🟩
Snort 2.4.0	security	1.17 MB	2005-09-29	🟩
Tcpdump 3.9.3	security	0.45 MB	2005-10-29	🟩
TrueCrypt for SLAX v5.0.6 (+deps) 4.1	security	0.25 MB	2006-03-20	🟩
wipe 0.20-1	security	0.04 MB	2006-02-09	🟩

- Drivers



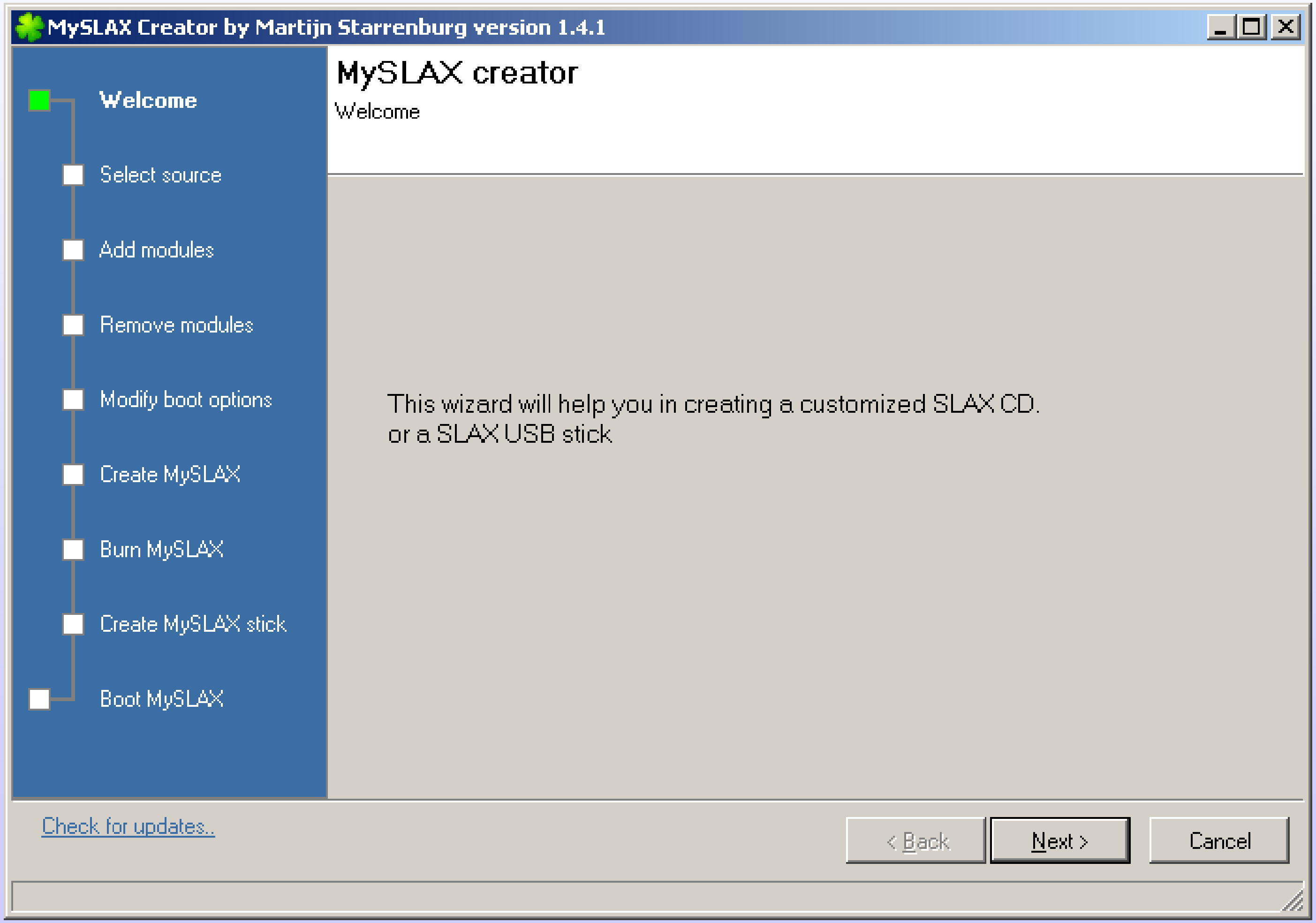
ft Internet Explorer
Address http://slax.linux-live.org/modules.php?category=drivers
Internet

driver modules

module	category	size	last change	rating
bjfilter for PIXUS printers 2.50	drivers	0.02 MB	2006-03-13	
Canon Pixus Printer Driver 0.2	drivers	13.24 MB	2006-03-28	
captive ntfs drivers 1.0	drivers	2.13 MB	2005-09-01	
captive-static-1.1.7 1.0	drivers	12.88 MB	2006-02-10	
ESounD (Enlightned Sound Daemon) 0.2.35	drivers	0.12 MB	2006-03-07	
ESP Ghostscript 7.07.1	drivers	3.79 MB	2005-10-20	
Gimp Print drivers 4.2.7	drivers	2.29 MB	2005-07-07	
gnu-gs-fonts 6.0	drivers	2.55 MB	2005-10-20	
Host AP 0.3.9	drivers	0.22 MB	2005-08-24	
HPIJS print drivers 1.7	drivers	1.12 MB	2005-07-07	
HPLIP - HP printer drivers 0.9.4	drivers	8.31 MB	2006-02-14	
ipw2100 1.1.2	drivers	1.16 MB	2005-08-06	
ipw2200 firmware 2.4	drivers	0.25 MB	2006-02-28	
LCDproc (with all drivers) v0.4.5	drivers	0.11 MB	2005-08-28	
Linux driver for SM56 Modem gcc3	drivers	0.57 MB	2005-11-04	
linux-wlan-ng FOR PRISM2 USB ONLY 0.2.3	drivers	0.36 MB	2006-02-01	
madwifi 20050814	drivers	0.25 MB	2005-08-24	
madwifi dated 03-19-2006 0060319	drivers	0.26 MB	2006-03-19	
NFORCE Drivers 1.0	drivers	5.36 MB	2005-07-24	
NVIDIA Display Driver 1.0-8178	drivers	5.81 MB	2005-12-28	
NVIDIA Display Driver xconf 1.0	drivers	0.00 MB	2005-12-30	
NVIDIA Drivers (for slax 5.0.7b) 1.0-7676	drivers	5.41 MB	2006-02-11	
NVidia Drivers (TNT Version) 71.74	drivers	4.73 MB	2005-11-04	
NVidia Graphics Drivers 76.67	drivers	5.37 MB	2005-11-04	
orinoco-patched 2.6.12	drivers	0.09 MB	2005-09-09	
printer driver - PIXMA iP1500 2.50	drivers	1.91 MB	2006-03-03	
rt2500 NB 20050907	drivers	0.08 MB	2005-09-07	
sane 1.0.16	drivers	2.91 MB	2005-10-21	
sane 1.0.17	drivers	3.07 MB	2006-03-15	
Via Unichrome video drivers r30	drivers	0.88 MB	2006-02-14	
Wireless Driver for ACX111 cards 2.6.16 - 5.0.8	drivers	0.13 MB	2006-03-26	
Zydas 1201 Wifi device drivers 0.14	drivers	0.10 MB	2005-12-21	

MySLAX

- http://myslax.bonsonno.org/



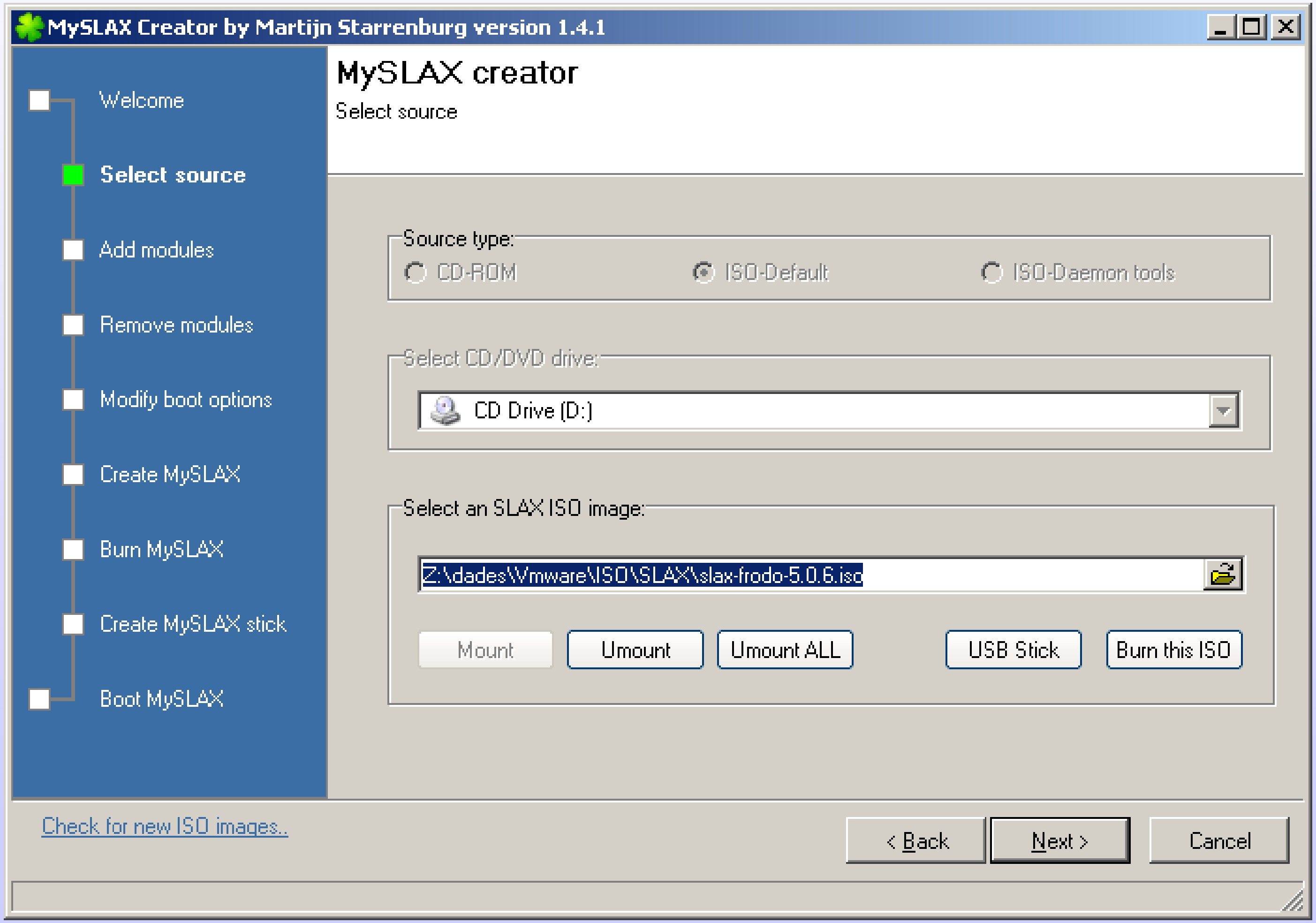
MySLAX creator

Welcome

This wizard will help you in creating a customized SLAX CD.
or a SLAX USB stick

MySLAX

- Montar una ISO


MySLAX Creator by Martijn Starrenburg version 1.4.1

MySLAX creator
Select source

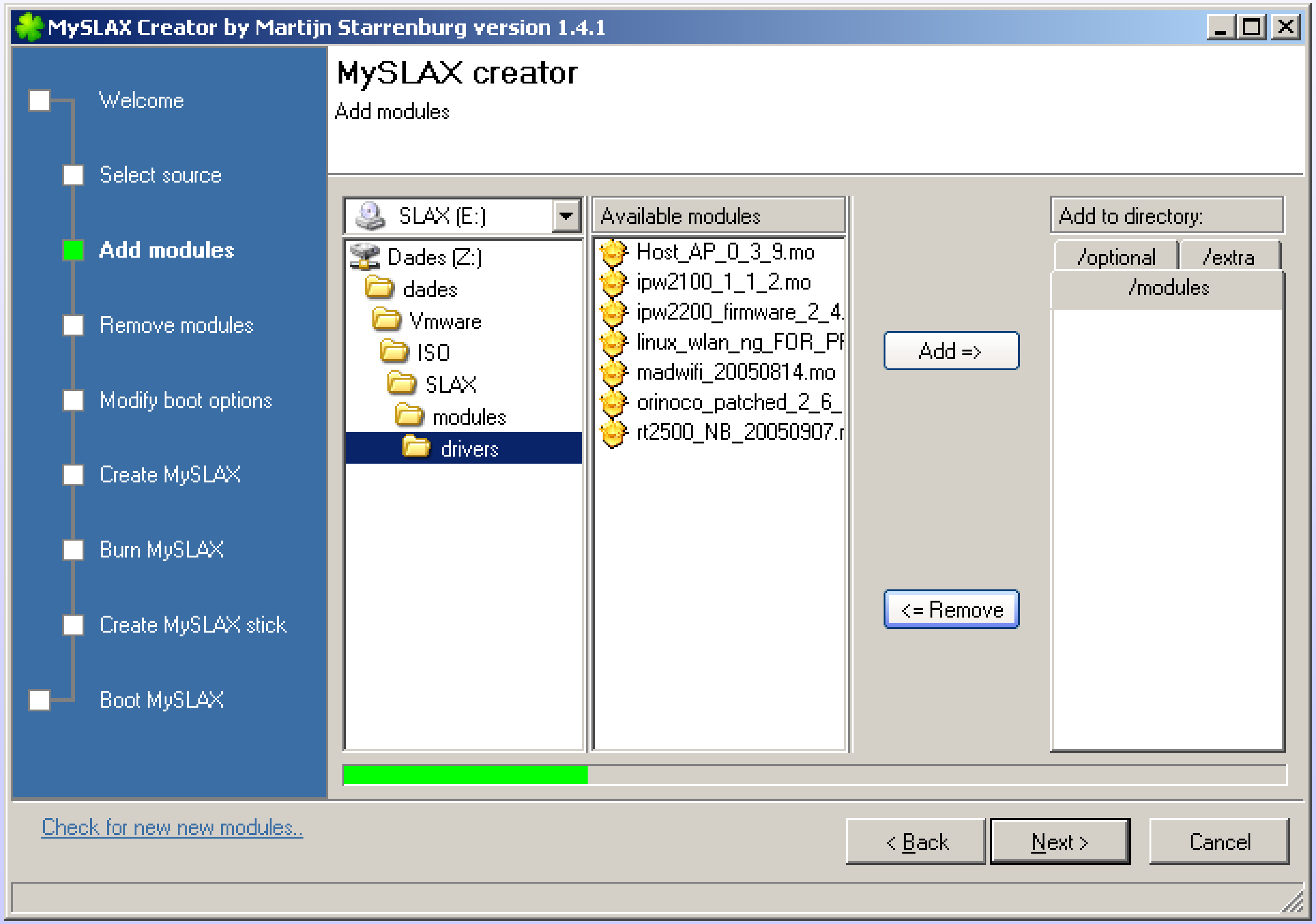
Source type:
○ CD-ROM ● ISO-Default ○ ISO-Daemon tools

Select CD/DVD drive: CD Drive (D:)

Select an SLAX ISO image: Z:\dades\Vmware\ISO\SLAX\slax-frodo-5.0.6.iso

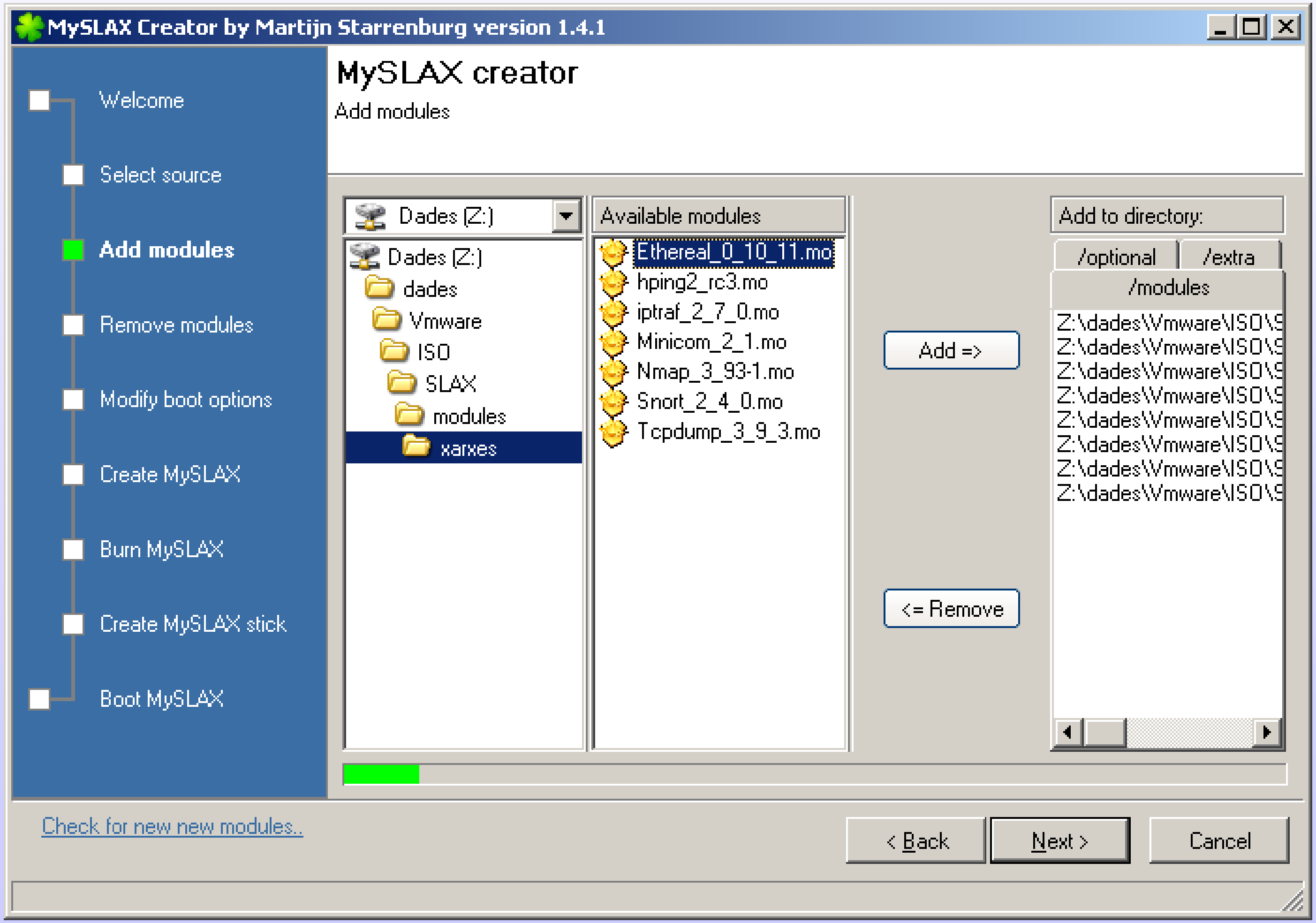
MySLAX

- Añadir módulos: Drivers



MySLAX

- Network utils: Ethereal, Nmap, Snort ...



MySLAX Creator by Martijn Starrenburg version 1.4.1

MySLAX creator

Add modules

Dades (Z:)
- dades
  - Vmware
    - ISO
      - SLAX
        - modules
          - xarxes

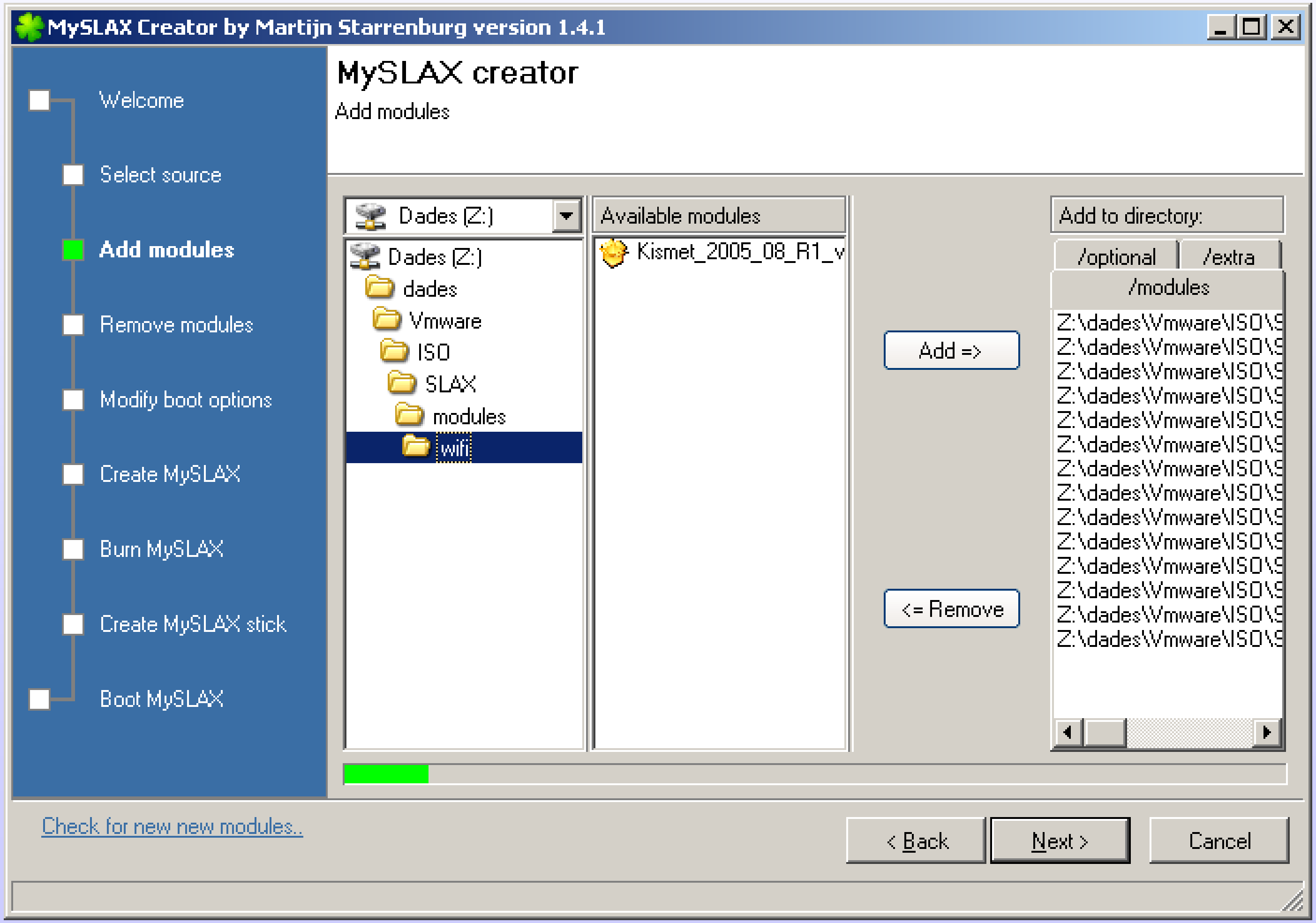
Available modules
- Ethereal_0_10_11.mo
- hping2_rc3.mo
- iptraf_2_7_0.mo
- Minicom_2_1.mo
- Nmap_3_93-1.mo
- Snort_2_4_0.mo
- Tcpdump_3_9_3.mo

Add to directory: /optional /extra /modules

```
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
```

MySLAX

- Kismet!!



MySLAX Creator by Martijn Starrenburg version 1.4.1

MySLAX creator
Add modules

Dades (Z:)

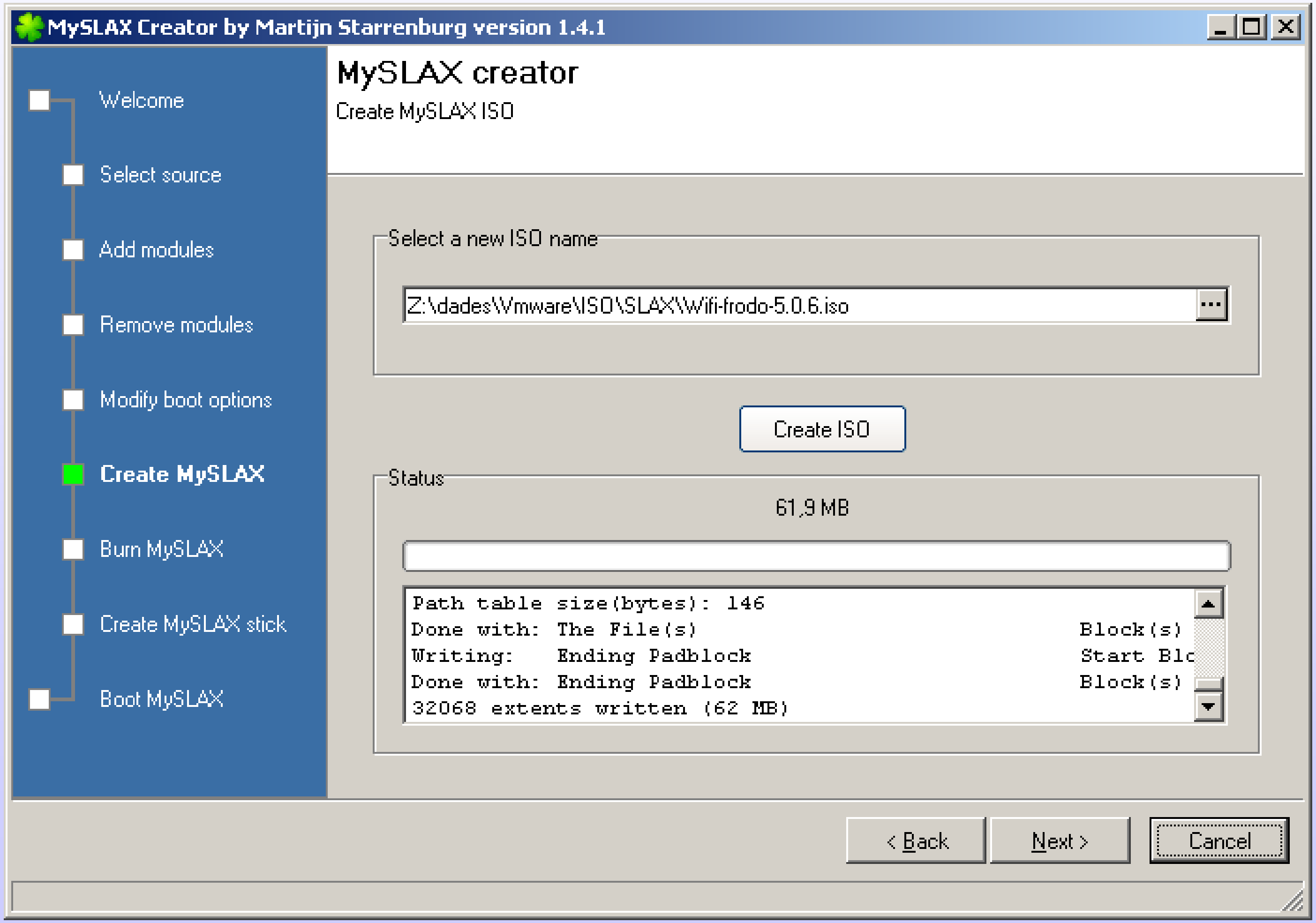
Available modules: Kismet_2005_08_R1_v

Add to directory: /modules

```
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
Z:\dades\Vmware\ISO\S
```

MySLAX

- Creamos la ISO...



Select a new ISO name

Z:\dades\Vmware\ISO\SLAX\Wifi-frodo-5.0.6.iso

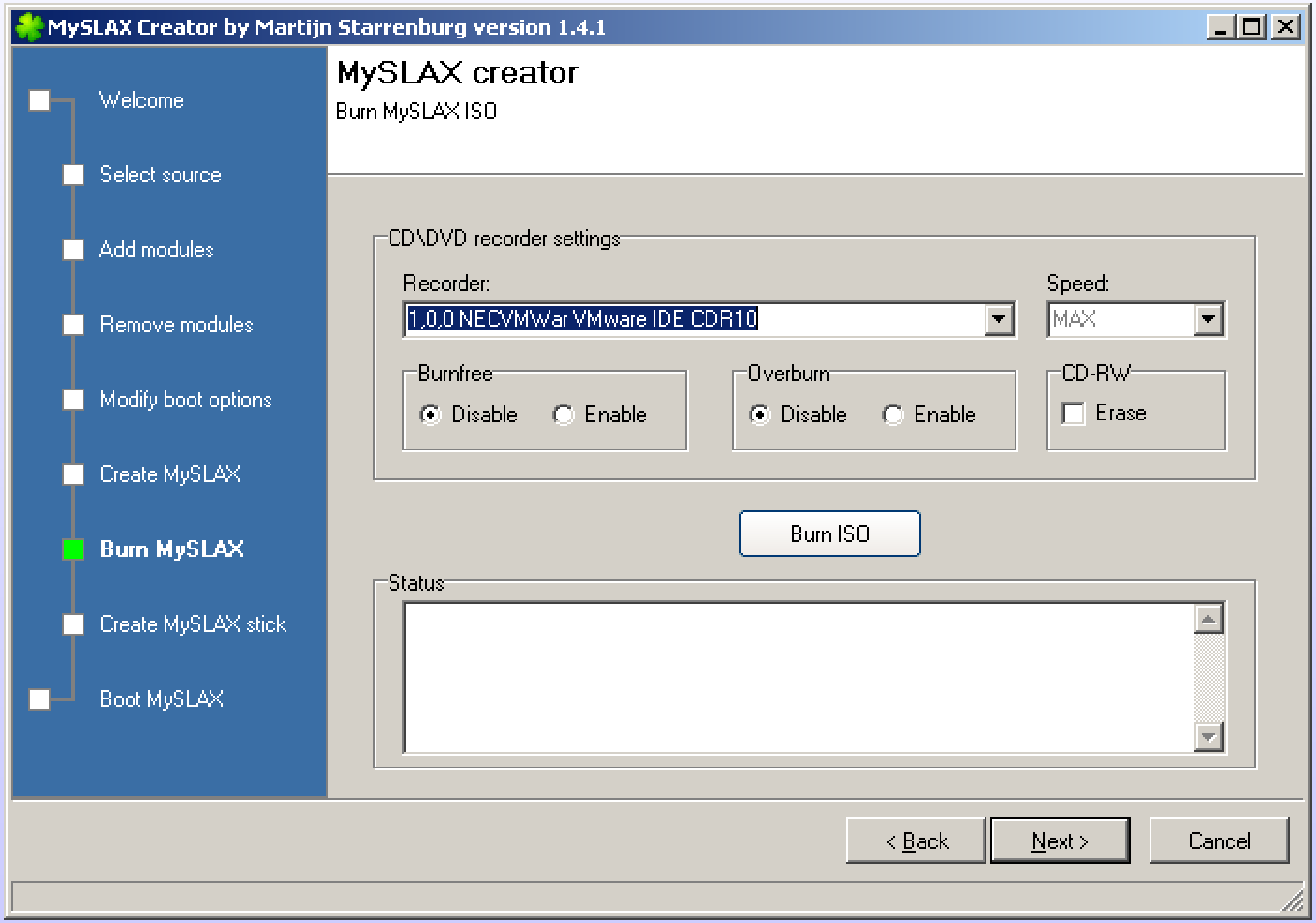
Status

61,9 MB

```
Path table size(bytes): 146
Done with:  The File(s)                              Block(s)
Writing:    Ending Padblock                          Start Blc
Done with:  Ending Padblock                          Block(s)
32068 extents written (62 MB)
```

MySLAX

- Grabamos un CD...



MySLAX Creator by Martijn Starrenburg version 1.4.1

MySLAX creator

Burn MySLAX ISO

CD\DVD recorder settings

Recorder: 1,0,0 NECVMWar VMware IDE CDR10

Speed: MAX

Burnfree: ● Disable ○ Enable

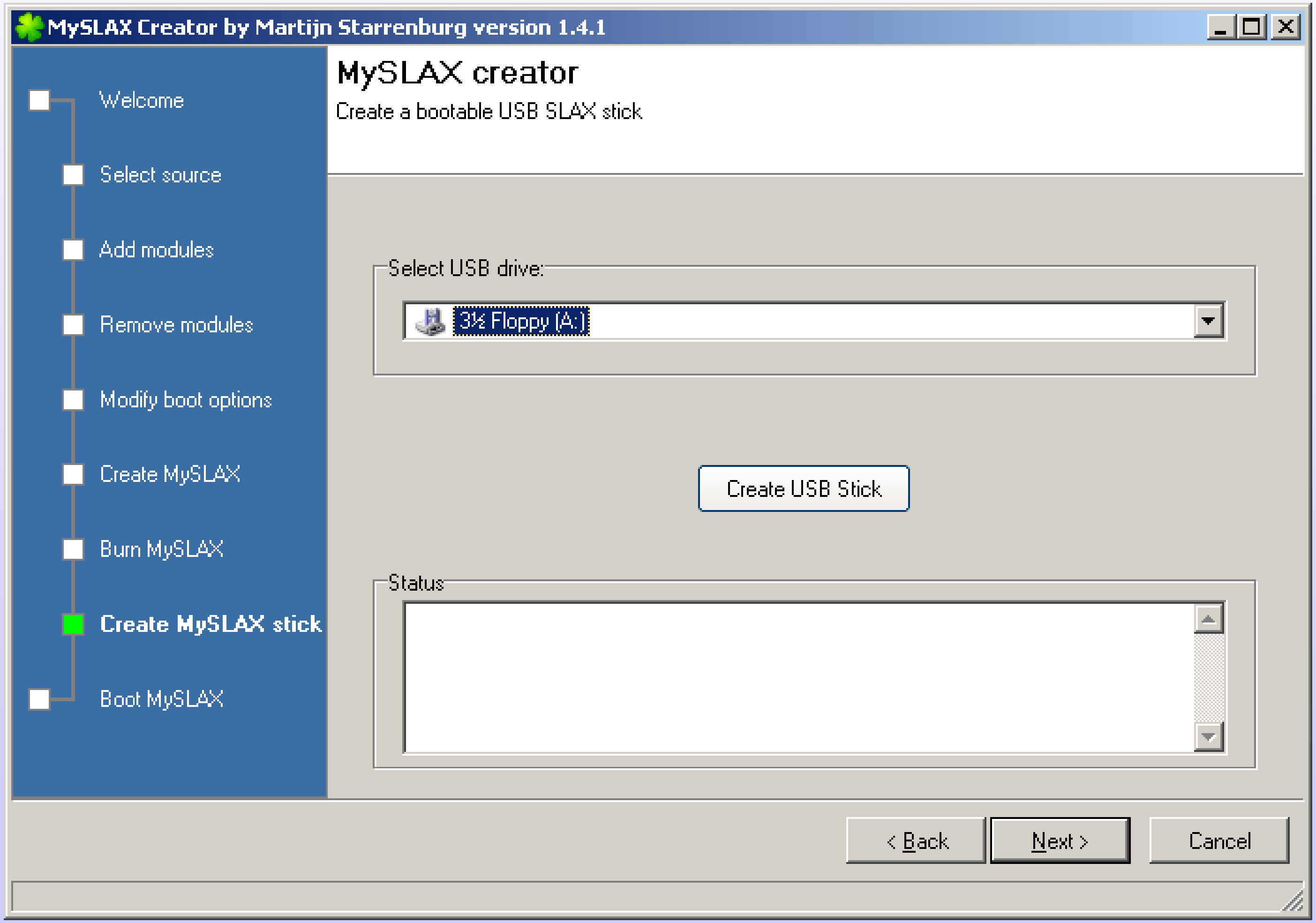
Overburn: ● Disable ○ Enable

CD-RW: □ Erase

Status

MySLAX

- Grabamos una llave USB...



MySLAX Creator by Martijn Starrenburg version 1.4.1

MySLAX creator

Create a bootable USB SLAX stick

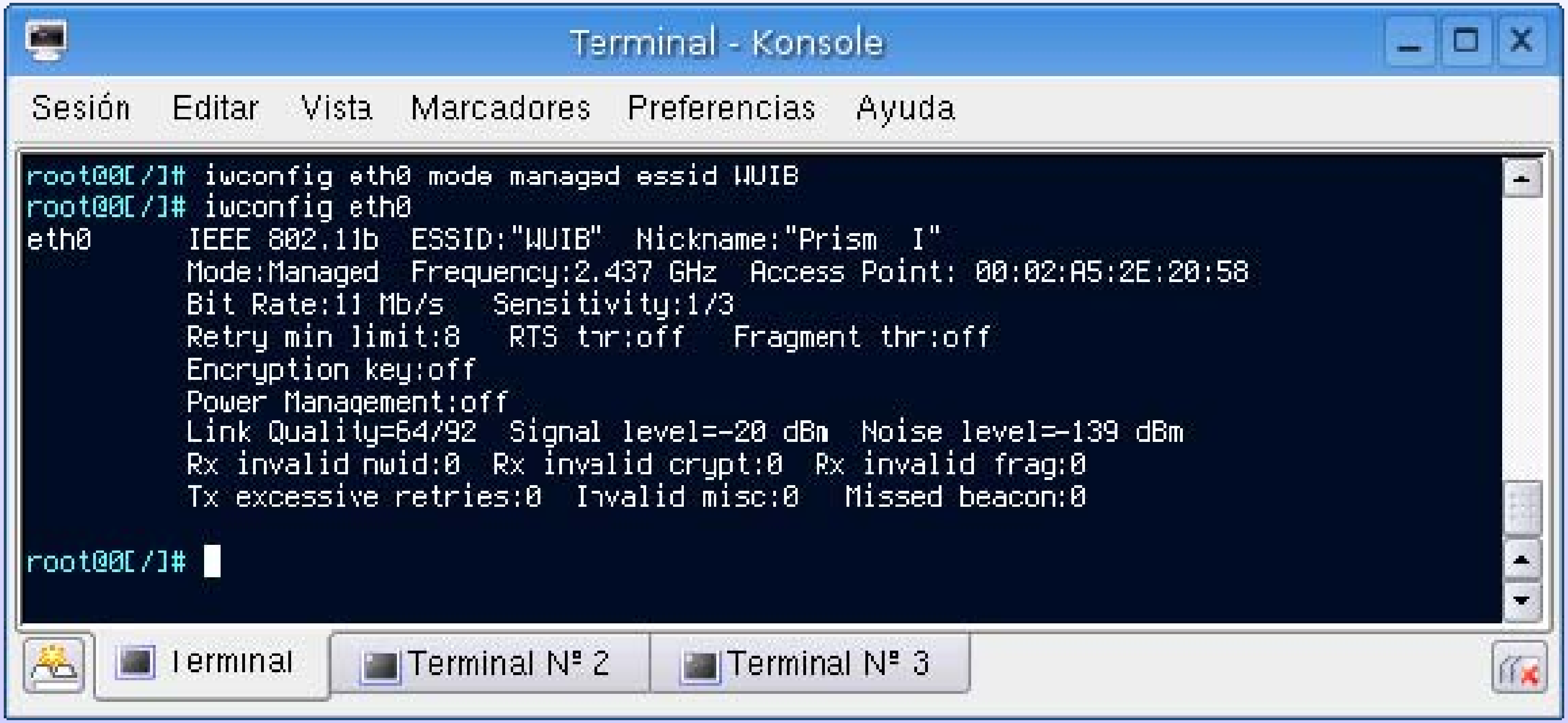
Select USB drive: 3½ Floppy (A:)

Wireless-tools

- iwconfig: Configuración wifi en linux: wireless-tools
  - mode = [ad-hoc,managed,master,monitor]
  - essid: Indica el SSID de la red (ANY para cualquiera)
  - freq/channel: configura el canal
  - key: para WEP
- iwlist: Ofrece información sobre la interfaz
  - freq/channel: canales que soporta
  - scan: lista los APs o Ad-hoc cercanos
- iwpriv: Configura parámetros opcionales

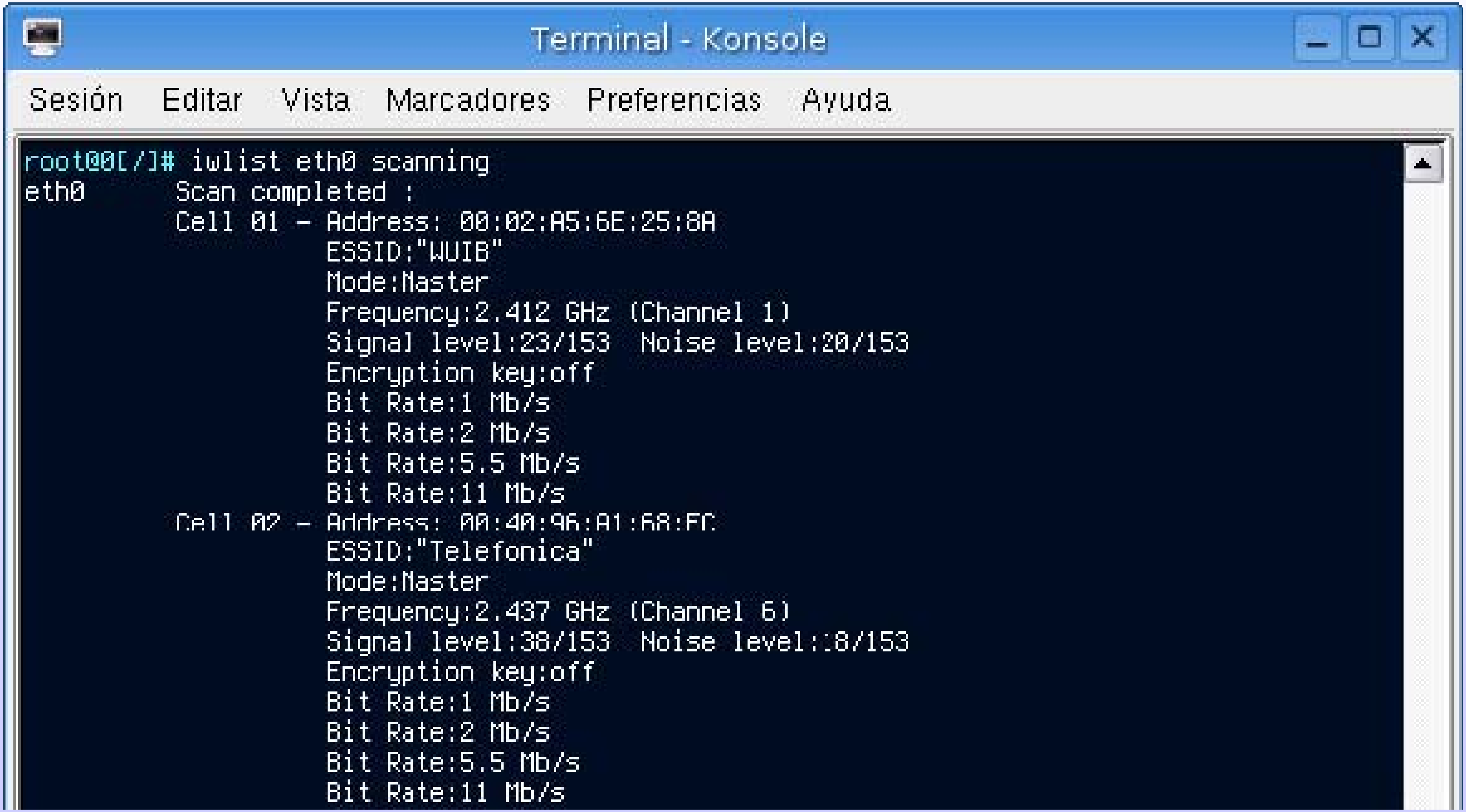
iwconfig

- Asociación:



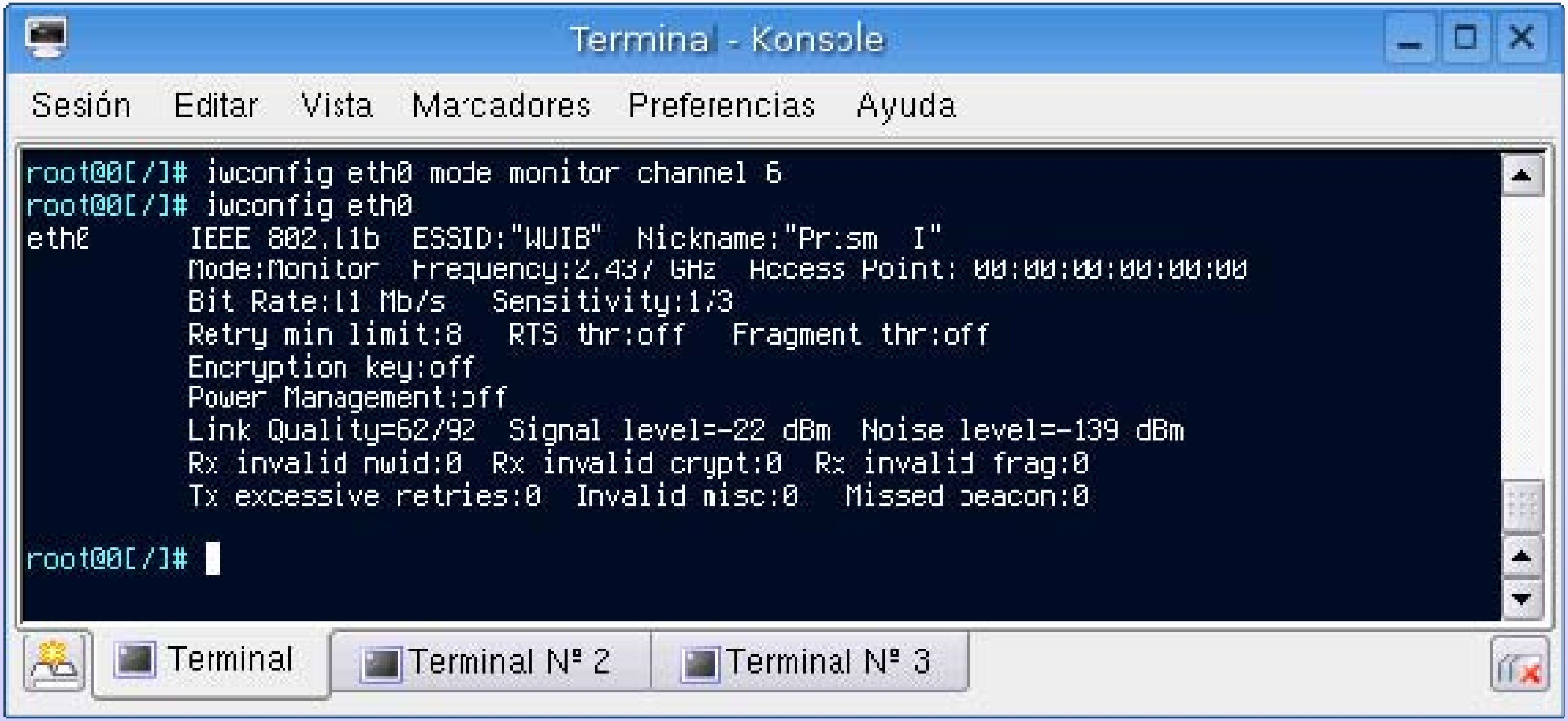
```
root@0[/]# iwconfig eth0 mode managed essid WUIB
root@0[/]# iwconfig eth0
eth0      IEEE 802.11b  ESSID:"WUIB"  Nickname:"Prism  I"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 00:02:A5:2E:20:58
          Bit Rate:11 Mb/s   Sensitivity:1/3
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=64/92  Signal level=-20 dBm  Noise level=-139 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@0[/]#
```

iwlist: scan



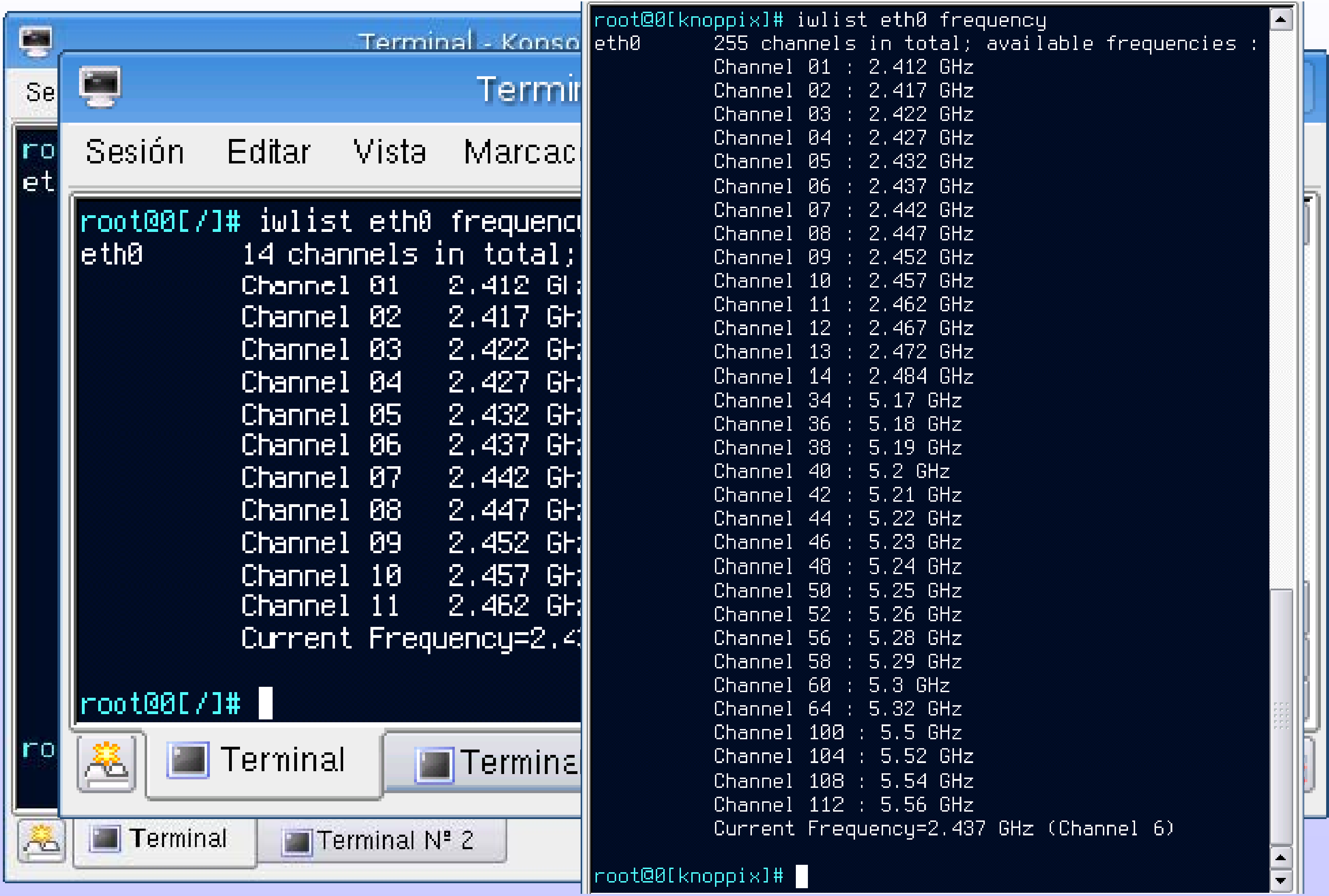
```
root@0[/]# iwlist eth0 scanning
eth0      Scan completed :
          Cell 01 - Address: 00:02:A5:6E:25:8A
                    ESSID:"WUIB"
                    Mode:Master
                    Frequency:2.412 GHz (Channel 1)
                    Signal level:23/153  Noise level:20/153
                    Encryption key:off
                    Bit Rate:1 Mb/s
                    Bit Rate:2 Mb/s
                    Bit Rate:5.5 Mb/s
                    Bit Rate:11 Mb/s
          Cell 02 - Address: 00:40:96:A1:68:FC
                    ESSID:"Telefonica"
                    Mode:Master
                    Frequency:2.437 GHz (Channel 6)
                    Signal level:38/153  Noise level:18/153
                    Encryption key:off
                    Bit Rate:1 Mb/s
                    Bit Rate:2 Mb/s
                    Bit Rate:5.5 Mb/s
                    Bit Rate:11 Mb/s
```

iwconfig: mode monitor



```
root@0[/]# iwconfig eth0 mode monitor channel 6
root@0[/]# iwconfig eth0
eth0      IEEE 802.11b  ESSID:"WUIB"  Nickname:"Prism  I"
          Mode:Monitor  Frequency:2.437 GHz  Access Point: 00:00:00:00:00:00
          Bit Rate:11 Mb/s   Sensitivity:1/3
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=62/92  Signal level=-22 dBm  Noise level=-139 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@0[/]#
```

iwlist: freq/channel



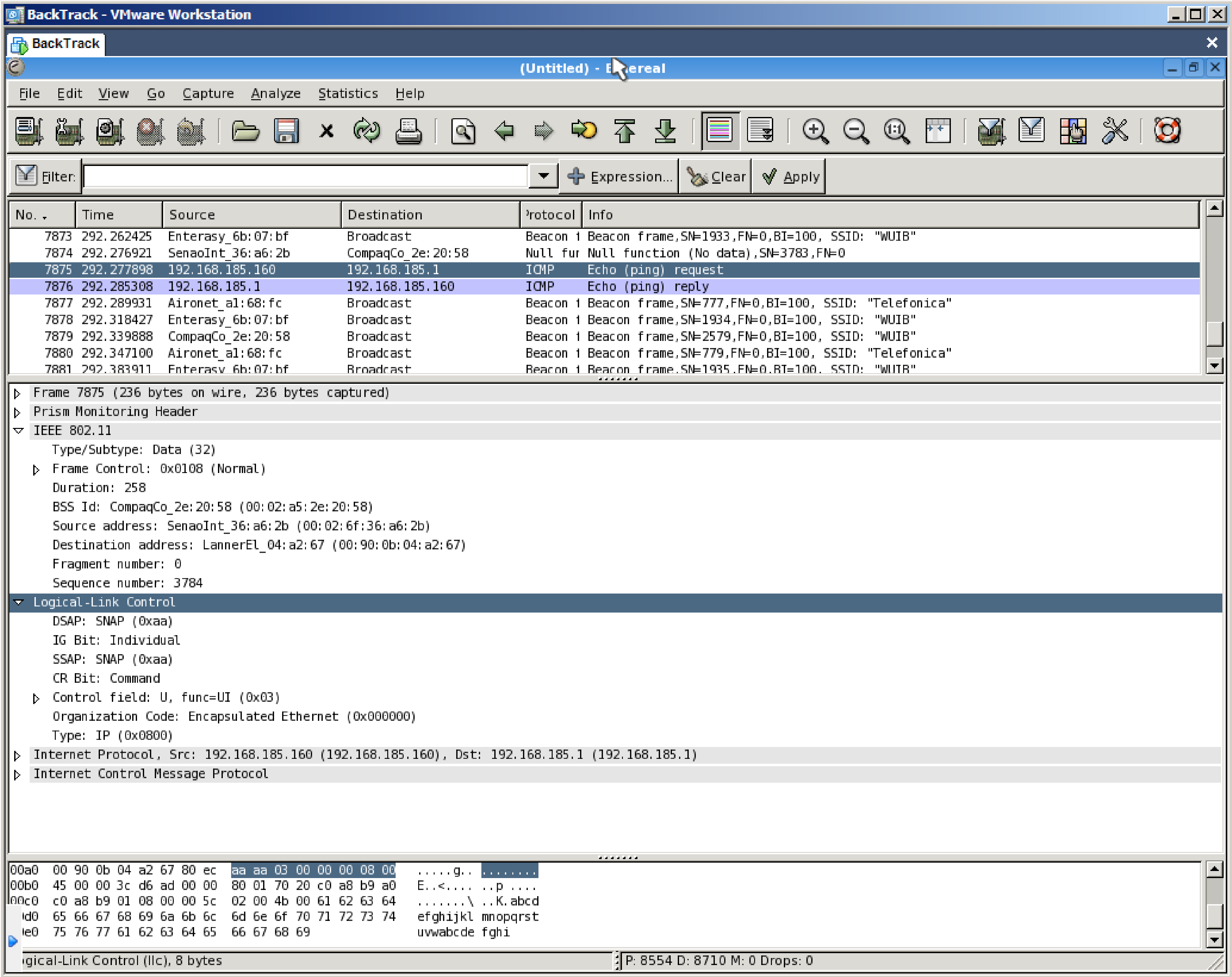
```
ro
et
ro
```

```
root@0[/]# iwlist eth0 frequenc
eth0       14 channels in total;
           Channel 01    2.412 Gl
           Channel 02    2.417 GH
           Channel 03    2.422 GH
           Channel 04    2.427 GH
           Channel 05    2.432 GH
           Channel 06    2.437 GH
           Channel 07    2.442 GH
           Channel 08    2.447 GH
           Channel 09    2.452 GH
           Channel 10    2.457 GH
           Channel 11    2.462 GH
           Current Frequency=2.4

root@0[/]#
```

```
root@0[knoppix]# iwlist eth0 frequency
eth0      255 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
          Channel 14 : 2.484 GHz
          Channel 34 : 5.17 GHz
          Channel 36 : 5.18 GHz
          Channel 38 : 5.19 GHz
          Channel 40 : 5.2 GHz
          Channel 42 : 5.21 GHz
          Channel 44 : 5.22 GHz
          Channel 46 : 5.23 GHz
          Channel 48 : 5.24 GHz
          Channel 50 : 5.25 GHz
          Channel 52 : 5.26 GHz
          Channel 56 : 5.28 GHz
          Channel 58 : 5.29 GHz
          Channel 60 : 5.3 GHz
          Channel 64 : 5.32 GHz
          Channel 100 : 5.5 GHz
          Channel 104 : 5.52 GHz
          Channel 108 : 5.54 GHz
          Channel 112 : 5.56 GHz
          Current Frequency=2.437 GHz (Channel 6)

root@0[knoppix]#
```

Ethereal

- Sniffer con modo gráfico
- Modo consola: tethereal
  - La alternativa a tcpdump...
- Protocol dissectors!!
- Con editcap podemos convertir otros formatos de captura
  - AiroPeek/Wildpackets
  - Network Associates
  - etc...



```
No. .  Time        Source               Destination       'rotocol  Info
 7873  292.262425  Enterasy_6b:07:bf    Broadcast         Beacon f  Beacon frame,SN=1933,FN=0,BI=100, SSID: "WUIB"
 7874  292.276921  SenaoInt_36:a6:2b    CompaqCo_2e:20:58 Null fur  Null function (No data),SN=3783,FN=0
 7875  292.277898  192.168.185.160      192.168.185.1     ICMP      Echo (ping) request
 7876  292.285308  192.168.185.1        192.168.185.160   ICMP      Echo (ping) reply
 7877  292.289931  Aironet_a1:68:fc     Broadcast         Beacon f  Beacon frame,SN=777,FN=0,BI=100, SSID: "Telefonica"
 7878  292.318427  Enterasy_6b:07:bf    Broadcast         Beacon f  Beacon frame,SN=1934,FN=0,BI=100, SSID: "WUIB"
 7879  292.339888  CompaqCo_2e:20:58    Broadcast         Beacon f  Beacon frame,SN=2579,FN=0,BI=100, SSID: "WUIB"
 7880  292.347100  Aironet_a1:68:fc     Broadcast         Beacon f  Beacon frame,SN=779,FN=0,BI=100, SSID: "Telefonica"
 7881  292.383911  Enterasy_6b:07:bf    Broadcast         Beacon f  Beacon frame,SN=1935,FN=0,BI=100, SSID: "WUIB"
```

```
▷ Frame 7875 (236 bytes on wire, 236 bytes captured)
▷ Prism Monitoring Header
▽ IEEE 802.11
    Type/Subtype: Data (32)
  ▷ Frame Control: 0x0108 (Normal)
    Duration: 258
    BSS Id: CompaqCo_2e:20:58 (00:02:a5:2e:20:58)
    Source address: SenaoInt_36:a6:2b (00:02:6f:36:a6:2b)
    Destination address: LannerEl_04:a2:67 (00:90:0b:04:a2:67)
    Fragment number: 0
    Sequence number: 3784
▽ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ▷ Control field: U, func=UI (0x03)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: IP (0x0800)
▷ Internet Protocol, Src: 192.168.185.160 (192.168.185.160), Dst: 192.168.185.1 (192.168.185.1)
▷ Internet Control Message Protocol
```

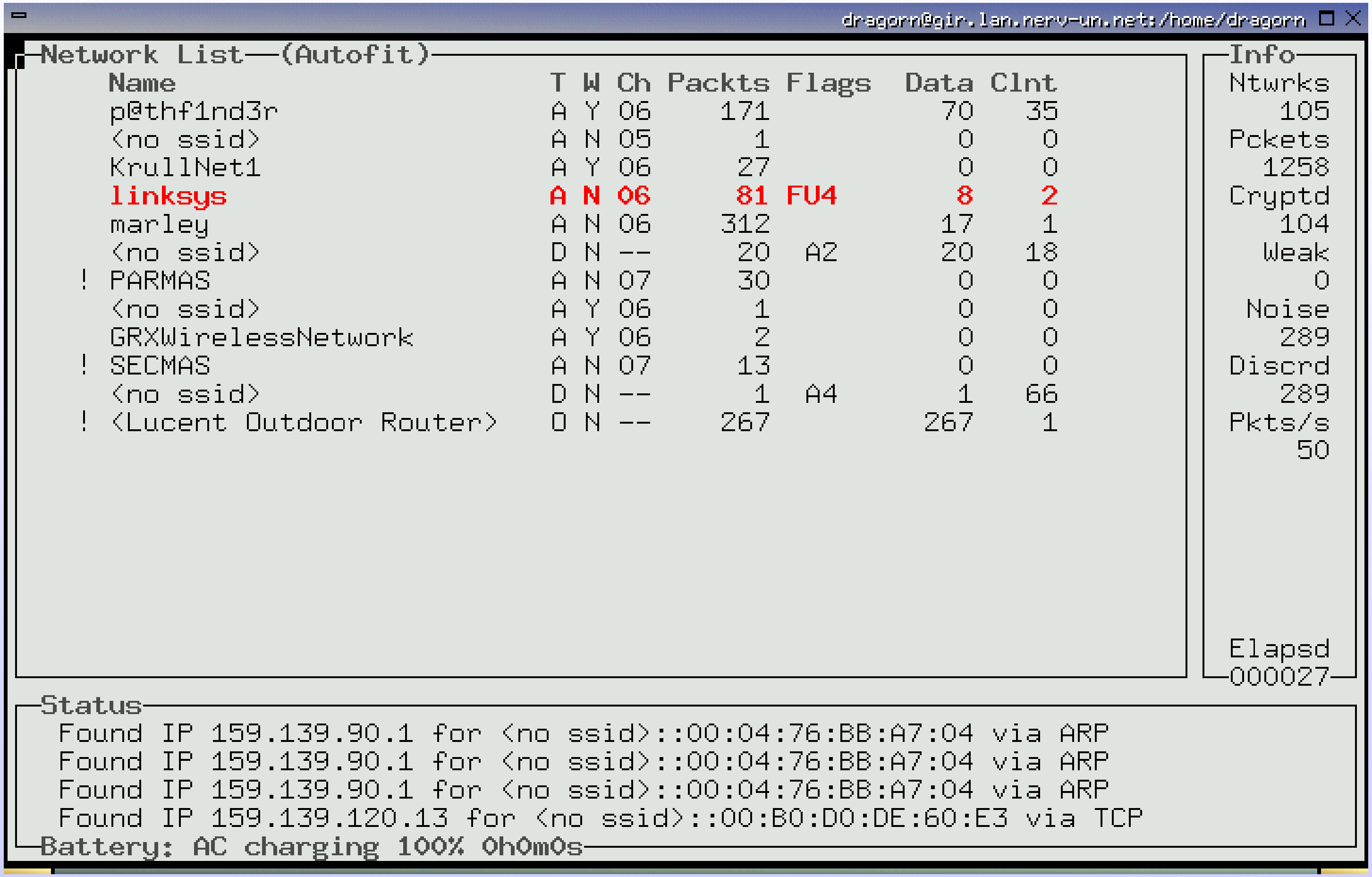
```
00a0  00 90 0b 04 a2 67 80 ec  aa aa 03 00 00 00 08 00   .....g.. ........
00b0  45 00 00 3c d6 ad 00 00  80 01 70 20 c0 a8 b9 a0   E..<.... ..p ....
00c0  c0 a8 b9 01 08 00 00 5c  02 00 4b 00 61 62 63 64   .......\ ..K.abcd
 d0   65 66 67 68 69 6a 6b 6c  6d 6e 6f 70 71 72 73 74   efghijkl mnopqrst
 e0   75 76 77 61 62 63 64 65  66 67 68 69               uvwabcde fghi
```

```
gical-Link Control (llc), 8 bytes          P: 8554 D: 8710 M: 0 Drops: 0
```

Kismet

- La herramienta por excelencia en wifi!!
- Análisis de redes wifi
  - Trabaja en modo monitor
  - Realiza channel hopping
- Cliente/Servidor
- Imprescindible conocer el driver compatible
  - Para trabajar en modo monitor
  - Parámetro: “-c rt2500,eth0,comentario”
  - Fichero de configuración: “-f kismet.conf”
- Puede sincronizar la información con GPS
  - gpsmap para realizar mapas

Kismet



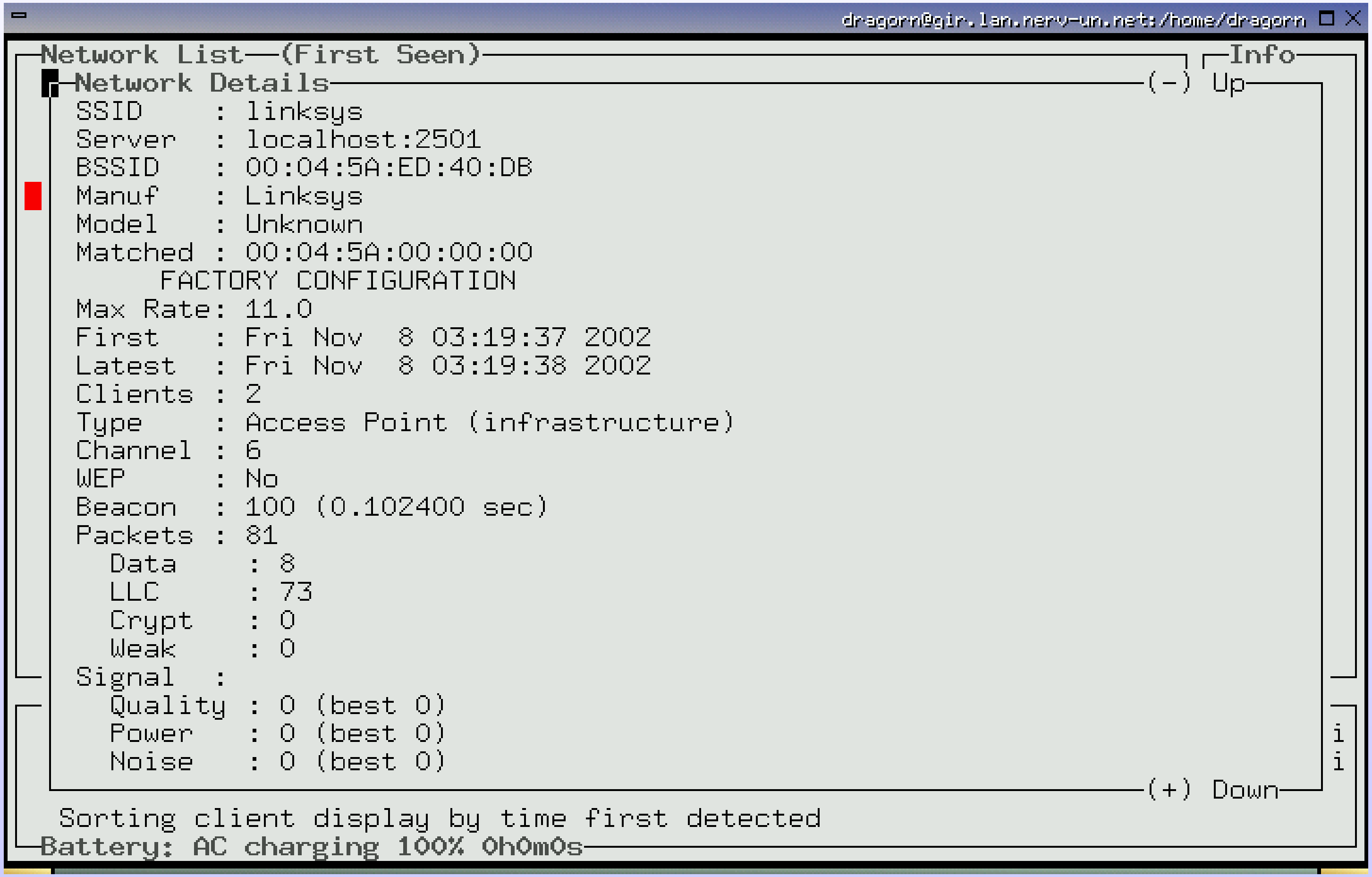
```
Network List—(Autofit)                                               Info
      Name                       T W Ch Packts Flags  Data Clnt      Ntwrks
      p@thf1nd3r                 A Y 06    171           70   35        105
      <no ssid>                  A N 05      1            0    0     Pckets
      KrullNet1                  A Y 06     27            0    0       1258
      linksys                    A N 06     81 FU4        8    2     Cryptd
      marley                     A N 06    312           17    1        104
      <no ssid>                  D N --     20  A2       20   18       Weak
    ! PARMAS                     A N 07     30            0    0          0
      <no ssid>                  A Y 06      1            0    0      Noise
      GRXWirelessNetwork         A Y 06      2            0    0        289
    ! SECMAS                     A N 07     13            0    0     Discrd
      <no ssid>                  D N --      1  A4        1   66        289
    ! <Lucent Outdoor Router>    O N --    267          267    1     Pkts/s
                                                                         50

                                                                     Elapsd
                                                                     000027
Status
  Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
  Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
  Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
  Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP
Battery: AC charging 100% 0h0m0s
```

Kismet

- Hot-keys:
  - s: Para ordenar (canal, potencia,etc...)
  - h: Ayuda
  - i: Obtener información
  - c: Mostrar los clientes de la red
  - p: Captura de paquetes en tiempo real
  - d: Volcado de strings de la captura
  - l: información sobre señal/ruido
  - x: cerrar ventana
  - Q: salir de Kismet

Kismet

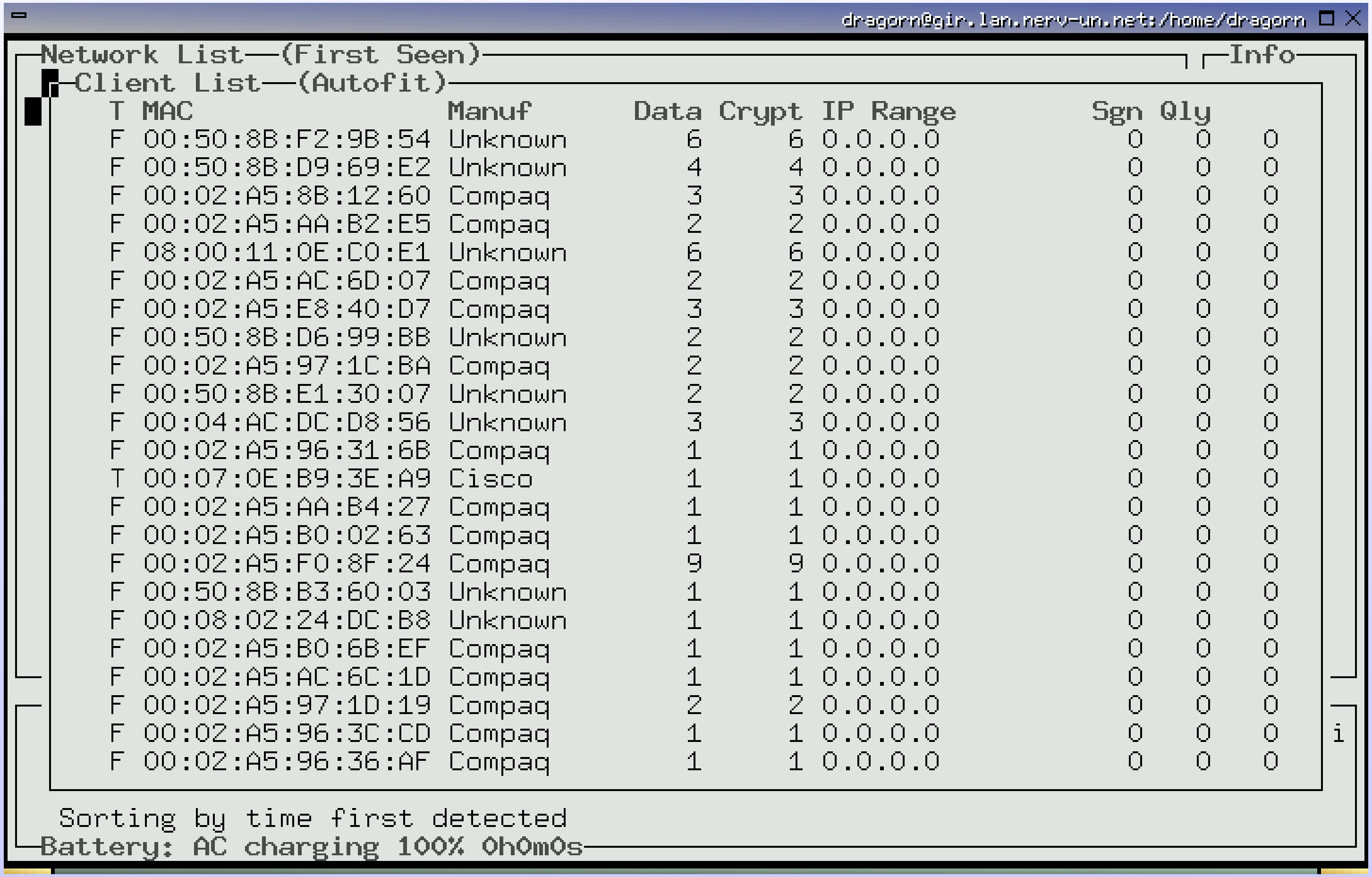
- AP info



```
Network List—(First Seen)                                          Info
  Network Details                                             (-)  Up
   SSID    : linksys
   Server  : localhost:2501
   BSSID   : 00:04:5A:ED:40:DB
   Manuf   : Linksys
   Model   : Unknown
   Matched : 00:04:5A:00:00:00
        FACTORY CONFIGURATION
   Max Rate: 11.0
   First   : Fri Nov  8 03:19:37 2002
   Latest  : Fri Nov  8 03:19:38 2002
   Clients : 2
   Type    : Access Point (infrastructure)
   Channel : 6
   WEP     : No
   Beacon  : 100 (0.102400 sec)
   Packets : 81
     Data     : 8
     LLC      : 73
     Crypt    : 0
     Weak     : 0
   Signal   :
     Quality : 0 (best 0)
     Power   : 0 (best 0)                                                i
     Noise   : 0 (best 0)                                                i
                                                              (+)  Down
  Sorting client display by time first detected
Battery: AC charging 100% 0h0m0s
```

Kismet

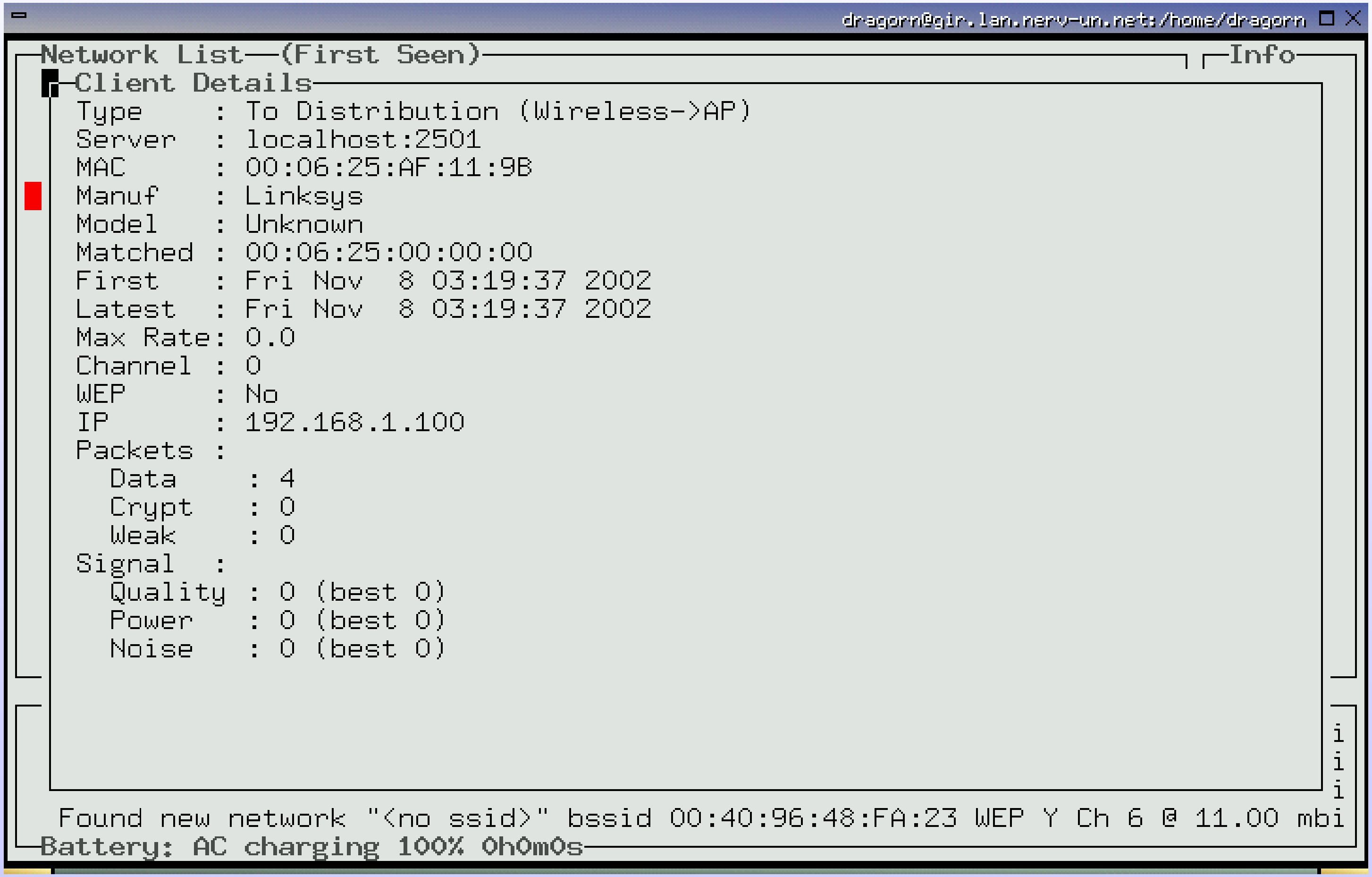
- Clientes



```
dragorn@gir.lan.nerv-un.net:/home/dragorn
Network List—(First Seen)                                    Info
 Client List—(Autofit)
   T MAC               Manuf      Data Crypt IP Range     Sgn Qly
   F 00:50:8B:F2:9B:54 Unknown       6     6 0.0.0.0        0   0   0
   F 00:50:8B:D9:69:E2 Unknown       4     4 0.0.0.0        0   0   0
   F 00:02:A5:8B:12:60 Compaq        3     3 0.0.0.0        0   0   0
   F 00:02:A5:AA:B2:E5 Compaq        2     2 0.0.0.0        0   0   0
   F 08:00:11:0E:C0:E1 Unknown       6     6 0.0.0.0        0   0   0
   F 00:02:A5:AC:6D:07 Compaq        2     2 0.0.0.0        0   0   0
   F 00:02:A5:E8:40:D7 Compaq        3     3 0.0.0.0        0   0   0
   F 00:50:8B:D6:99:BB Unknown       2     2 0.0.0.0        0   0   0
   F 00:02:A5:97:1C:BA Compaq        2     2 0.0.0.0        0   0   0
   F 00:50:8B:E1:30:07 Unknown       2     2 0.0.0.0        0   0   0
   F 00:04:AC:DC:D8:56 Unknown       3     3 0.0.0.0        0   0   0
   F 00:02:A5:96:31:6B Compaq        1     1 0.0.0.0        0   0   0
   T 00:07:0E:B9:3E:A9 Cisco         1     1 0.0.0.0        0   0   0
   F 00:02:A5:AA:B4:27 Compaq        1     1 0.0.0.0        0   0   0
   F 00:02:A5:B0:02:63 Compaq        1     1 0.0.0.0        0   0   0
   F 00:02:A5:F0:8F:24 Compaq        9     9 0.0.0.0        0   0   0
   F 00:50:8B:B3:60:03 Unknown       1     1 0.0.0.0        0   0   0
   F 00:08:02:24:DC:B8 Unknown       1     1 0.0.0.0        0   0   0
   F 00:02:A5:B0:6B:EF Compaq        1     1 0.0.0.0        0   0   0
   F 00:02:A5:AC:6C:1D Compaq        1     1 0.0.0.0        0   0   0
   F 00:02:A5:97:1D:19 Compaq        2     2 0.0.0.0        0   0   0
   F 00:02:A5:96:3C:CD Compaq        1     1 0.0.0.0        0   0   0    i
   F 00:02:A5:96:36:AF Compaq        1     1 0.0.0.0        0   0   0

 Sorting by time first detected
Battery: AC charging 100% 0h0m0s
```

Kismet

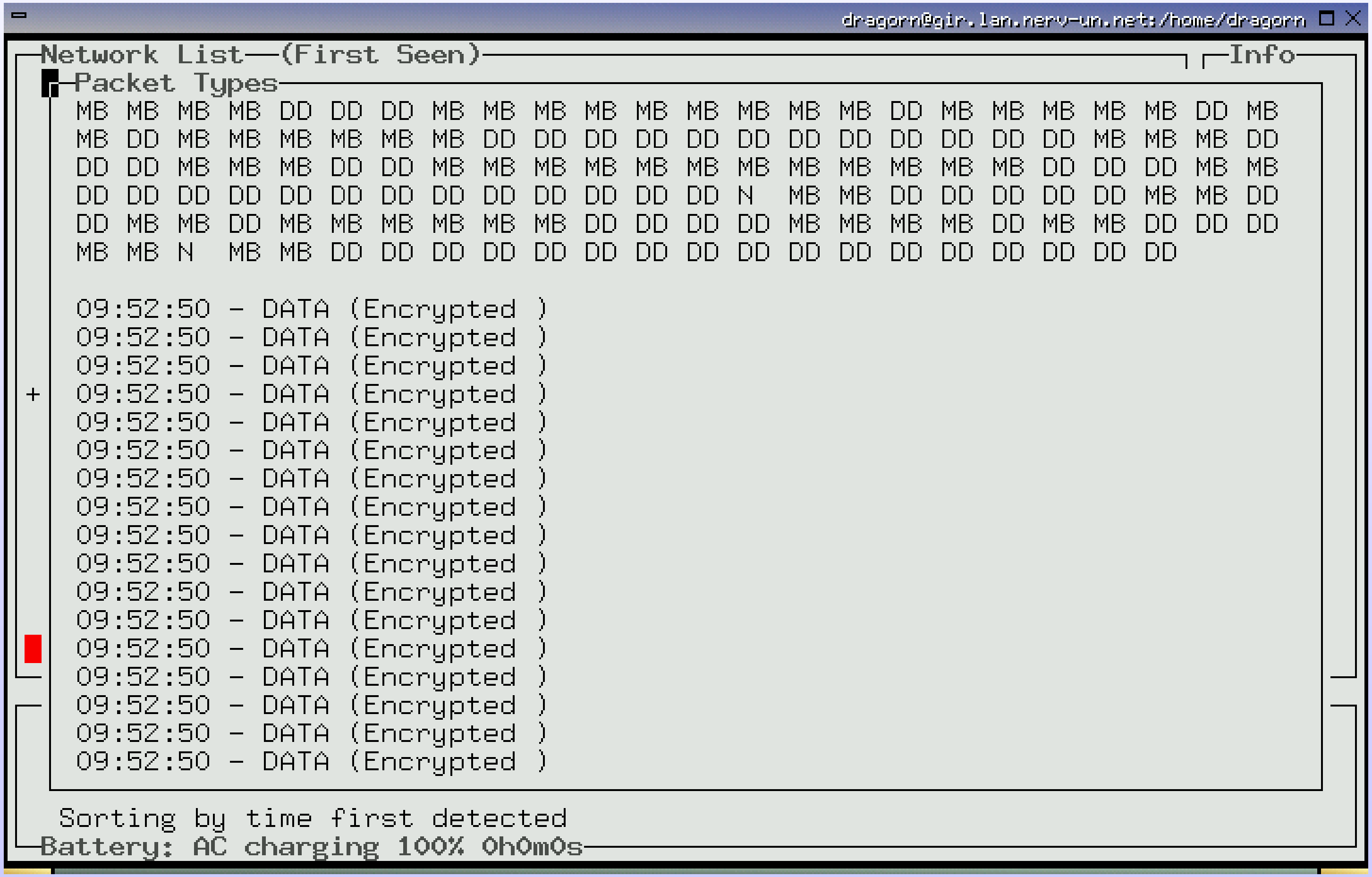
- Client info



```
dragorn@gir.lan.nerv-un.net:/home/dragorn
Network List—(First Seen)                                        Info
  Client Details
  Type     : To Distribution (Wireless->AP)
  Server   : localhost:2501
  MAC      : 00:06:25:AF:11:9B
  Manuf    : Linksys
  Model    : Unknown
  Matched  : 00:06:25:00:00:00
  First    : Fri Nov  8 03:19:37 2002
  Latest   : Fri Nov  8 03:19:37 2002
  Max Rate: 0.0
  Channel  : 0
  WEP      : No
  IP       : 192.168.1.100
  Packets  :
    Data     : 4
    Crypt    : 0
    Weak     : 0
  Signal   :
    Quality : 0 (best 0)
    Power    : 0 (best 0)
    Noise    : 0 (best 0)
                                                                      i
                                                                      i
                                                                      i
 Found new network "<no ssid>" bssid 00:40:96:48:FA:23 WEP Y Ch 6 @ 11.00 mbi
Battery: AC charging 100% 0h0m0s
```

Kismet

- Paquetes



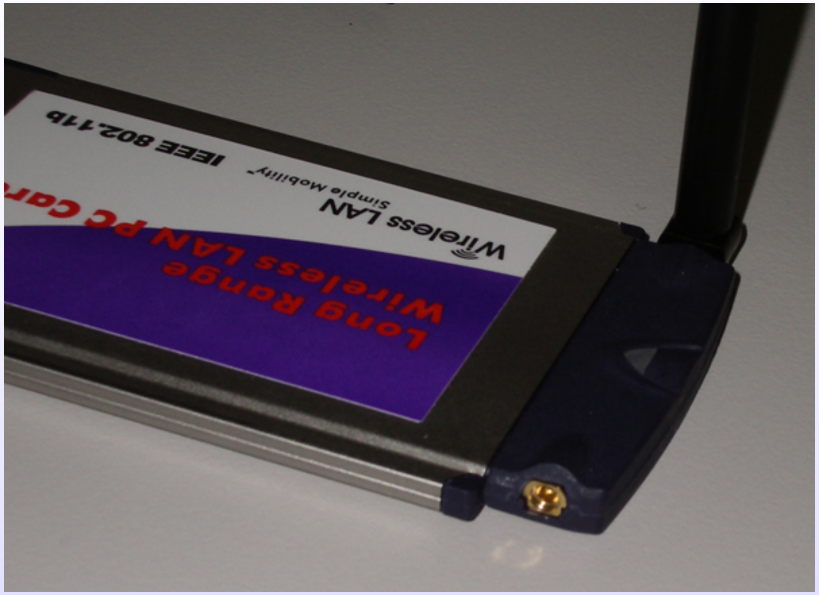
```
dragorn@gir.lan.nerv-un.net:/home/dragorn

Network List—(First Seen)                                             Info
  Packet Types
  MB MB MB MB DD DD DD MB MB MB MB MB MB MB MB MB DD MB MB MB MB MB DD MB
  MB DD MB MB MB MB MB MB DD DD DD DD DD DD DD DD DD DD DD DD MB MB MB DD
  DD DD MB MB MB DD DD MB MB MB MB MB MB MB MB MB MB MB MB DD DD DD MB MB
  DD DD DD DD DD DD DD DD DD DD DD DD DD N  MB MB DD DD DD DD DD MB MB DD
  DD MB MB DD MB MB MB MB MB MB DD DD DD DD MB MB MB MB DD MB MB DD DD DD
  MB MB N  MB MB DD DD DD DD DD DD DD DD DD DD DD DD DD DD DD DD DD

  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
+ 09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )
  09:52:50 - DATA (Encrypted )

 Sorting by time first detected
Battery: AC charging 100% 0h0m0s
```

Kismet

- Sources... Hay que testear el driver con nuestro material
  - hostap
  - madwifi_ag
  - rt2500
  - cisco_wifix
  - ipw2100,ipw2200 → Centrino

hostap

Long Range
Wireless LAN PC Card
Wireless LAN
Simple Mobility
IEEE 802.11b


Long Range
Wireless LAN PC Card
Wireless LAN
Simple Mobility
IEEE 802.11b

ENTERASYS
NETWORKS
RoamAbout
802.11 DS High Rate

madwifi_ag

RoamAbout
802.11a/b/g
2.4/5GHz Client Card
ENTERASYS
NETWORKS

rt2500

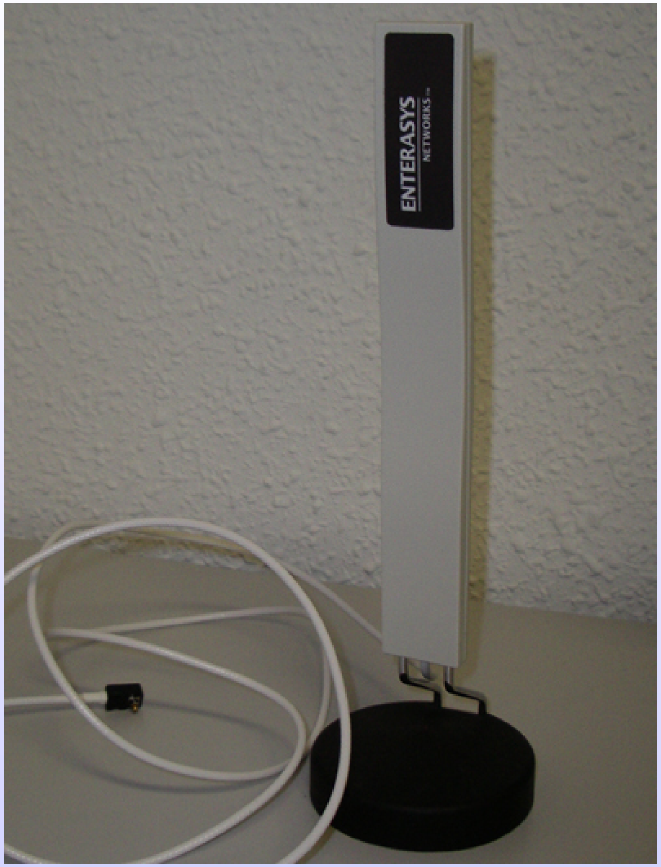
cisco_wifix

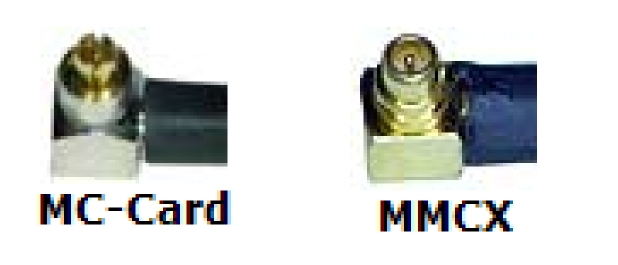
CISCO SYSTEMS
CISCO AIRONET 350 SERIES
WIRELESS LAN ADAPTER

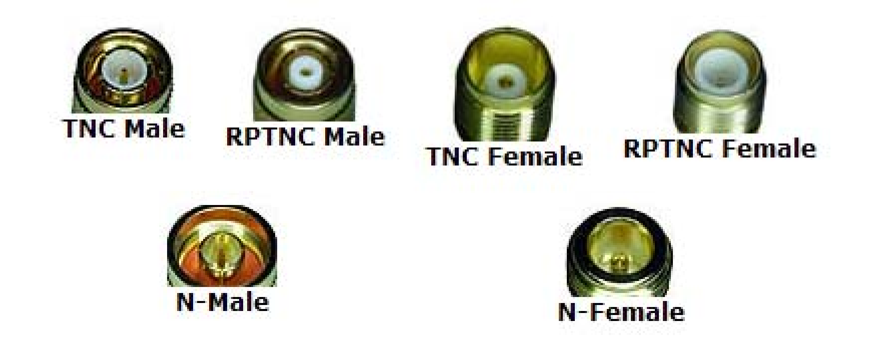
CISCO SYSTEMS
CISCO AIRONET 350 SERIES
WIRELESS LAN ADAPTER

Antenas

- Antenas y conectores

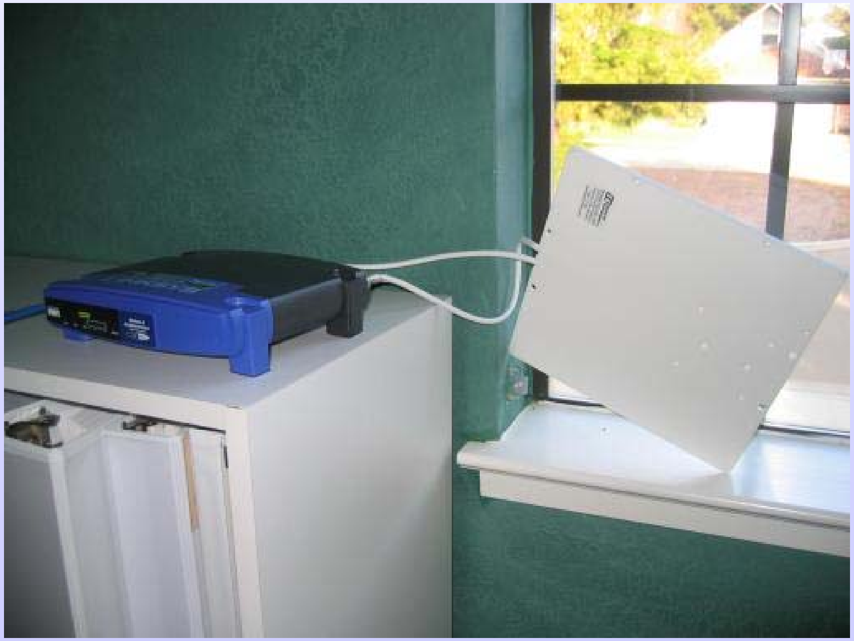






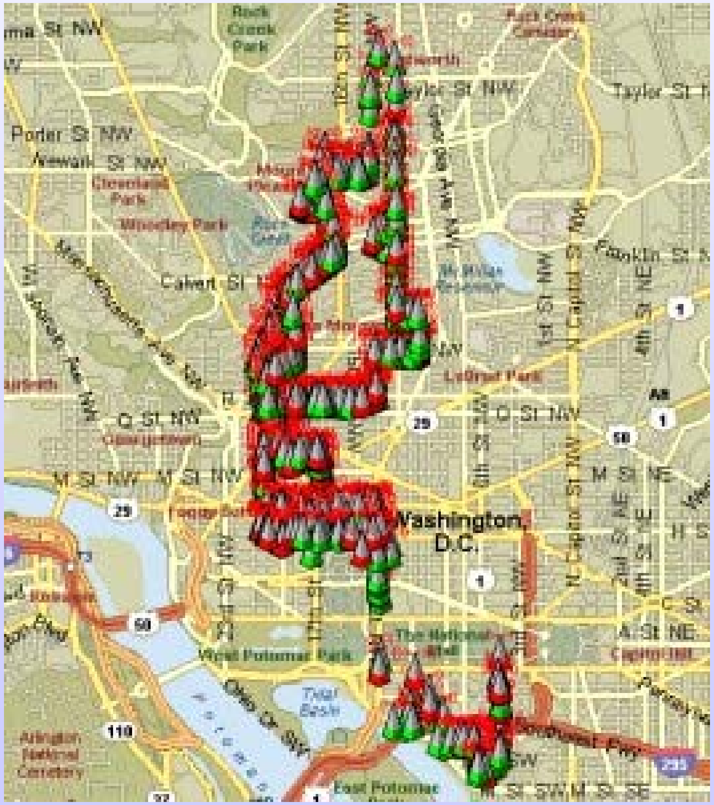
Kismet on Linksys

- AP basado en linux → upgrade firmware
  - http://toys.lerdorf.com/archives/20-Kismet-on-the-Linksys-WRT54G.html
  - source=wrt54g,eth2,wrt54g



GPS

- Sincronizar capturas con GPS...

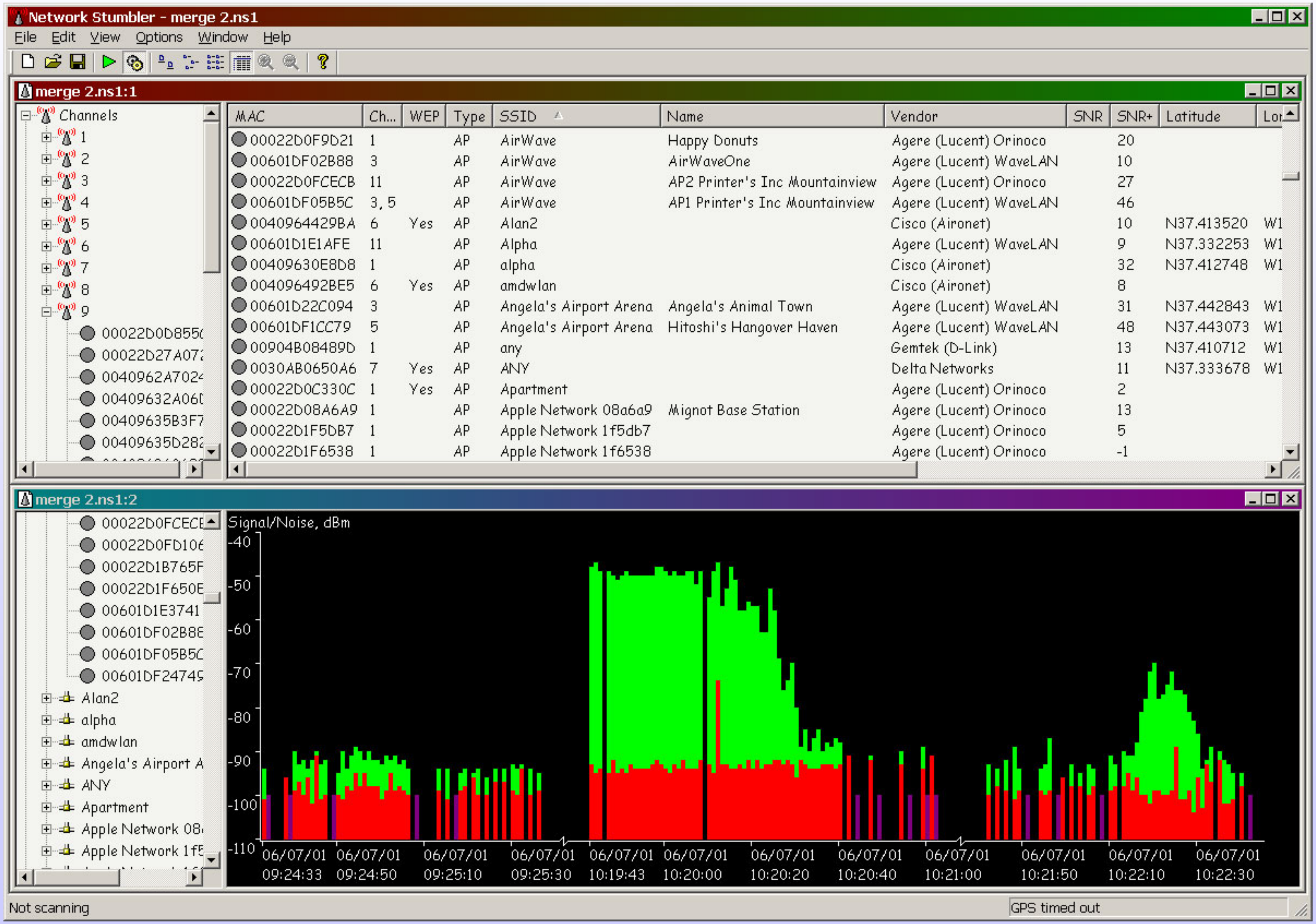


Forget GPS, hello WPS

- http://www.skyhookwireless.com

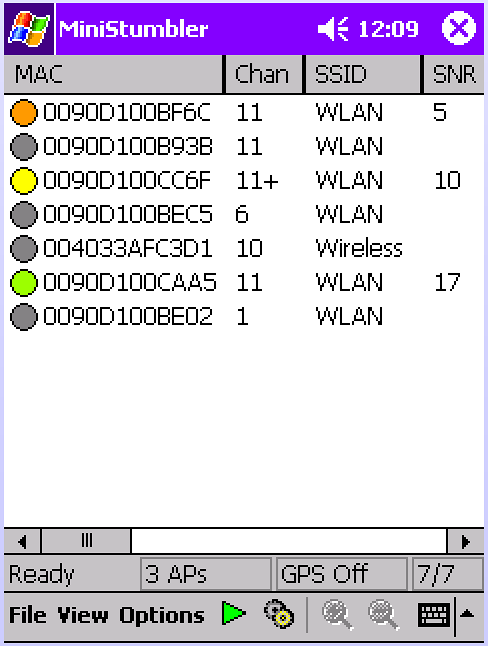
SKYHOOK WIRELESS
Access Point
Latitude
Longitude
STOP

Netstumbler



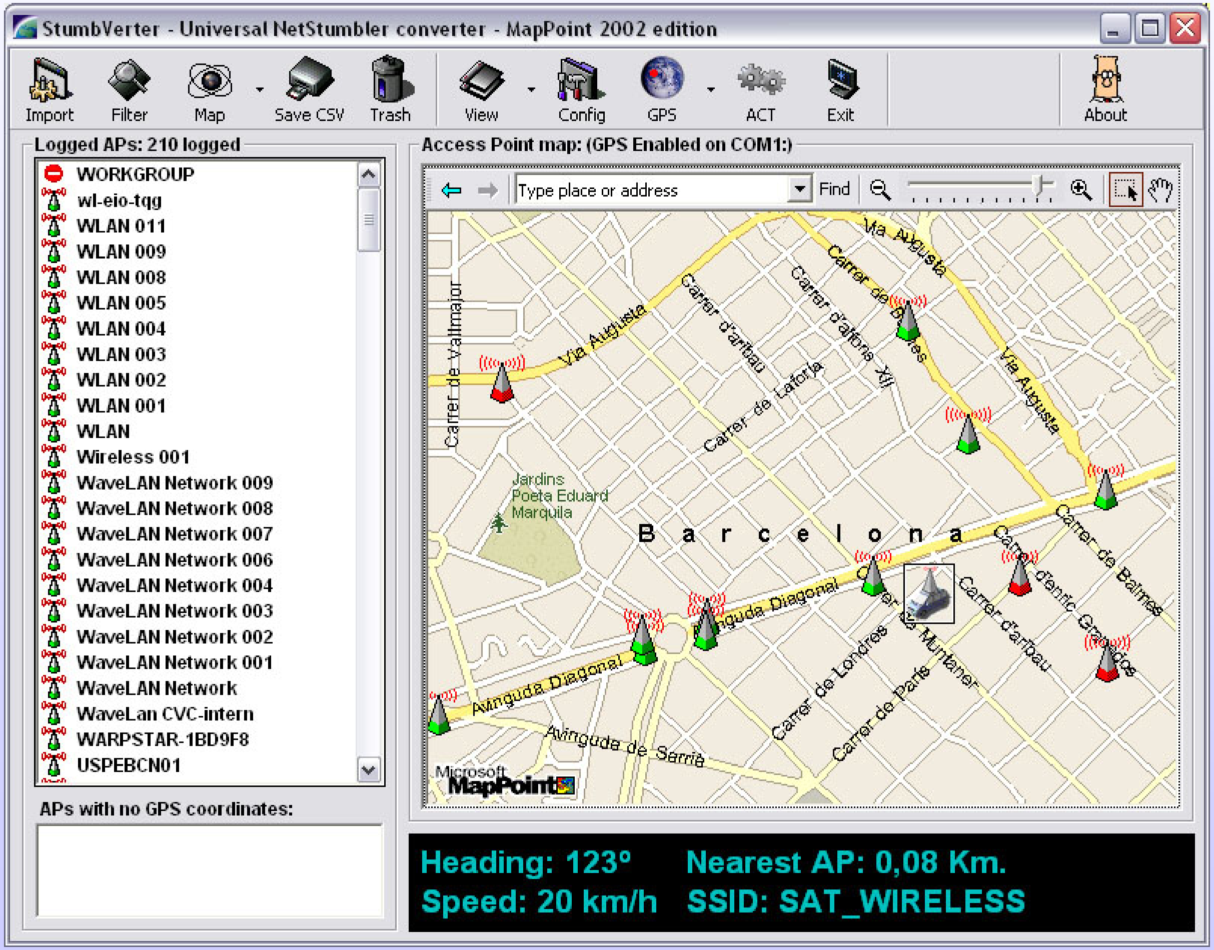
MAC	Ch...	WEP	Type	SSID	Name	Vendor	SNR	SNR+	Latitude	Lon
00022D0F9D21	1		AP	AirWave	Happy Donuts	Agere (Lucent) Orinoco		20		
00601DF02B88	3		AP	AirWave	AirWaveOne	Agere (Lucent) WaveLAN		10		
00022D0FCECB	11		AP	AirWave	AP2 Printer's Inc Mountainview	Agere (Lucent) Orinoco		27		
00601DF05B5C	3, 5		AP	AirWave	AP1 Printer's Inc Mountainview	Agere (Lucent) WaveLAN		46		
0040964429BA	6	Yes	AP	Alan2		Cisco (Aironet)		10	N37.413520	W1
00601D1E1AFE	11		AP	Alpha		Agere (Lucent) WaveLAN		9	N37.332253	W1
00409630E8D8	1		AP	alpha		Cisco (Aironet)		32	N37.412748	W1
004096492BE5	6	Yes	AP	amdwlan		Cisco (Aironet)		8		
00601D22C094	3		AP	Angela's Airport Arena	Angela's Animal Town	Agere (Lucent) WaveLAN		31	N37.442843	W1
00601DF1CC79	5		AP	Angela's Airport Arena	Hitoshi's Hangover Haven	Agere (Lucent) WaveLAN		48	N37.443073	W1
00904B08489D	1		AP	any		Gemtek (D-Link)		13	N37.410712	W1
0030AB0650A6	7	Yes	AP	ANY		Delta Networks		11	N37.333678	W1
00022D0C330C	1	Yes	AP	Apartment		Agere (Lucent) Orinoco		2		
00022D08A6A9	1		AP	Apple Network 08a6a9	Mignot Base Station	Agere (Lucent) Orinoco		13		
00022D1F5DB7	1		AP	Apple Network 1f5db7		Agere (Lucent) Orinoco		5		
00022D1F6538	1		AP	Apple Network 1f6538		Agere (Lucent) Orinoco		-1		

Netstumbler


MiniStumbler 12:09

MAC	Chan	SSID	SNR
● 0090D100BF6C	11	WLAN	5
● 0090D100B93B	11	WLAN	
● 0090D100CC6F	11+	WLAN	10
● 0090D100BEC5	6	WLAN	
● 004033AFC3D1	10	Wireless	
● 0090D100CAA5	11	WLAN	17
● 0090D100BE02	1	WLAN	

Ready | 3 APs | GPS Off | 7/7


StumbVerter - Universal NetStumbler converter - MapPoint 2002 edition

Logged APs: 210 logged

- WORKGROUP
- wl-eio-tqg
- WLAN 011
- WLAN 009
- WLAN 008
- WLAN 005
- WLAN 004
- WLAN 003
- WLAN 002
- WLAN 001
- WLAN
- Wireless 001
- WaveLAN Network 009
- WaveLAN Network 008
- WaveLAN Network 007
- WaveLAN Network 006
- WaveLAN Network 004
- WaveLAN Network 003
- WaveLAN Network 002
- WaveLAN Network 001
- WaveLAN Network
- WaveLan CVC-intern
- WARPSTAR-1BD9F8
- USPEBCN01

APs with no GPS coordinates:

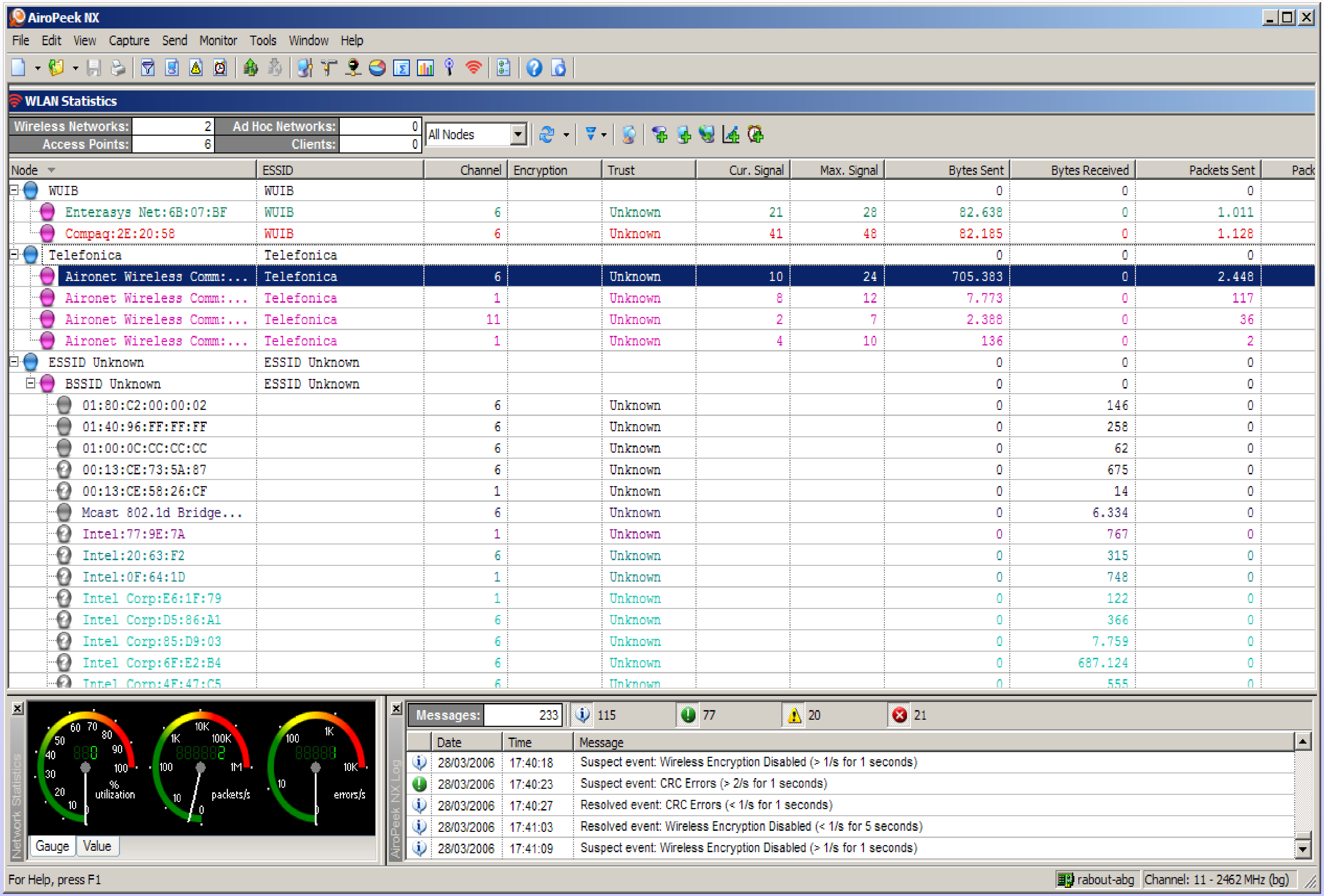
Access Point map: (GPS Enabled on COM1:)

Heading: 123° Nearest AP: 0,08 Km.
Speed: 20 km/h SSID: SAT_WIRELESS

Airopeek

- Producto de WlidPackets
- Proporciona drivers para trabajar en modo monitor
- Sniffer analizador de protocolos
- Barrido de canales wifi
- Utilidades Expert para análisis

Airopeek



Wireless Networks: 2 Ad Hoc Networks: 0
Access Points: 6 Clients: 0
All Nodes

Node	ESSID	Channel	Encryption	Trust	Cur. Signal	Max. Signal	Bytes Sent	Bytes Received	Packets Sent	Pack
WUIB	WUIB						0	0	0	
Enterasys Net:6B:07:BF	WUIB	6		Unknown	21	28	82.638	0	1.011	
Compaq:2E:20:58	WUIB	6		Unknown	41	48	82.185	0	1.128	
Telefonica	Telefonica						0	0	0	
Aironet Wireless Comm:...	Telefonica	6		Unknown	10	24	705.383	0	2.448	
Aironet Wireless Comm:...	Telefonica	1		Unknown	8	12	7.773	0	117	
Aironet Wireless Comm:...	Telefonica	11		Unknown	2	7	2.388	0	36	
Aironet Wireless Comm:...	Telefonica	1		Unknown	4	10	136	0	2	
ESSID Unknown	ESSID Unknown						0	0	0	
BSSID Unknown	ESSID Unknown						0	0	0	
01:80:C2:00:00:02		6		Unknown			0	146	0	
01:40:96:FF:FF:FF		6		Unknown			0	258	0	
01:00:0C:CC:CC:CC		6		Unknown			0	62	0	
00:13:CE:73:5A:87		6		Unknown			0	675	0	
00:13:CE:58:26:CF		1		Unknown			0	14	0	
Mcast 802.1d Bridge...		6		Unknown			0	6.334	0	
Intel:77:9E:7A		1		Unknown			0	767	0	
Intel:20:63:F2		6		Unknown			0	315	0	
Intel:0F:64:1D		1		Unknown			0	748	0	
Intel Corp:E6:1F:79		1		Unknown			0	122	0	
Intel Corp:D5:86:A1		6		Unknown			0	366	0	
Intel Corp:85:D9:03		6		Unknown			0	7.759	0	
Intel Corp:6F:E2:B4		6		Unknown			0	687.124	0	
Intel Corp:4F:47:C5		6		Unknown			0	555	0	

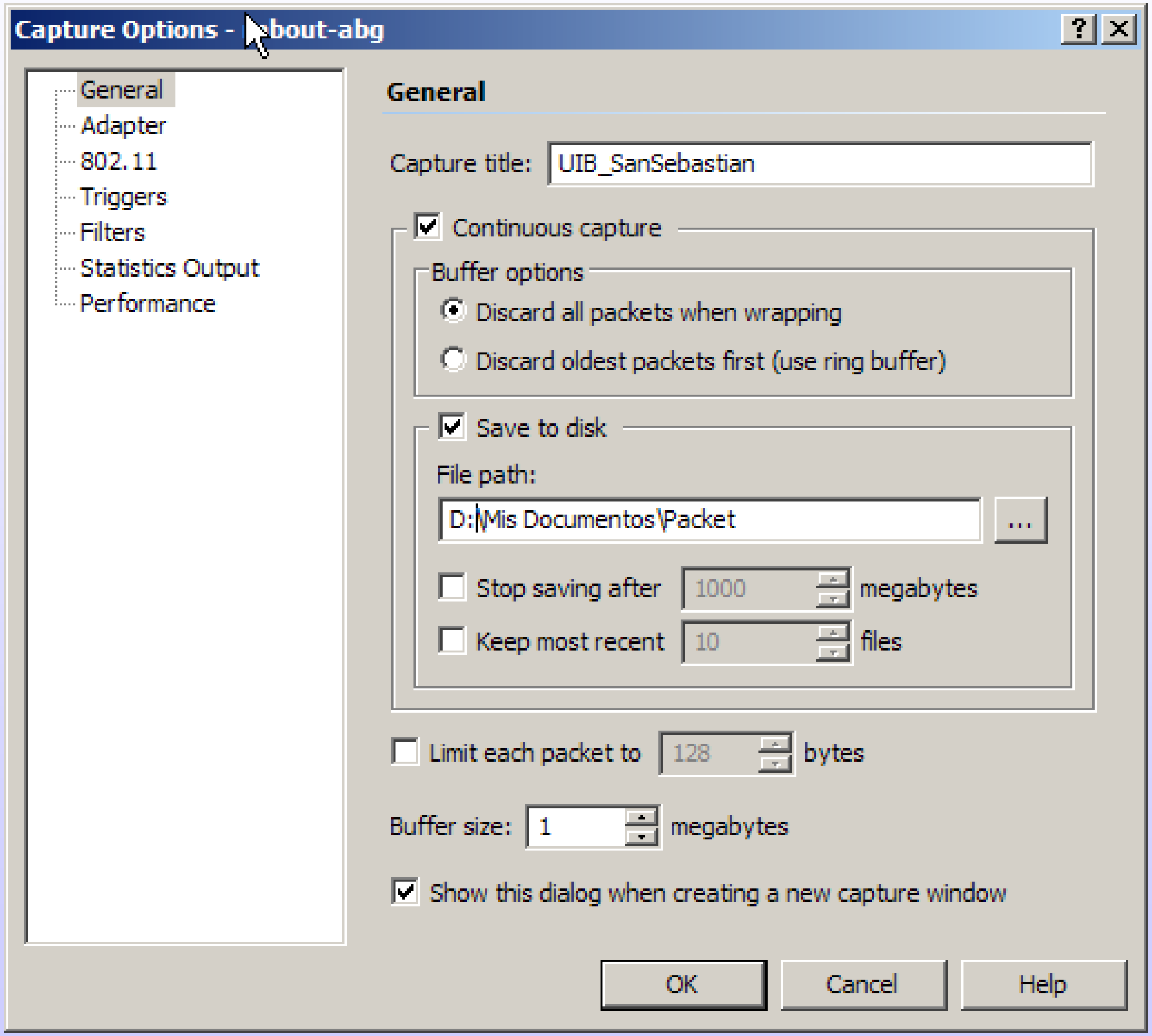
Messages: 233 | ⓘ 115 | ● 77 | ⚠ 20 | ⊗ 21

	Date	Time	Message
ⓘ	28/03/2006	17:40:18	Suspect event: Wireless Encryption Disabled (> 1/s for 1 seconds)
●	28/03/2006	17:40:23	Suspect event: CRC Errors (> 2/s for 1 seconds)
ⓘ	28/03/2006	17:40:27	Resolved event: CRC Errors (< 1/s for 1 seconds)
ⓘ	28/03/2006	17:41:03	Resolved event: Wireless Encryption Disabled (< 1/s for 5 seconds)
ⓘ	28/03/2006	17:41:09	Suspect event: Wireless Encryption Disabled (> 1/s for 1 seconds)

For Help, press F1 | rabout-abg | Channel: 11 - 2462 MHz (bg)

Airopeek

- Captura:



Capture Options - bout-abg

General

Capture title: UIB_SanSebastian

☑ Continuous capture

Buffer options

● Discard all packets when wrapping

○ Discard oldest packets first (use ring buffer)

☑ Save to disk

File path: D:\Mis Documentos\Packet

☐ Stop saving after 1000 megabytes

☐ Keep most recent 10 files

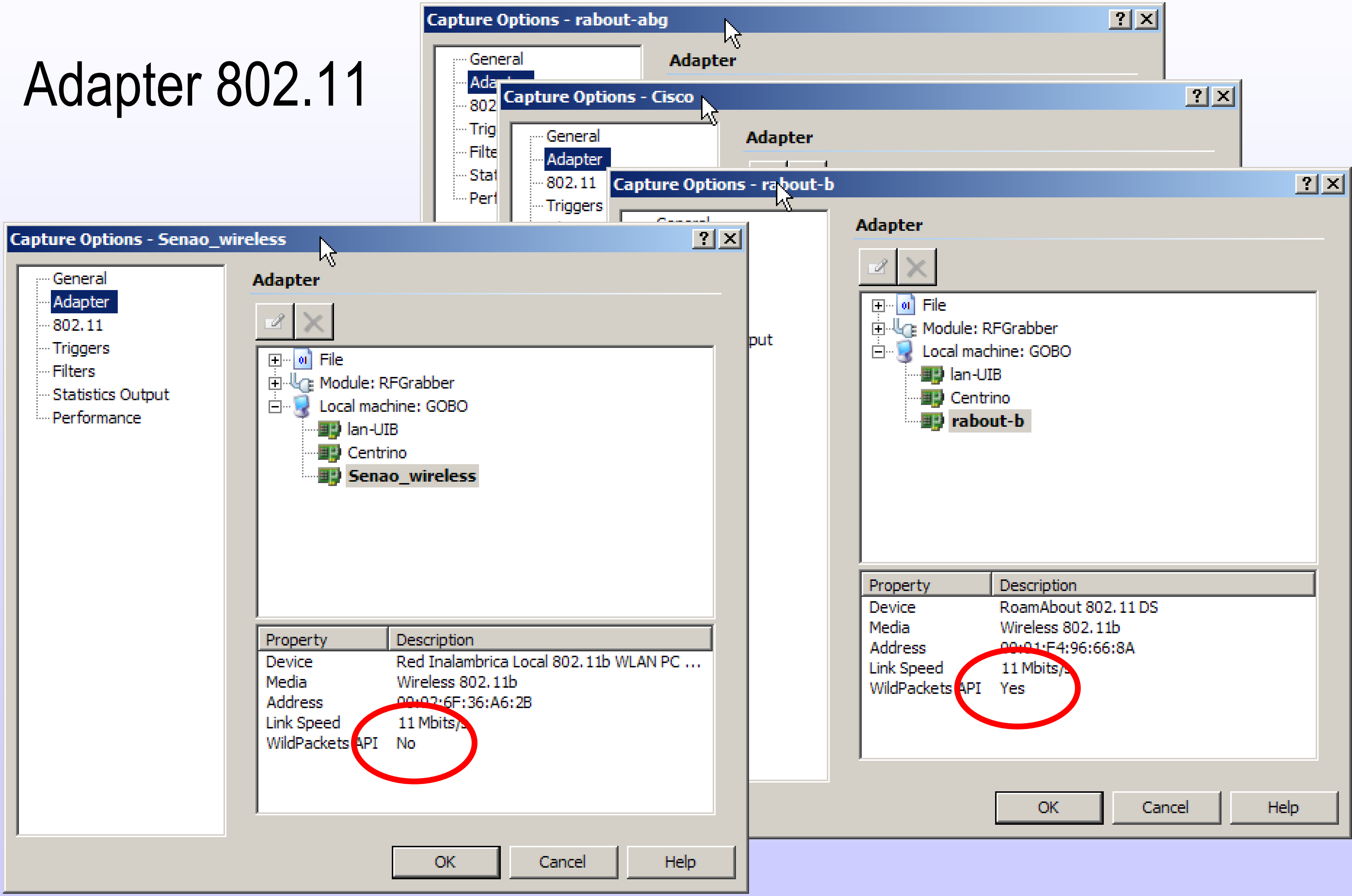
☐ Limit each packet to 128 bytes

Buffer size: 1 megabytes

☑ Show this dialog when creating a new capture window

Airopeek

- Adapter 802.11



Capture Options - rabout-abg

Capture Options - Cisco

Capture Options - rabout-b

Adapter

- File
- Module: RFGrabber
- Local machine: GOBO
  - lan-UIB
  - Centrino
  - rabout-b

Property	Description
Device	RoamAbout 802.11 DS
Media	Wireless 802.11b
Address	00:01:F4:96:66:8A
Link Speed	11 Mbits/s
WildPackets API	Yes

Capture Options - Senao_wireless

- General
- Adapter
- 802.11
- Triggers
- Filters
- Statistics Output
- Performance

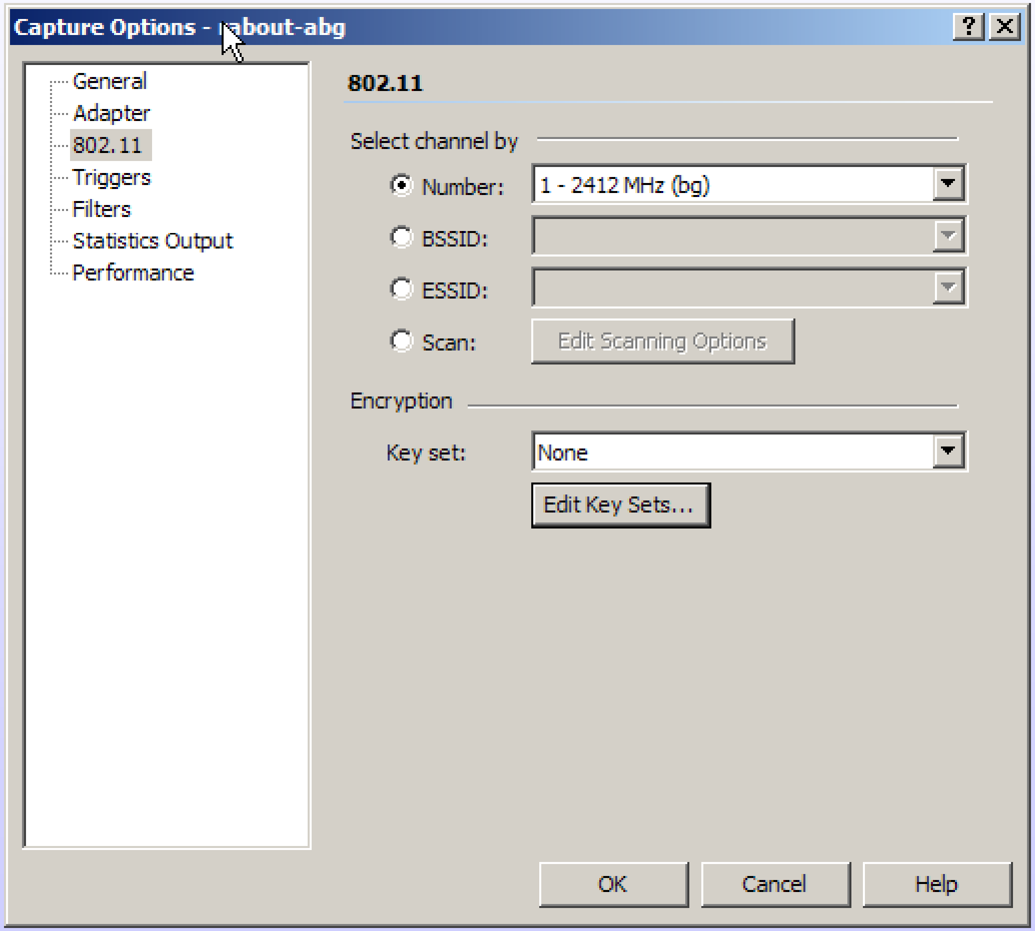
Adapter

- File
- Module: RFGrabber
- Local machine: GOBO
  - lan-UIB
  - Centrino
  - Senao_wireless

Property	Description
Device	Red Inalambrica Local 802.11b WLAN PC ...
Media	Wireless 802.11b
Address	00:02:6F:36:A6:2B
Link Speed	11 Mbits/s
WildPackets API	No

Airopeek

- Opciones de captura:



Capture Options - rabout-abg

802.11

Select channel by

● Number: 1 - 2412 MHz (bg)

○ BSSID:

○ ESSID:

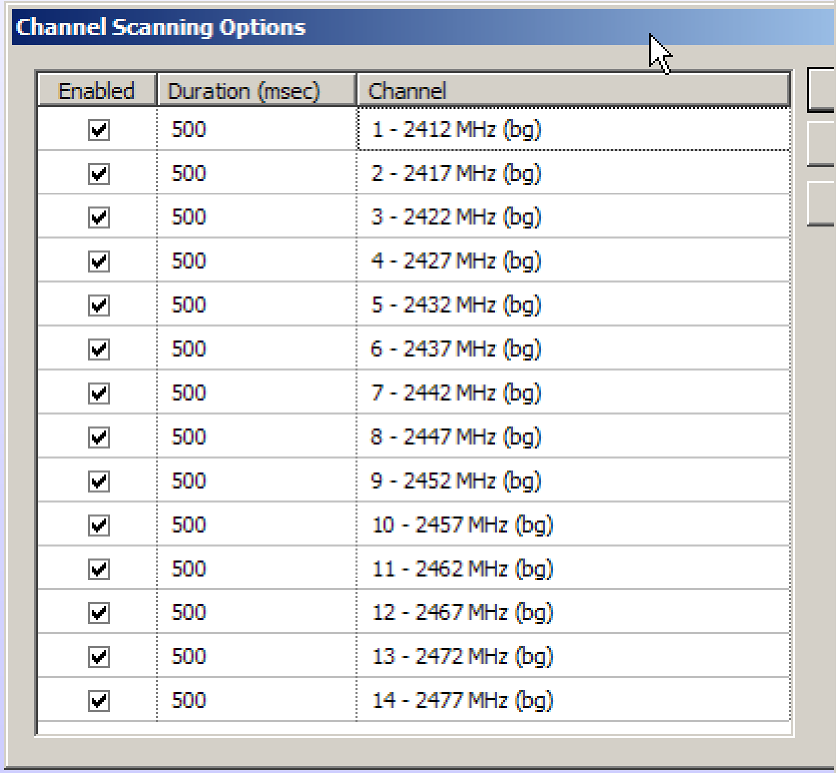
○ Scan: Edit Scanning Options

Encryption

Key set: None

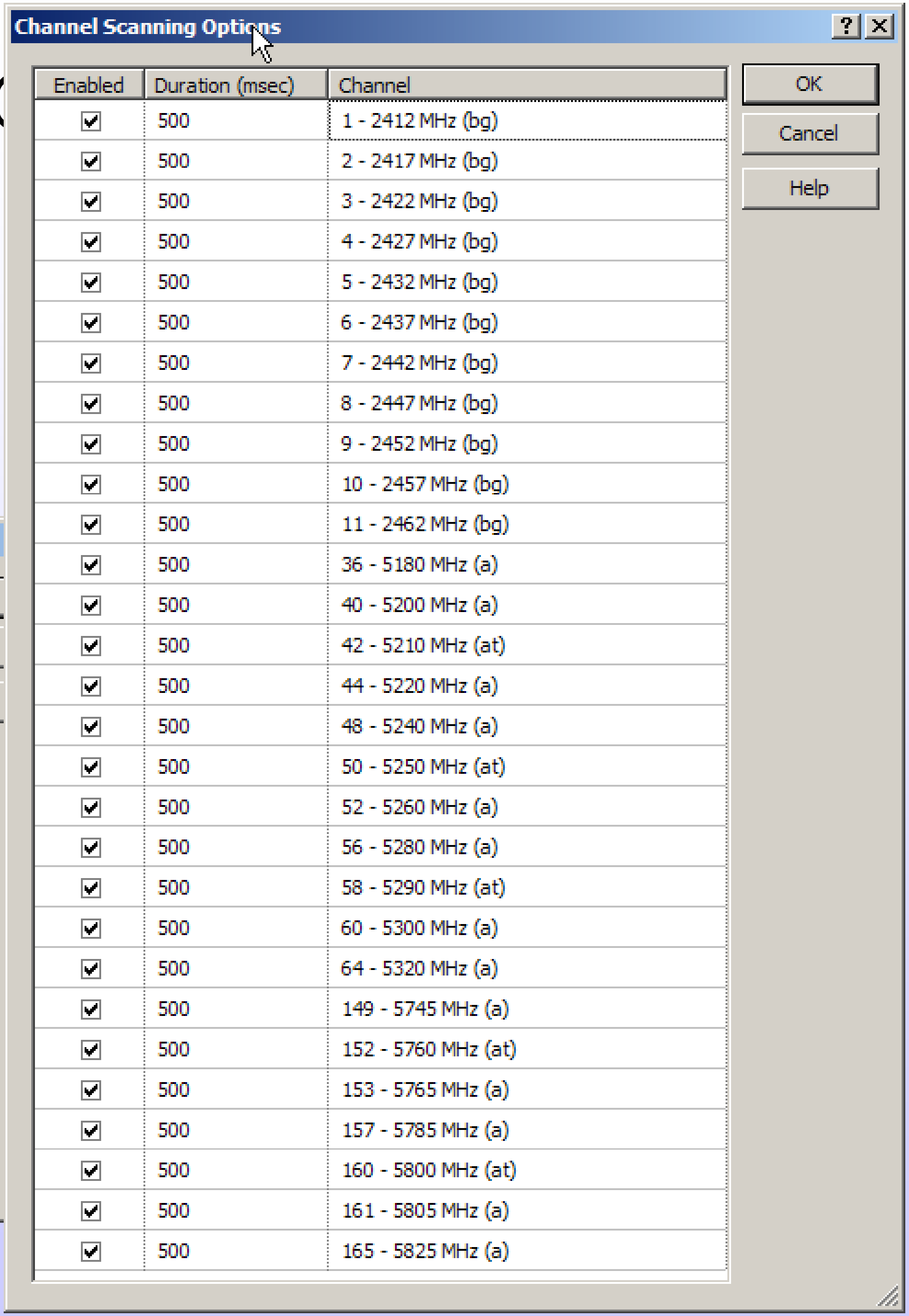
Airop

- Channel Scanning:



Channel Scanning Options

Enabled	Duration (msec)	Channel
☑	500	1 - 2412 MHz (bg)
☑	500	2 - 2417 MHz (bg)
☑	500	3 - 2422 MHz (bg)
☑	500	4 - 2427 MHz (bg)
☑	500	5 - 2432 MHz (bg)
☑	500	6 - 2437 MHz (bg)
☑	500	7 - 2442 MHz (bg)
☑	500	8 - 2447 MHz (bg)
☑	500	9 - 2452 MHz (bg)
☑	500	10 - 2457 MHz (bg)
☑	500	11 - 2462 MHz (bg)
☑	500	12 - 2467 MHz (bg)
☑	500	13 - 2472 MHz (bg)
☑	500	14 - 2477 MHz (bg)

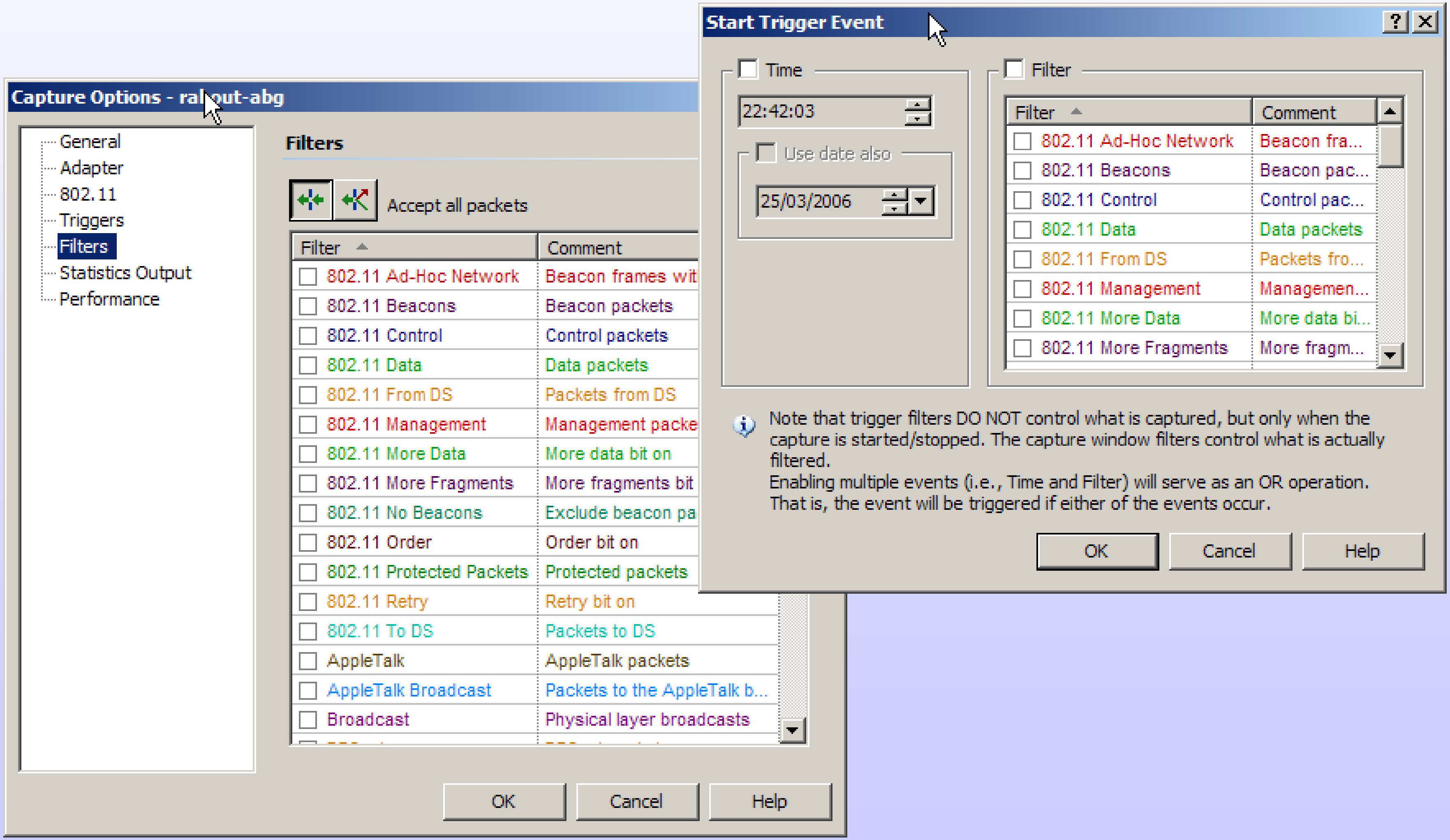


Channel Scanning Options

Enabled	Duration (msec)	Channel
☑	500	1 - 2412 MHz (bg)
☑	500	2 - 2417 MHz (bg)
☑	500	3 - 2422 MHz (bg)
☑	500	4 - 2427 MHz (bg)
☑	500	5 - 2432 MHz (bg)
☑	500	6 - 2437 MHz (bg)
☑	500	7 - 2442 MHz (bg)
☑	500	8 - 2447 MHz (bg)
☑	500	9 - 2452 MHz (bg)
☑	500	10 - 2457 MHz (bg)
☑	500	11 - 2462 MHz (bg)
☑	500	36 - 5180 MHz (a)
☑	500	40 - 5200 MHz (a)
☑	500	42 - 5210 MHz (at)
☑	500	44 - 5220 MHz (a)
☑	500	48 - 5240 MHz (a)
☑	500	50 - 5250 MHz (at)
☑	500	52 - 5260 MHz (a)
☑	500	56 - 5280 MHz (a)
☑	500	58 - 5290 MHz (at)
☑	500	60 - 5300 MHz (a)
☑	500	64 - 5320 MHz (a)
☑	500	149 - 5745 MHz (a)
☑	500	152 - 5760 MHz (at)
☑	500	153 - 5765 MHz (a)
☑	500	157 - 5785 MHz (a)
☑	500	160 - 5800 MHz (at)
☑	500	161 - 5805 MHz (a)
☑	500	165 - 5825 MHz (a)

Airopeek

- Filtros y triggers:



Capture Options - ralout-abg

Filters

Accept all packets

Filter	Comment
□ 802.11 Ad-Hoc Network	Beacon frames wit
□ 802.11 Beacons	Beacon packets
□ 802.11 Control	Control packets
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets from DS
□ 802.11 Management	Management packe
□ 802.11 More Data	More data bit on
□ 802.11 More Fragments	More fragments bit
□ 802.11 No Beacons	Exclude beacon pa
□ 802.11 Order	Order bit on
□ 802.11 Protected Packets	Protected packets
□ 802.11 Retry	Retry bit on
□ 802.11 To DS	Packets to DS
□ AppleTalk	AppleTalk packets
□ AppleTalk Broadcast	Packets to the AppleTalk b...
□ Broadcast	Physical layer broadcasts

Start Trigger Event

□ Time

22:42:03

□ Use date also

25/03/2006

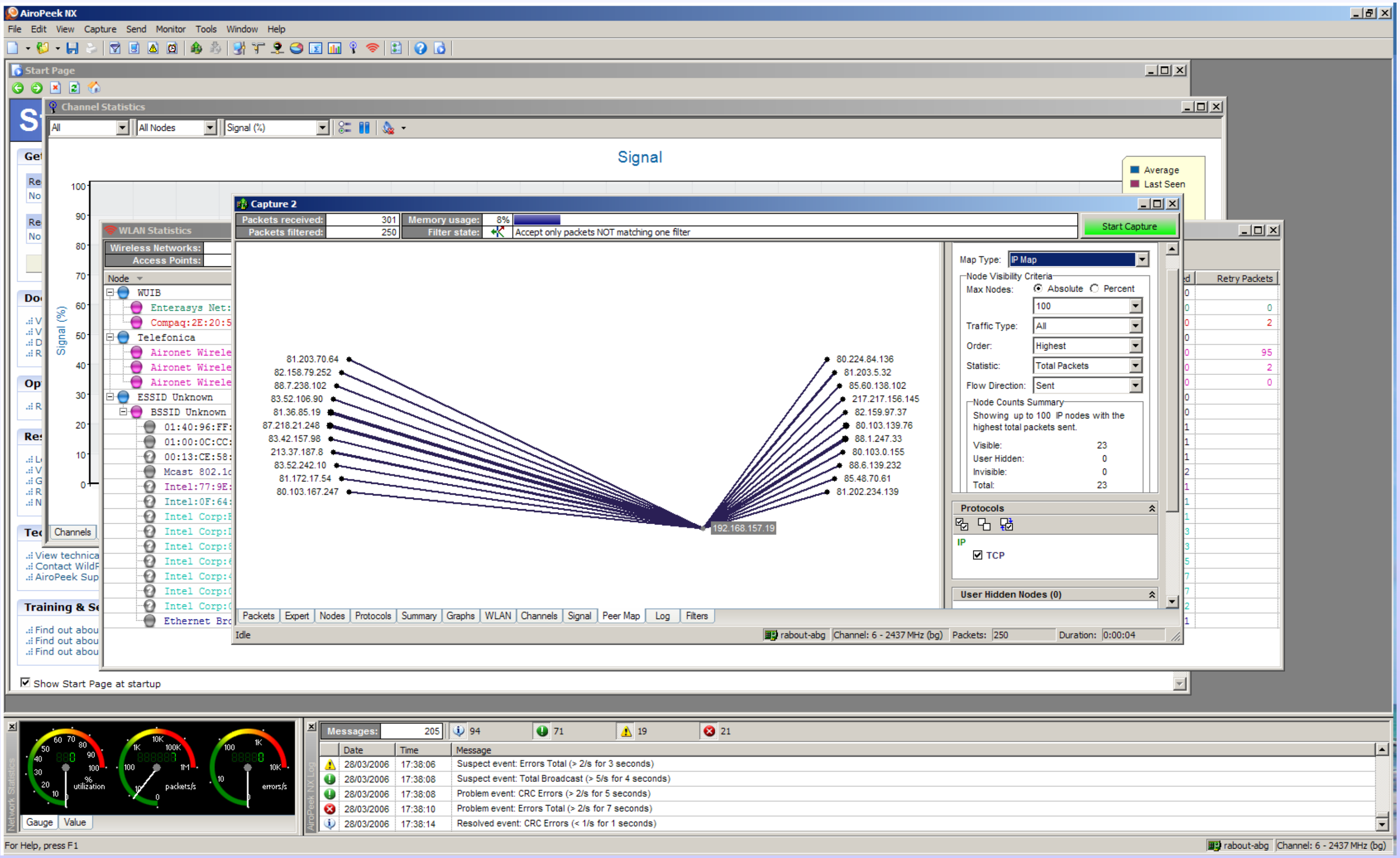
□ Filter

Filter	Comment
□ 802.11 Ad-Hoc Network	Beacon fra...
□ 802.11 Beacons	Beacon pac...
□ 802.11 Control	Control pac...
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets fro...
□ 802.11 Management	Managemen...
□ 802.11 More Data	More data bi...
□ 802.11 More Fragments	More fragm...

Note that trigger filters DO NOT control what is captured, but only when the capture is started/stopped. The capture window filters control what is actually filtered.
Enabling multiple events (i.e., Time and Filter) will serve as an OR operation. That is, the event will be triggered if either of the events occur.

Airopeek

- Capturas, estadísticas, peer-maps, etc...



Capture 2

Packets received:	301	Memory usage:	8%
Packets filtered:	250	Filter state:	Accept only packets NOT matching one filter

Map Type: IP Map

Node Visibility Criteria
Max Nodes: ● Absolute ○ Percent
100
Traffic Type: All
Order: Highest
Statistic: Total Packets
Flow Direction: Sent

Node Counts Summary
Showing up to 100 IP nodes with the highest total packets sent.

Visible:	23
User Hidden:	0
Invisible:	0
Total:	23

Protocols
IP
☑ TCP

User Hidden Nodes (0)

Idle rabout-abg Channel: 6 - 2437 MHz (bg) Packets: 250 Duration: 0:00:04

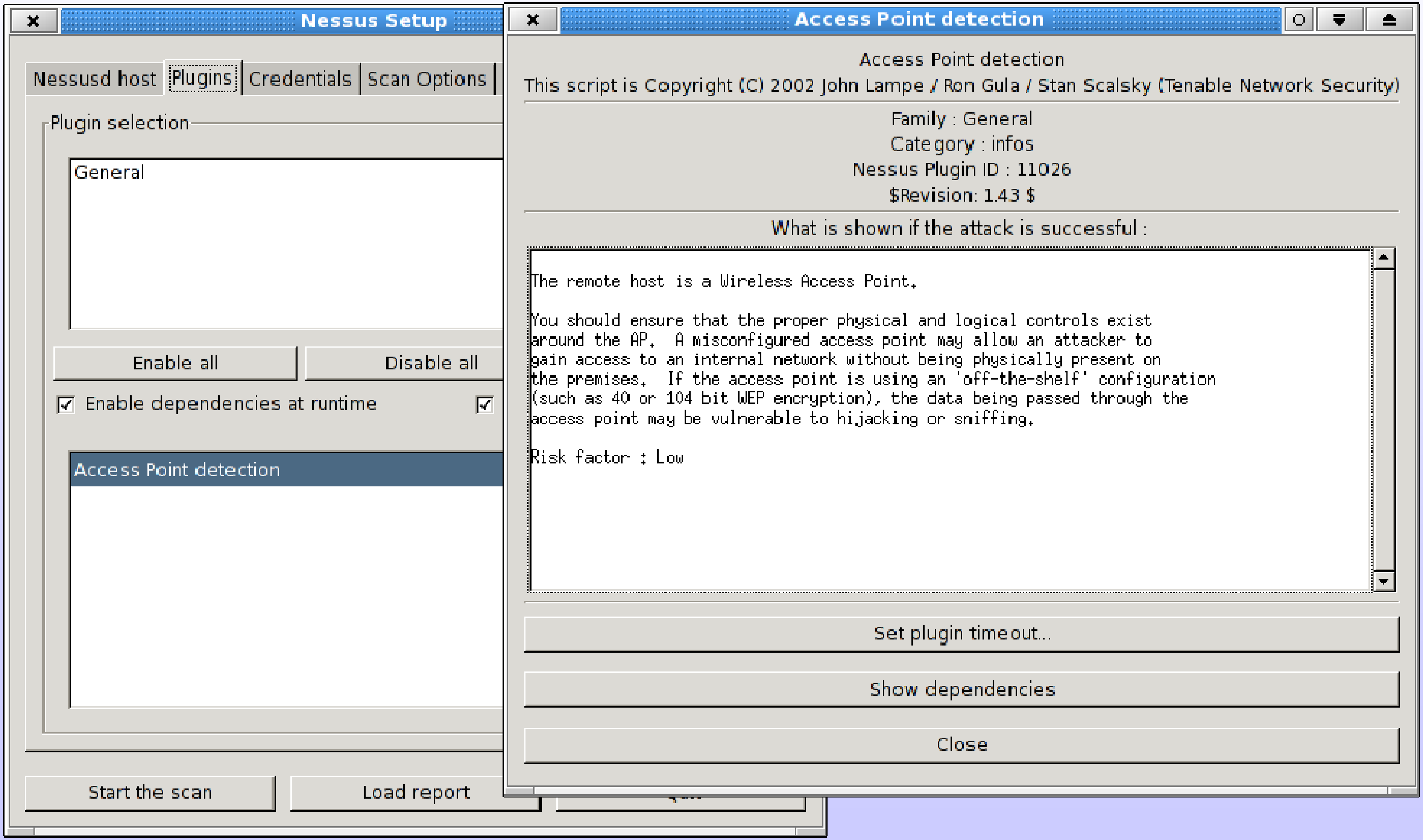
Messages: 205 94 71 19 21

	Date	Time	Message
⚠	28/03/2006	17:38:06	Suspect event: Errors Total (> 2/s for 3 seconds)
!	28/03/2006	17:38:08	Suspect event: Total Broadcast (> 5/s for 4 seconds)
!	28/03/2006	17:38:08	Problem event: CRC Errors (> 2/s for 5 seconds)
✖	28/03/2006	17:38:10	Problem event: Errors Total (> 2/s for 7 seconds)
ℹ	28/03/2006	17:38:14	Resolved event: CRC Errors (< 1/s for 1 seconds)

rabout-abg Channel: 6 - 2437 MHz (bg)

Nessus

- Fingerprinting de APs



Access Point detection

This script is Copyright (C) 2002 John Lampe / Ron Gula / Stan Scalsky (Tenable Network Security)

Family : General
Category : infos
Nessus Plugin ID : 11026
$Revision: 1.43 $

What is shown if the attack is successful :

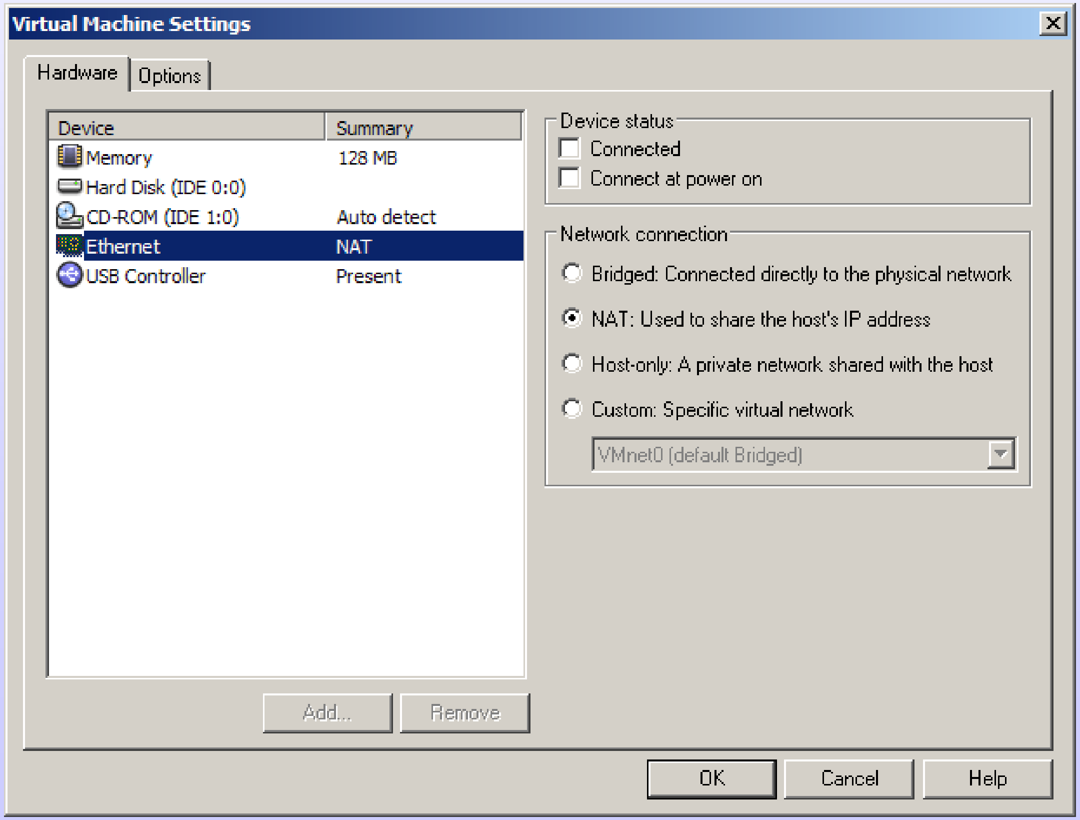
```
The remote host is a Wireless Access Point.

You should ensure that the proper physical and logical controls exist
around the AP.  A misconfigured access point may allow an attacker to
gain access to an internal network without being physically present on
the premises.  If the access point is using an 'off-the-shelf' configuration
(such as 40 or 104 bit WEP encryption), the data being passed through the
access point may be vulnerable to hijacking or sniffing.

Risk factor : Low
```

Windows y linux

- Un equipo con windows y linux analizando ambos en modo RFMon....
  - VMware!! http://www.vmware.com/
- Problemática:
  - VMware permite crear máquinas virtuales
  - Virtualiza: Discos, ethernet, usb,... pero wifi? → No!!
  - No tenemos acceso a los dispositivos wifi....

Windows y Linux

- Solución:
  - Llaves USB-wifi!!!
  - Se virtualiza el controlador USB



Virtual Machine Settings

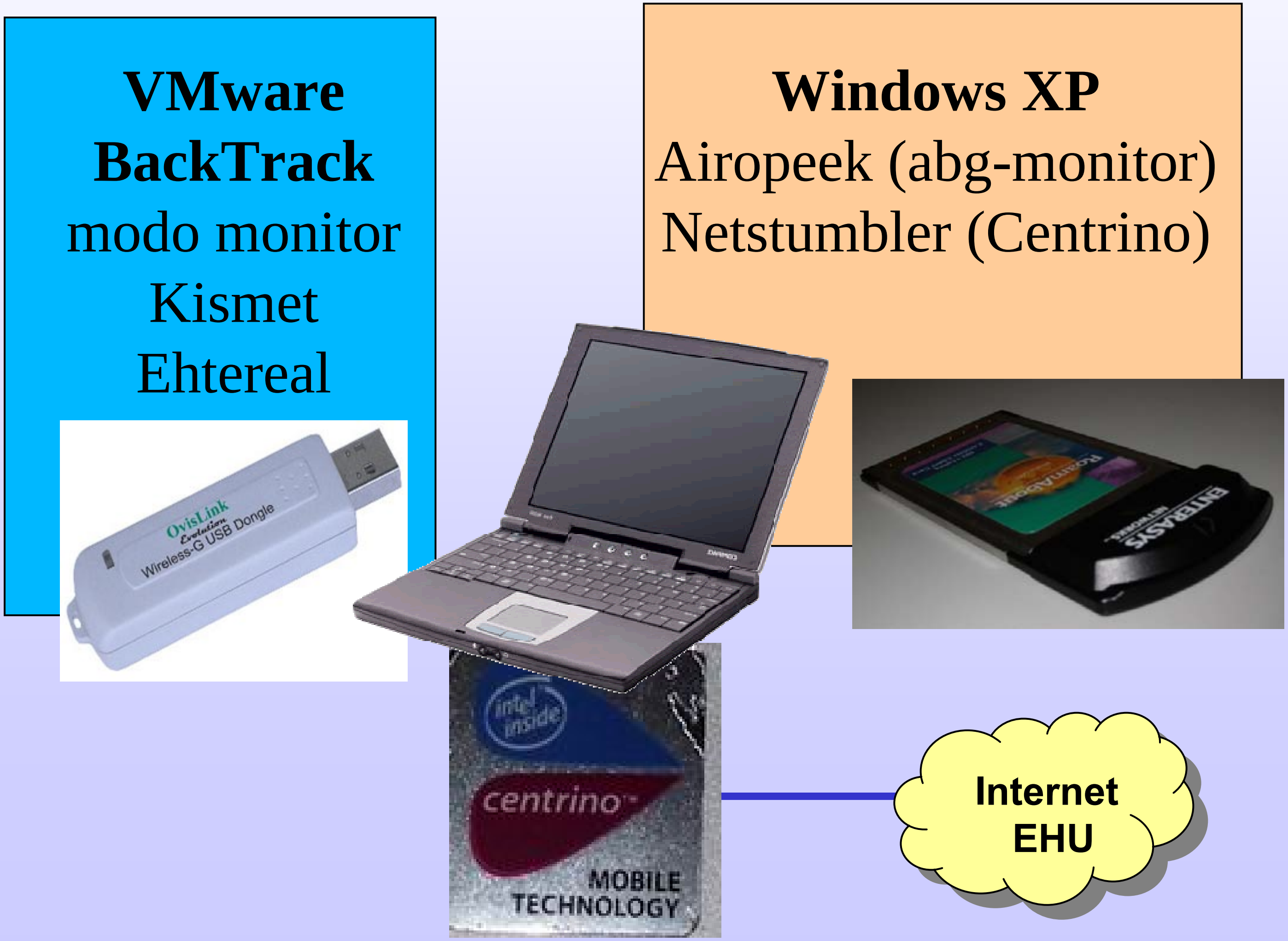
Device	Summary
Memory	128 MB
Hard Disk (IDE 0:0)	
CD-ROM (IDE 1:0)	Auto detect
Ethernet	NAT
USB Controller	Present

Device status
□ Connected
□ Connect at power on

Network connection
○ Bridged: Connected directly to the physical network
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0 (default Bridged)

Windows y linux

- Equipo dual windows-linux para wifi

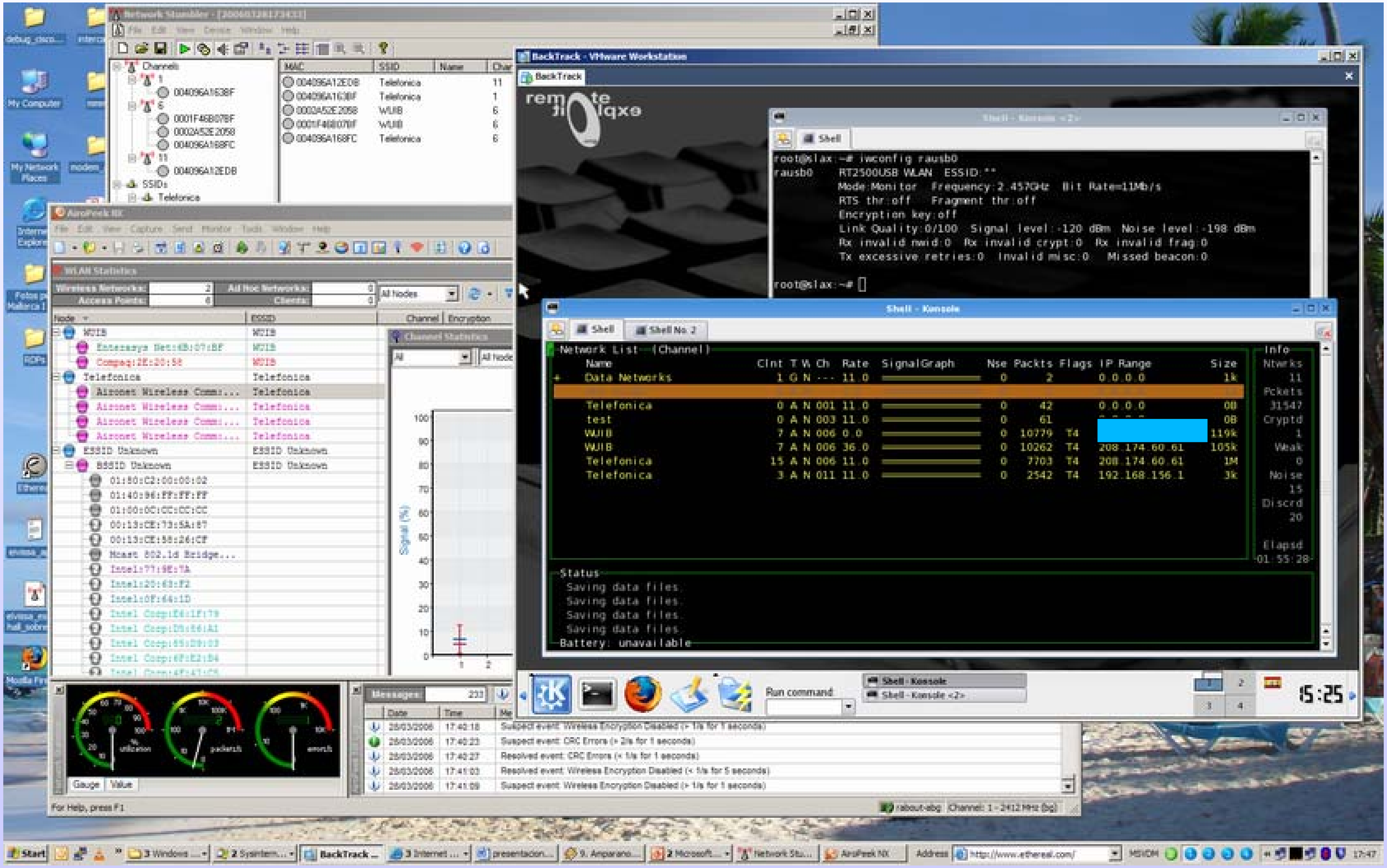


VMware
BackTrack
modo monitor
Kismet
Ehtereal

Windows XP
Airopeek (abg-monitor)
Netstumbler (Centrino)

Internet
EHU

Windows y Linux



```
Channels
  1
    004096A1638F
  6
    0001F46B078F
    0002A52E2058
    004096A169FC
  11
    004096A12EDB
SSIDs
  Telefonica
```

MAC	SSID	Name	Chan
004096A12EDB	Telefonica		11
004096A1638F	Telefonica		1
0002A52E2058	WUIB		6
0001F46B078F	WUIB		6
004096A169FC	Telefonica		6

Wireless Networks:	2	Ad Hoc Networks:	0
Access Points:	6	Clients:	0

All Nodes

Node	ESSID
WUIB	WUIB
Enterasys Net:4B:07:BF	WUIB
Compaq:2E:20:58	WUIB
Telefonica	Telefonica
Aironet Wireless Comm:...	Telefonica
Aironet Wireless Comm:...	Telefonica
Aironet Wireless Comm:...	Telefonica
Aironet Wireless Comm:...	Telefonica
ESSID Unknown	ESSID Unknown
BSSID Unknown	ESSID Unknown
01:80:C2:00:00:02	
01:40:96:FF:FF:FF	
01:00:0C:CC:CC:CC	
00:13:CE:73:5A:87	
00:13:CE:58:26:CF	
Mcast 802.1d Bridge...	
Intel:77:9E:7A	
Intel:20:63:F2	
Intel:0F:64:1D	
Intel Corp:E6:1F:79	
Intel Corp:D5:56:A1	
Intel Corp:65:D9:03	
Intel Corp:6F:E2:B4	
Intel Corp:4F:41:C5	

Messages: 233

Date	Time	Message
28/03/2006	17:40:18	Suspect event: Wireless Encryption Disabled (> 1/s for 1 seconds)
28/03/2006	17:40:23	Suspect event: CRC Errors (> 2/s for 1 seconds)
28/03/2006	17:40:27	Resolved event: CRC Errors (< 1/s for 1 seconds)
28/03/2006	17:41:03	Resolved event: Wireless Encryption Disabled (< 1/s for 5 seconds)
28/03/2006	17:41:09	Suspect event: Wireless Encryption Disabled (> 1/s for 1 seconds)

rabout-abg Channel: 1 - 2412 MHz (bg)

```
root@slax:~# iwconfig rausb0
rausb0    RT2500USB WLAN  ESSID:""
          Mode:Monitor  Frequency:2.457GHz  Bit Rate=11Mb/s
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Link Quality:0/100  Signal level:-120 dBm  Noise level:-198 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

root@slax:~# 
```

```
Network List (Channel)                                                          Info
     Name                  Clnt T W Ch  Rate SignalGraph  Nse Packts Flags IP Range      Size  Ntwrks
 +   Data Networks            1 G N --- 11.0 ==========    0      2       0.0.0.0          1k    11
     [illegible]                                                                                Pckets
     Telefonica               0 A N 001 11.0 ==========    0     42       0.0.0.0          0B  31547
     test                     0 A N 003 11.0 ==========    0     61       [redacted]       0B  Cryptd
     WUIB                     7 A N 006  0.0 ==========    0  10779 T4                   119k     1
     WUIB                     7 A N 006 36.0 ==========    0  10262 T4    208.174.60.61  105k  Weak
     Telefonica              15 A N 006 11.0 ==========    0   7703 T4    208.174.60.61    1M     0
     Telefonica               3 A N 011 11.0 ==========    0   2542 T4    192.168.156.1    3k  Noise
                                                                                                  15
                                                                                                Discrd
                                                                                                  20

                                                                                                Elapsd
                                                                                              01:55:28
Status
 Saving data files.
 Saving data files.
 Saving data files.
 Saving data files.
Battery: unavailable
```

Agenda

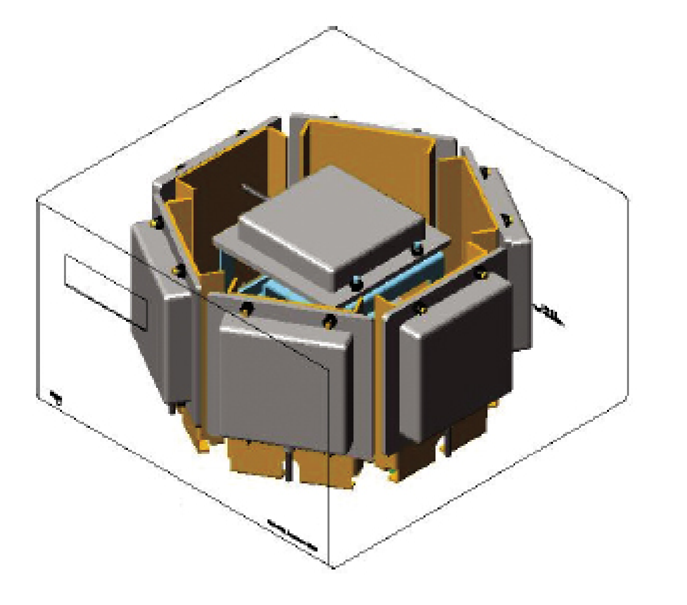
- ¿Qué es wifi?
- Escenarios
- Cobertura
- Arquitectura y gestión de red
- Cifrado
- Control de acceso: autenticación
- Mantenimiento de la red
- Monitorización y securización
- Herramientas
- Sistemas IDS

Sistemas IDS

- Sistemas IDS
  - IDS wired vs. IDS wireless
  - Escaneo según patrones conocidos: MAC, SNMP, servicios, tráfico, etc …
  - Los APs informan sobre los APs vecinos
  - Sondas en nuestros clientes que informan a un colector

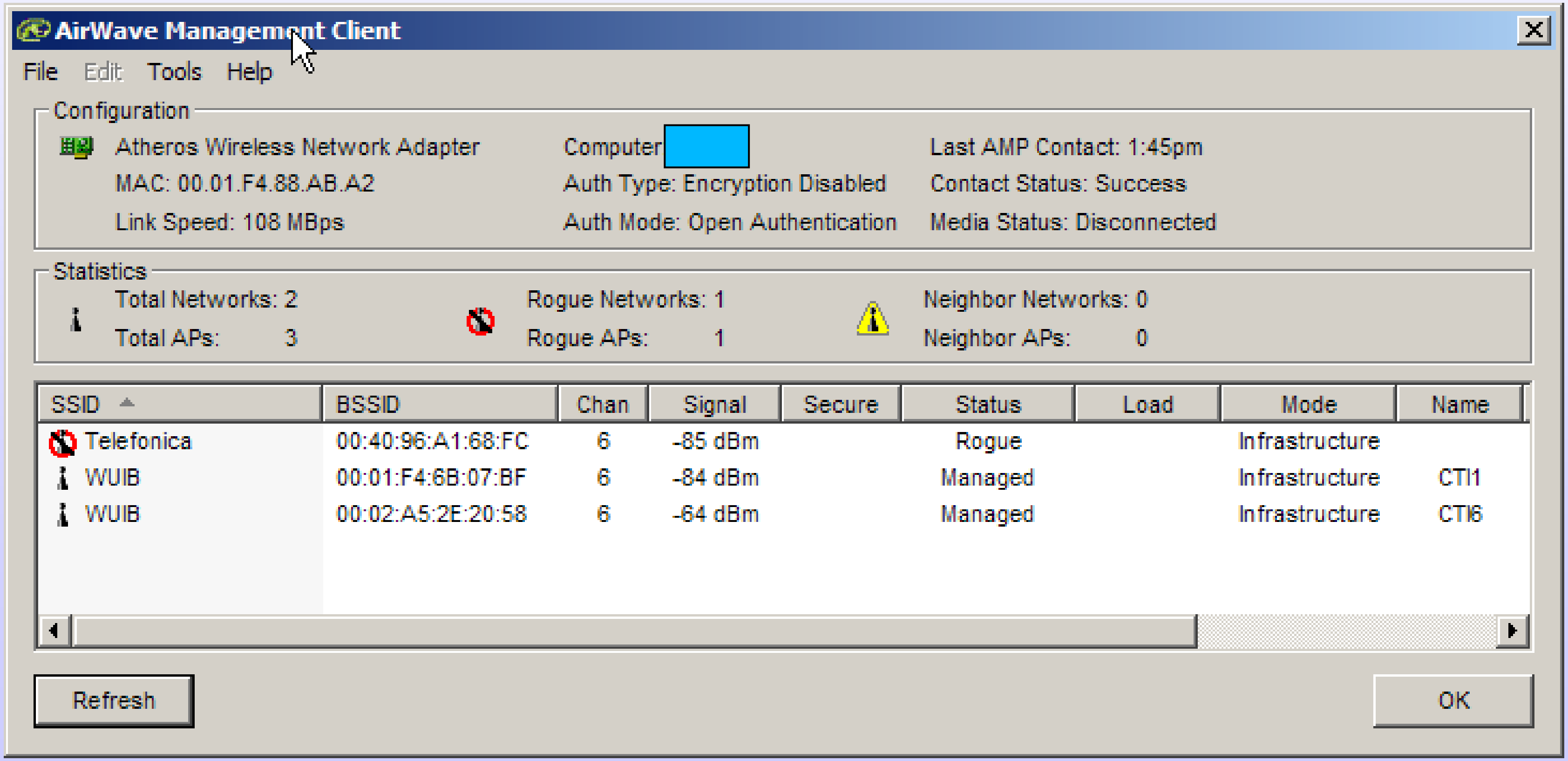
IDS de alta sensibilidad

- Producto IDS Bluesocket
  - Un AP de 8 antenas para un edificio de 5 plantas....



RAPIDS: Clientes IDS

- IDS instalado en un cliente (tipo netstumbler)
  - Informan a la plataforma de gestión



Configuration

Atheros Wireless Network Adapter
MAC: 00.01.F4.88.AB.A2
Link Speed: 108 MBps

Computer [redacted]
Auth Type: Encryption Disabled
Auth Mode: Open Authentication

Last AMP Contact: 1:45pm
Contact Status: Success
Media Status: Disconnected

Statistics

Total Networks: 2
Total APs: 3

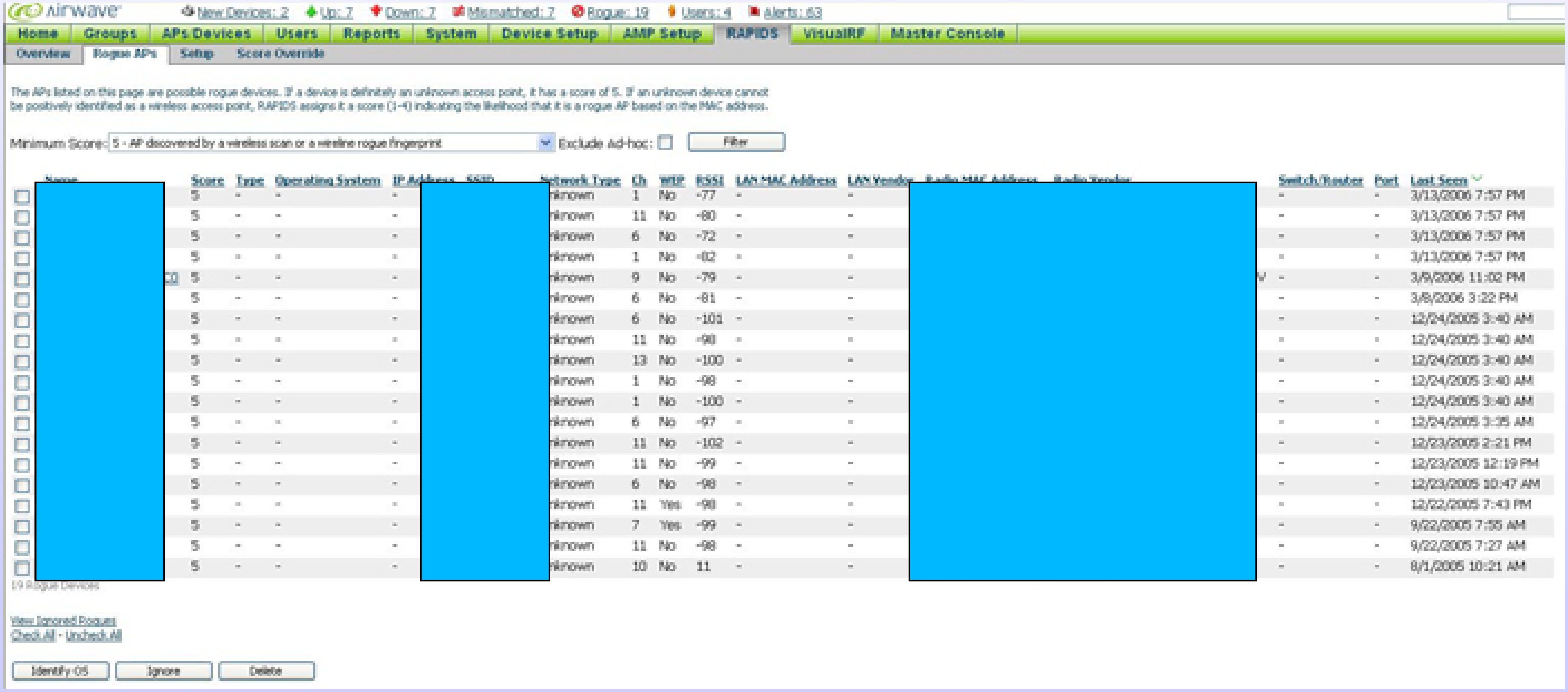
Rogue Networks: 1
Rogue APs: 1

Neighbor Networks: 0
Neighbor APs: 0

SSID	BSSID	Chan	Signal	Secure	Status	Load	Mode	Name
Telefonica	00:40:96:A1:68:FC	6	-85 dBm		Rogue		Infrastructure	
WUIB	00:01:F4:6B:07:BF	6	-84 dBm		Managed		Infrastructure	CTI1
WUIB	00:02:A5:2E:20:58	6	-64 dBm		Managed		Infrastructure	CTI6

RAPIDS: Plataforma de gestión

- Recibe información de los clientes (tipo Netstumbler)
- Realiza scans wired fingerprinting (tipo Nessus)



The APs listed on this page are possible rogue devices. If a device is definitely an unknown access point, it has a score of 5. If an unknown device cannot be positively identified as a wireless access point, RAPIDS assigns it a score (1-4) indicating the likelihood that it is a rogue AP based on the MAC address.

Minimum Score: 5 - AP discovered by a wireless scan or a wireline rogue fingerprint Exclude Ad-hoc: ☐ Filter

	Name	Score	Type	Operating System	IP Address	SSID	Network Type	Ch	WEP	RSSI	LAN MAC Address	LAN Vendor	Radio MAC Address	Radio Vendor	Switch/Router	Port	Last Seen
☐	[redacted]	5	-	-	-	[redacted]	nknown	1	No	-77	-	-	[redacted]	[redacted]	-	-	3/13/2006 7:57 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	No	-80	-	-	[redacted]	[redacted]	-	-	3/13/2006 7:57 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	6	No	-72	-	-	[redacted]	[redacted]	-	-	3/13/2006 7:57 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	1	No	-82	-	-	[redacted]	[redacted]	-	-	3/13/2006 7:57 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	9	No	-79	-	-	[redacted]	[redacted]	-	-	3/9/2006 11:02 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	6	No	-81	-	-	[redacted]	[redacted]	-	-	3/8/2006 3:22 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	6	No	-101	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:40 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	No	-98	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:40 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	13	No	-100	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:40 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	1	No	-98	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:40 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	1	No	-100	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:40 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	6	No	-97	-	-	[redacted]	[redacted]	-	-	12/24/2005 3:35 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	No	-102	-	-	[redacted]	[redacted]	-	-	12/23/2005 2:21 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	No	-99	-	-	[redacted]	[redacted]	-	-	12/23/2005 12:19 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	6	No	-98	-	-	[redacted]	[redacted]	-	-	12/23/2005 10:47 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	Yes	-98	-	-	[redacted]	[redacted]	-	-	12/22/2005 7:43 PM
☐	[redacted]	5	-	-	-	[redacted]	nknown	7	Yes	-99	-	-	[redacted]	[redacted]	-	-	9/22/2005 7:55 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	11	No	-98	-	-	[redacted]	[redacted]	-	-	9/22/2005 7:27 AM
☐	[redacted]	5	-	-	-	[redacted]	nknown	10	No	11	-	-	[redacted]	[redacted]	-	-	8/1/2005 10:21 AM

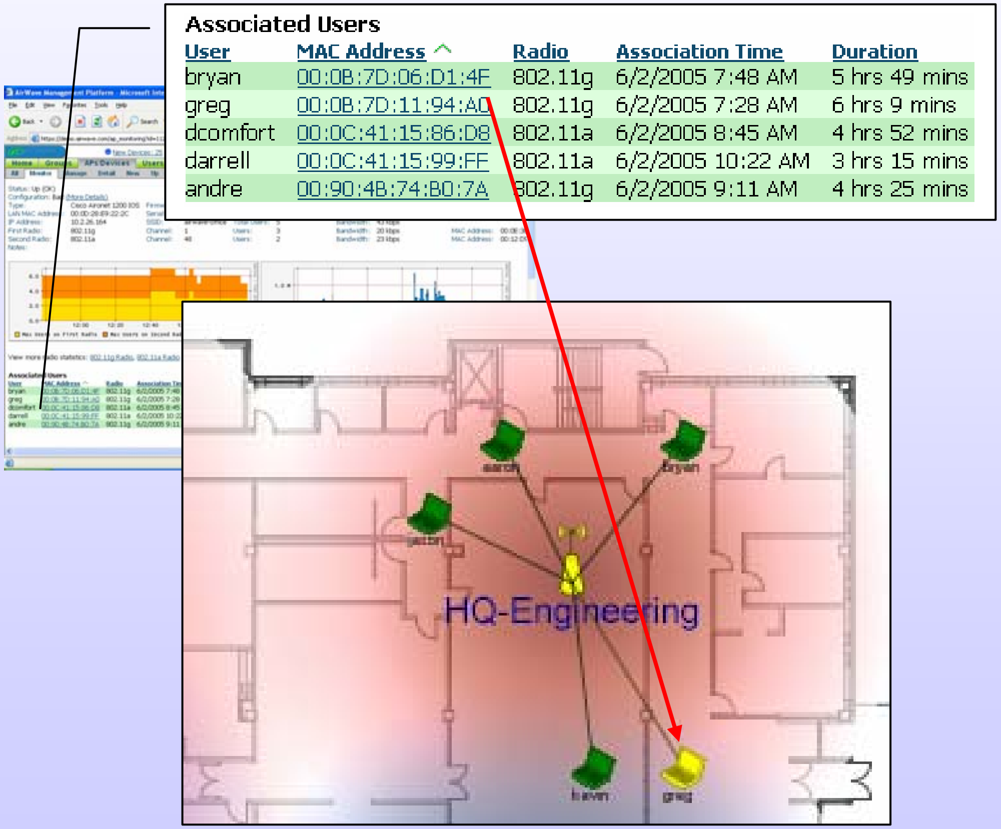
19 Rogue Devices

View Ignored Rogues
Check All - Uncheck All

Localización de usuarios maliciosos

- Utiliza la información de la plataforma de gestión

User-based Monitoring & Diagnostics

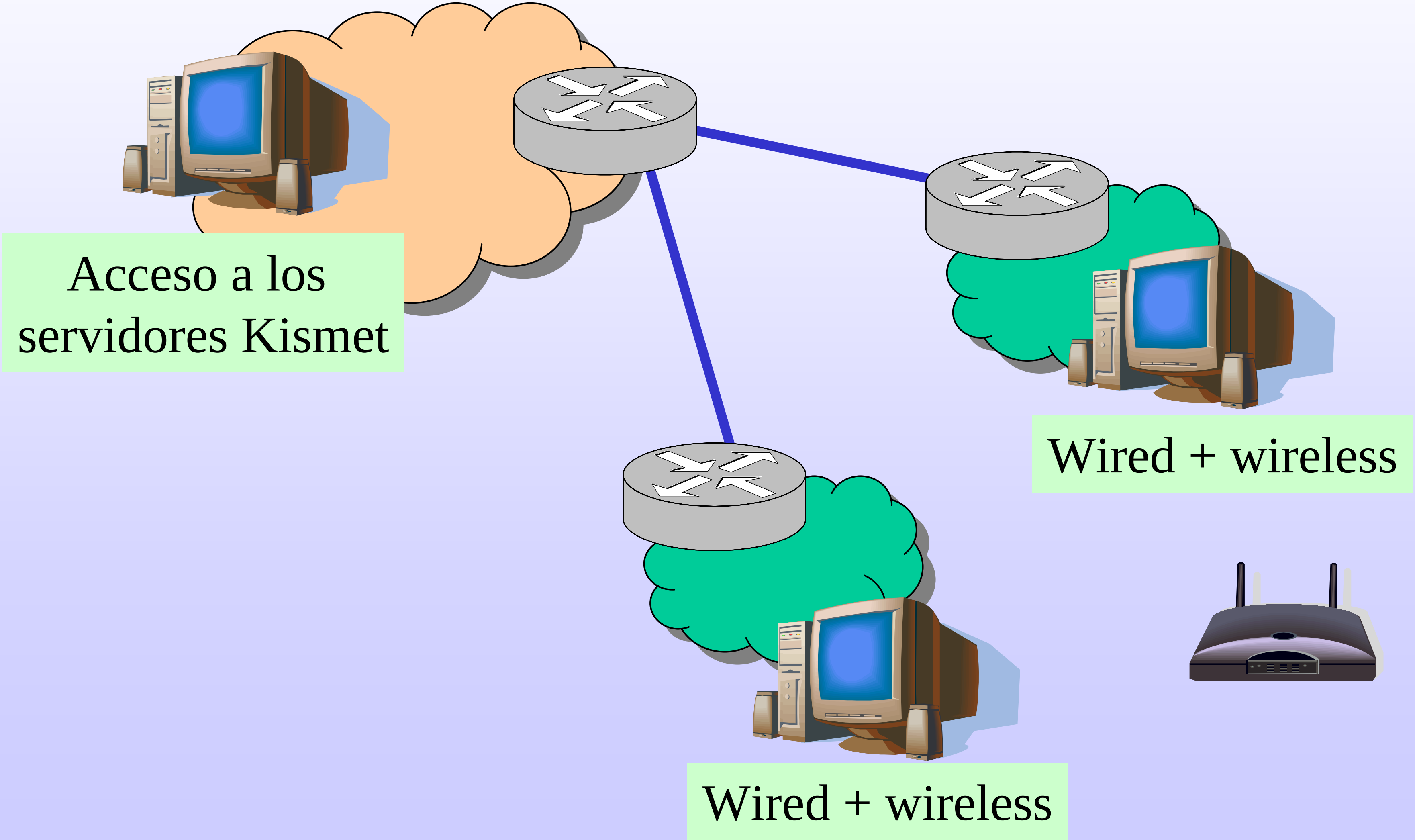


Associated Users

User	MAC Address	Radio	Association Time	Duration
bryan	00:0B:7D:06:D1:4F	802.11g	6/2/2005 7:48 AM	5 hrs 49 mins
greg	00:0B:7D:11:94:A0	802.11g	6/2/2005 7:28 AM	6 hrs 9 mins
dcomfort	00:0C:41:15:86:D8	802.11a	6/2/2005 8:45 AM	4 hrs 52 mins
darrell	00:0C:41:15:99:FF	802.11a	6/2/2005 10:22 AM	3 hrs 15 mins
andre	00:90:4B:74:B0:7A	802.11g	6/2/2005 9:11 AM	4 hrs 25 mins

Sondas Kismet

- Cliente-Servidor

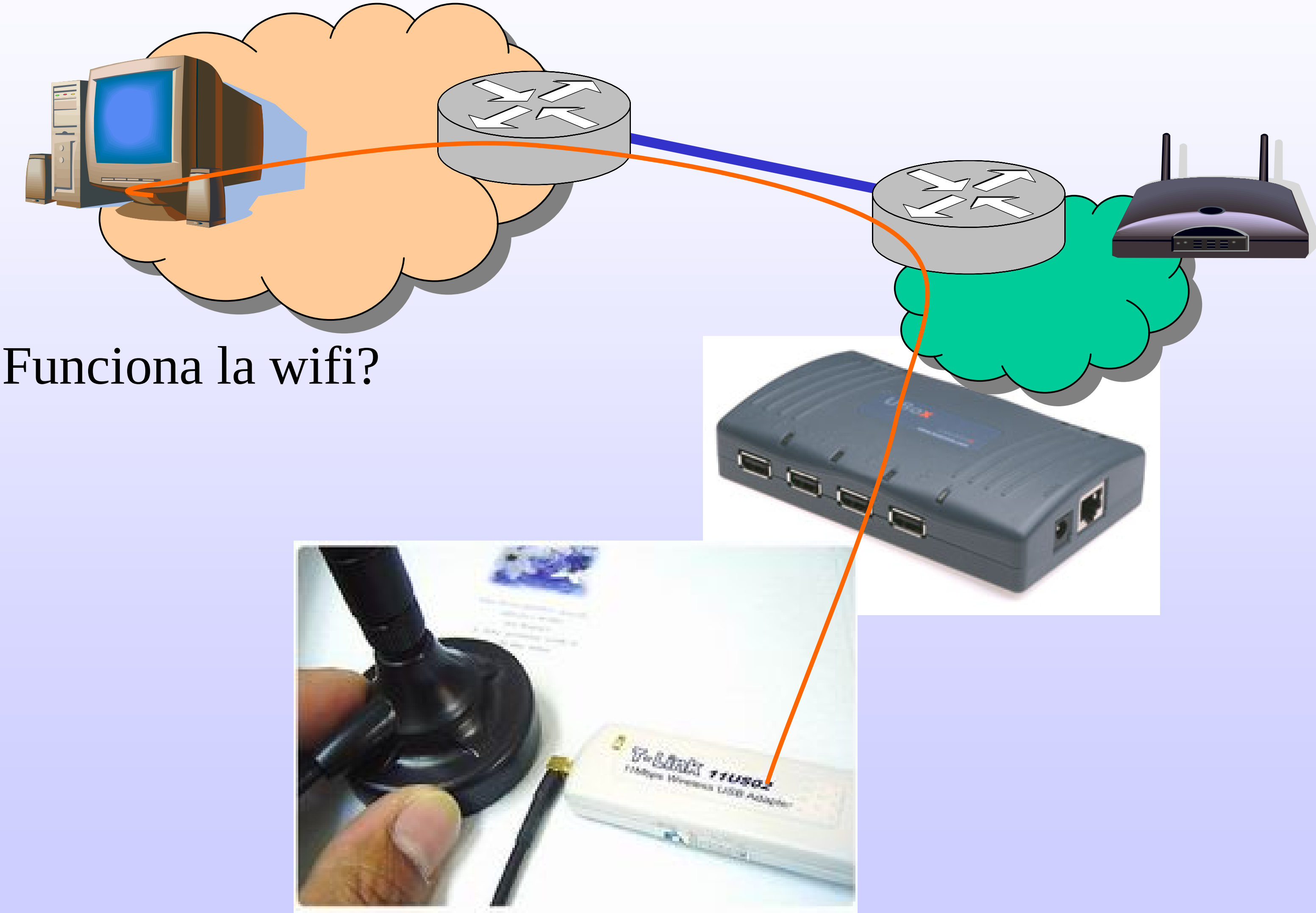


Acceso a los servidores Kismet

Wired + wireless

Wired + wireless

Sondas USB-Network



¿Funciona la wifi?

Conclusiones

- La seguridad
  - Presente desde el principio y en todas las fases del proyecto
- Imprescindible conocer las soluciones de los fabricantes
  - Conocer los protocolos no es suficiente
- Estudiar el entorno
  - Es un trabajo diario!!!
- Consolidar los indicadores
  - Sondas, Logs, IDS, Firewalls,...
- Conocer las herramientas de los enemigos
  - No basta con cerrar los ojos

Referencias

- http://www.remote-exploit.org
- http://slax.linux-live.org
- http://www.ethereal.com/
- http://www.knoppix.org/
- http://www.kismetwireless.net/
- http://www.rediris.es/jt/jt2005/archivo/archivo-jt.es.html

Gracias!!!

Toni Pérez
toni.perez@uib.es