WiUZ
Red inalámbrica de la Universidad de Zaragoza

José Antonio Valero Sánchez
javalero@unizar.es

Indice

1. Red Wifi de la Universidad de Zaragoza
   - Diseño
     - Hardware
     - Software
     - Clientes
   - Eduroam
   - Explotación
2. Problemas en la implantación/explotación
3. Problemas de Seguridad

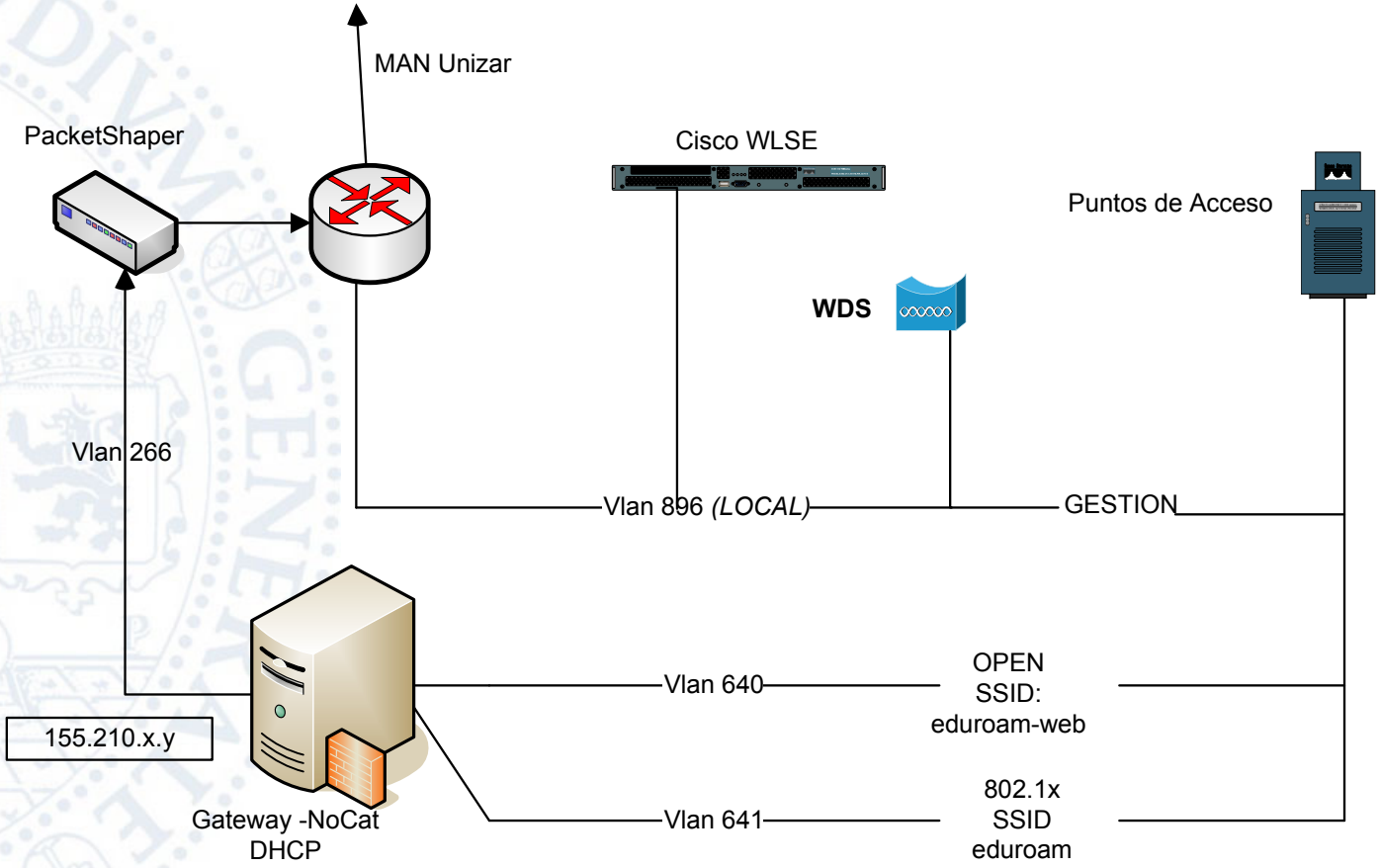
Diseño (I)

- Inicialmente:
  - Wiuz-1(Red abierta con nocat)
  - Wiuz-2 (802.1X)

Posteriormente:

- Wiuz-1 → Eduroam-Web
- Wiuz-2 → Eduroam (802.1X EAP-TTLS /WPA/WPA2)

Diseño (II)


MAN Unizar
PacketShaper
Cisco WLSE
Puntos de Acceso
WDS
Vlan 266
Vlan 896 (LOCAL)
GESTION
Vlan 640
OPEN
SSID:
eduroam-web
155.210.x.y
Gateway -NoCat
DHCP
Vlan 641
802.1x
SSID
eduroam

Componentes (Hardware)

Hardware Instalado

- Puntos de Acceso
  - 66 Cisco 1100
  - 161 Cisco 1131 (Activos 802.11b/g)
  - 2 Cisco 1300 (Enlace entre edificios)
- Equipamiento de Gestión
  - 3 Servidores
  - 1 appliance Cisco WLSE
  - 6 Ap en modo WDS

Componentes (Software)

Software Instalado

- Puntos de Acceso
  - Cisco IOS 12.3.7 JA2
- Equipamiento de Gestión
  - Linux Centos 4.2
  - Cisco WLSE 2.13
  - HP Openview 7.0.1
  - Nocat 0.82
  - Freeradius 1.0.1
  - Cisco ACS 3.3

Componentes (Clientes)

- Eduroam-Web
  - Red abierta sin cifrar
  - Servidor NoCat
  - Fácil acceso y configuración
  - Red con mayor número de usuarios
  - Sin restricciones actuales

Componentes (Clientes)

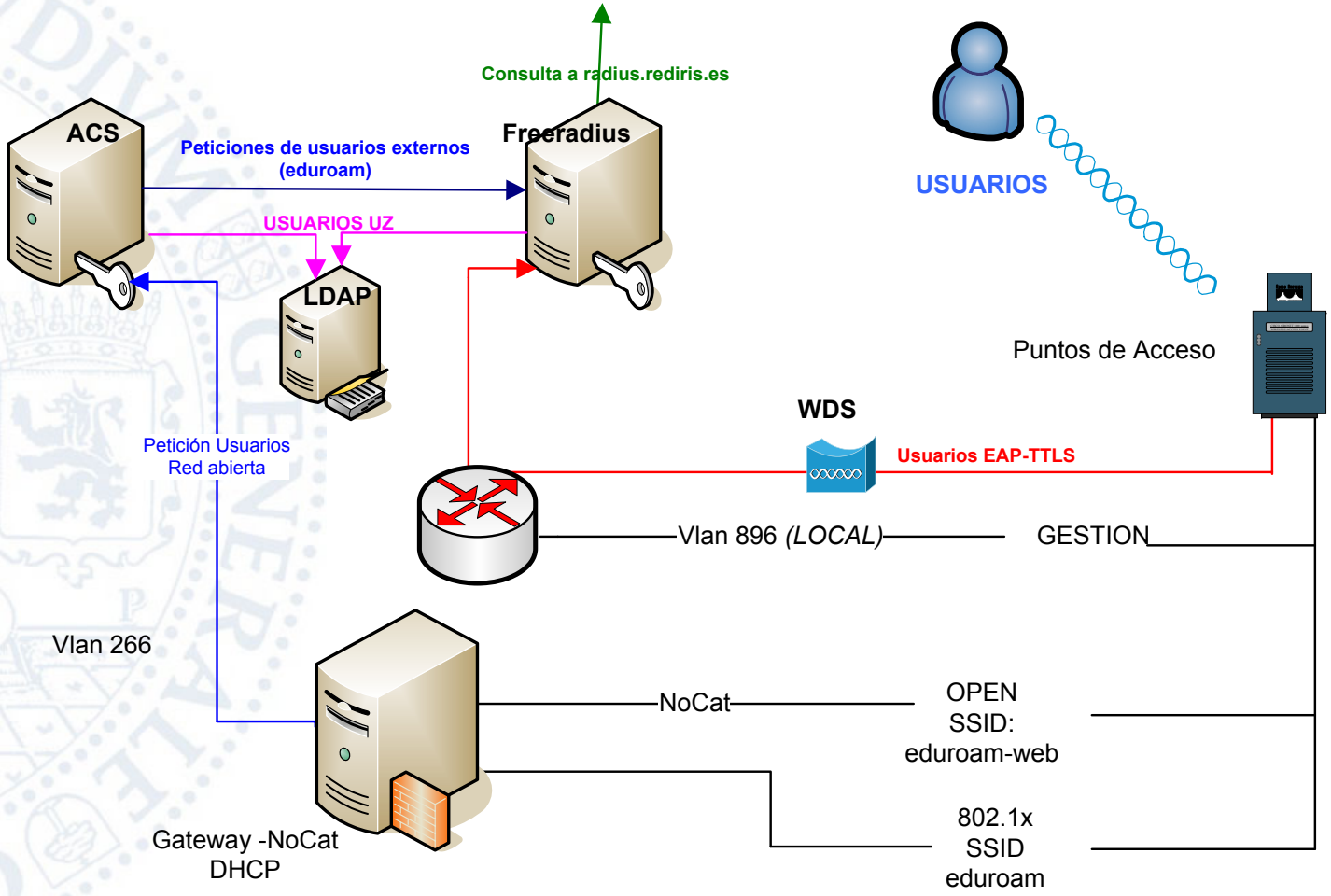
- Eduroam
  - Red Cifrada (WPA/WPA2 Mixed Mode)
  - Sin restricciones
  - 802.1X EAP-TTLS/PAP
  - Securew2 para Windows
  - Sólo algunas tarjetas la soportan

Componentes

Tendencias futuras

- Terminar el despliegue en todos los campus
- Motivar a los usuarios a usar la red cifrada
- Limitar usos de la red eduroam-web
- Redundancia de servidores a nivel de campus

Eduroam


Consulta a radius.rediris.es
ACS
Peticiones de usuarios externos
(eduroam)
Freeradius
USUARIOS
USUARIOS UZ
LDAP
Puntos de Acceso
WDS
Petición Usuarios
Red abierta
Usuarios EAP-TTLS
Vlan 896 (LOCAL)
GESTION
Vlan 266
NoCat
OPEN
SSID:
eduroam-web
Gateway -NoCat
DHCP
802.1x
SSID
eduroam

Explotación

- Herramientas de control y gestión
  - Gestión de Puntos de Acceso
    - WLSE
    - HP Openview NNM
    - Scripts en Expect
  - Control de Usuarios
    - Scripts en Perl
    - WLSE
    - Arptrack
    - Herramientas propias del servidor Nocat
  - Control de “qué hacen” los usuarios
    - PacketShaper
    - NetFlow 5

Gestión de Puntos de Acceso WLSE

Usos WLSE:

- IDS
- Detector de fallos
- Actualización del firmware
- Generación de reports
- Configurar canales
- Mapas de cobertura
- Control de usuarios

IDS- ROGUE ACCESS POINT

Rogue Access Point Details

BSSID	State	Vendor	
001195c25a8f	Rogue Access Point	Alpha Networks Inc.	Change to Friendly / Delete

Beacon Information

SSID	Beacon Interval	Channel	PHY	Data Rates
"\x00\x00\x00\x00\x00\x00" [6]	100	1	802.11g	Basic: 1.0Mbps, Basic: 2.0Mbps, Basic: 5.5Mbps, Basic: 11.0Mbps, 6.0Mbps, 12.0Mbps, 24.0Mbps, 36.0Mbps 9.0Mbps, 18.0Mbps, 48.0Mbps, 54.0Mbps

Location Estimation

Location	Timestamp	
Location could not be determined. Reporting AP location was not specified.	Wed Mar 08 16:43:46 UTC 2006	View in Location Manager

Switch Port Tracing

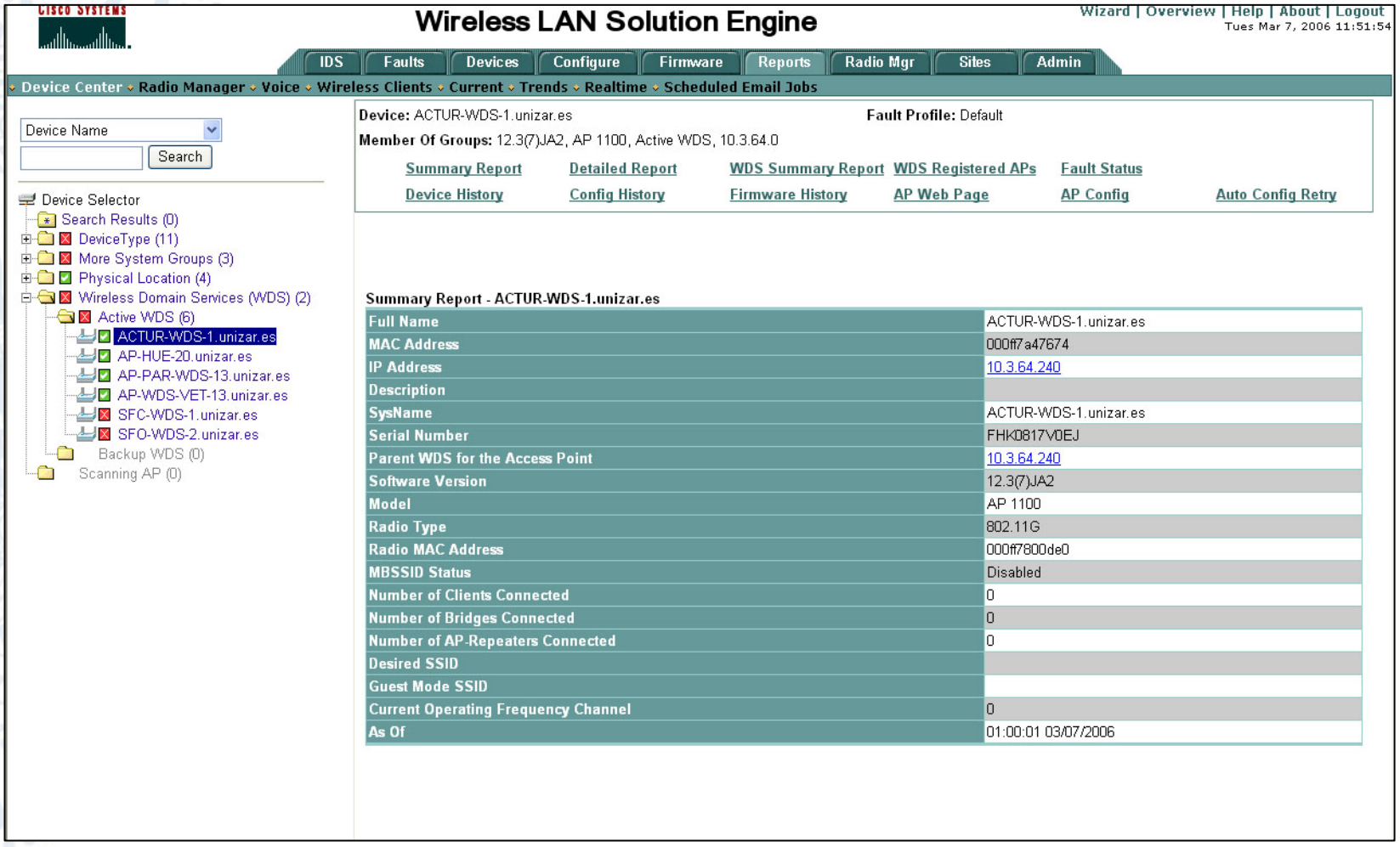
Switch IP	Switch Port	Traced MAC Address	Timestamp	
unknown			-	Re-Trace

Reporting APs

Reporting AP IP Address	Reporting AP BSSID	Current RSSI	Reporting AP Location
10.2.64.28	000ff7801f90	-90	Geologicas/Planta 0
10.2.64.98	00135ffb09d0	-92	
10.2.64.43	00135ffb6f50	-92	Geologicas/Planta 0
10.2.64.45	00135ffb69a0	-94	Geologicas/planta 2

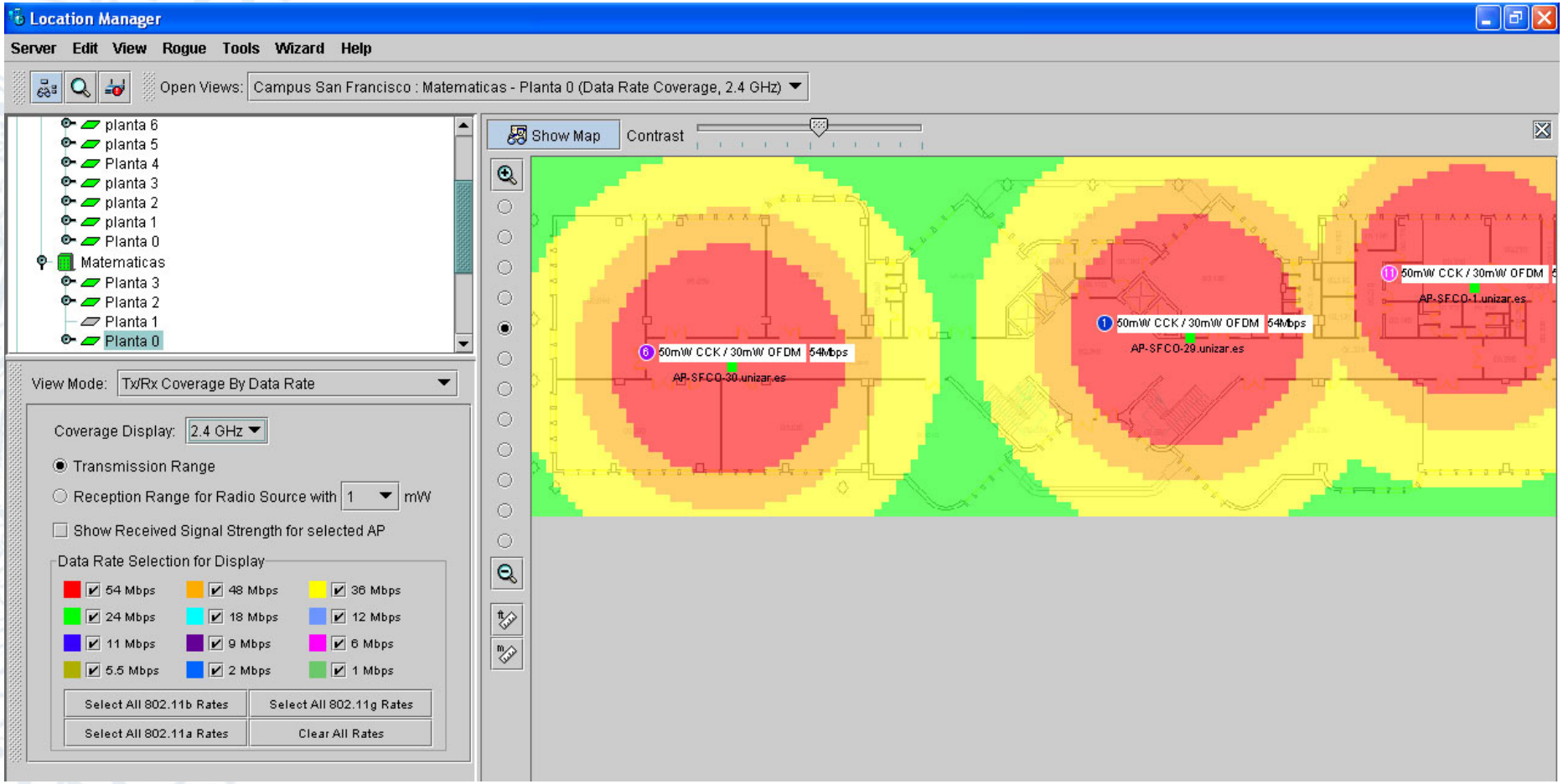
Gestión de Puntos de Acceso WLSE

DETECTOR DE FALLOS



Gestión de Puntos de Acceso WLSE

GENERADOR DE MAPAS



Gestión de Puntos de Acceso

- HP Openview NNM
  - Gestor de traps
- Scripts en Expect
  - Modificaciones en las configuraciones de equipos

```
#
# esta parte se comentara mas adelante, de momento insertala al
# principio de cada fichero de comandos.
#
set force_conservative 1  ;# set to 1 to force conservative mode even if
                          ;# script wasn't run conservatively originally
if {$force_conservative} {
        set send_slow {1 .001}
        proc send {ignore arg} {
                sleep .1
                exp_send -s -- $arg
        }
}
##################################################################

##################################################################
###
### PARAMETROS Y FORMATO DE LLAMADA
###
if $argc<3 {
    send_user "Uso: $argv0 ip ususario password\n"
    send_user "  ip => direccion IP del equipo a actualizar\n"
    send_user "  usuario => usuario para acceder al equipo, con priv.15\n"
    send_user "  password => password del usuario anterior\n"
    exit -1;
}

###
### VARIABLES
###
set MAQUINA [lindex $argv 0]
set DEFAULT_USER [lindex $argv 1]
set DEFAULT_PASSWORD [lindex $argv 2]
set DEFAULT_EN_PASSWORD [lindex $argv 2]

###
### LOG SI COMENTAMOS LA SIGUIENTE LINEA
###
#log_user 0
###
###CONEXION MAQUINA
                                                          52,1          11%
```

Control de Usuarios

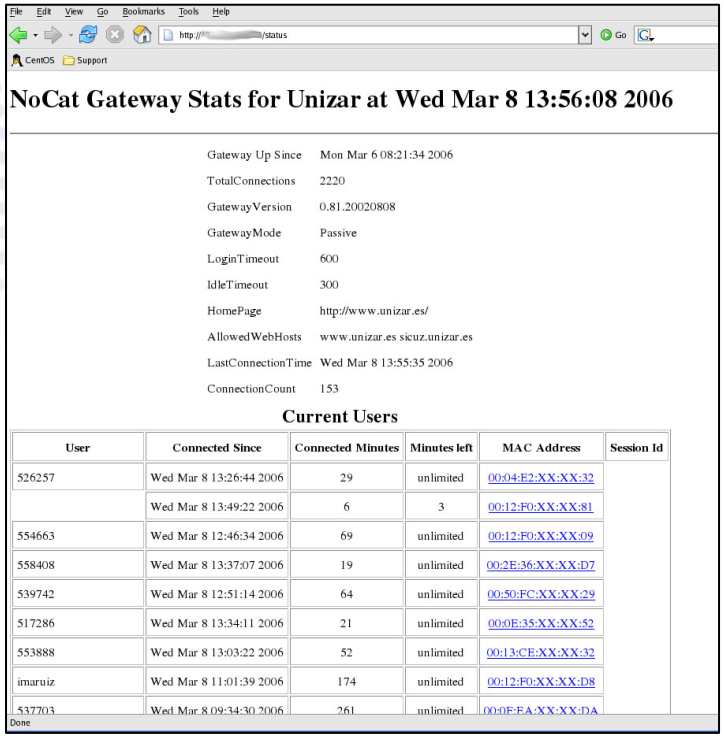
- Scripts en Perl
  - Tratamiento de ficheros de log (Nocat y Freeradius)

    Tendencias futuras: Gestionar los logs desde una base de datos
  - Estadísticas de conexión
    - Tiempos y tráfico totales de conexión a nivel de usuario
    - Fecha, IP, punto de conexión, duración y tráfico a nivel de sesiones por usuario

USUARIO	Fecha	Tiempo	IP	Mac	IN	OUT	AP
javalero	20060224-12:10	118	10.1.5.25	0013.ce59.711c	4133	3418	10.2.64.39
javalero	20060224-12:12	88	10.1.5.25	0013.ce59.711c	4630	6450	10.2.64.1
javalero	20060224-13:28	3256	10.1.5.25	0013.ce59.711c	125935	279248	10.2.64.1
javalero	20060227-08:37	30	10.1.7.22	00c0.49f9.148b	1620	1090	10.2.64.1
javalero	20060227-08:40	147	10.1.7.22	00c0.49f9.148b	3671	435	10.2.64.1
javalero	20060228-13:40	174	10.1.7.22	00c0.49f9.148b	1470	1422	10.2.64.1
javalero	20060307-10:08	1022	10.1.5.25	0013.ce59.711c	4178123	8243259	10.2.64.1
javalero	20060307-13:16	56	10.1.6.7	0013.46e5.a846	2118	1164	10.2.64.1
javalero	20060307-13:20	68	10.1.6.7	0013.46e5.a846	2646	1250	10.2.64.1

Control de Usuarios

- Arptrack
  - Guarda las direcciones Ip/Mac del router cada hora
- Herramientas propias del servidor Nocat



File Edit View Go Bookmarks Tools Help

http://[redacted]/status

CentOS Support

NoCat Gateway Stats for Unizar at Wed Mar 8 13:56:08 2006

Gateway Up Since	Mon Mar 6 08:21:34 2006
TotalConnections	2220
GatewayVersion	0.81.20020808
GatewayMode	Passive
LoginTimeout	600
IdleTimeout	300
HomePage	http://www.unizar.es/
AllowedWebHosts	www.unizar.es sicuz.unizar.es
LastConnectionTime	Wed Mar 8 13:55:35 2006
ConnectionCount	153

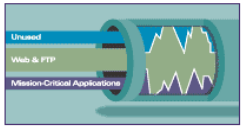
Current Users

User	Connected Since	Connected Minutes	Minutes left	MAC Address	Session Id
526257	Wed Mar 8 13:26:44 2006	29	unlimited	00:04:E2:XX:XX:32	
	Wed Mar 8 13:49:22 2006	6	3	00:12:F0:XX:XX:81	
554663	Wed Mar 8 12:46:34 2006	69	unlimited	00:12:F0:XX:XX:09	
558408	Wed Mar 8 13:37:07 2006	19	unlimited	00:2E:36:XX:XX:D7	
539742	Wed Mar 8 12:51:14 2006	64	unlimited	00:50:FC:XX:XX:29	
517286	Wed Mar 8 13:34:11 2006	21	unlimited	00:0E:35:XX:XX:52	
553888	Wed Mar 8 13:03:22 2006	52	unlimited	00:13:CE:XX:XX:32	
imaruiz	Wed Mar 8 11:01:39 2006	174	unlimited	00:12:F0:XX:XX:D8	
537703	Wed Mar 8 09:34:30 2006	261	unlimited	00:0F:EA:XX:XX:DA	

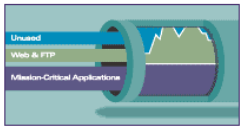
Done

“Qué hacen” los Usuarios

- PacketShaper



BEFORE PACKETEER



AFTER PACKETEER

PacketShaper®

top ten | monitor | manage | report | setup | info | feedback | packetguide

Unit: 011-10000304 Discovery: On Shaping: On

MONITOR TRAFFIC

Click "clear stats ..." to reset values shown in GREEN. Mar 10 2006 - 12:52:13

Monitor: Traffic Display: All classes clear stats ... update Auto (Off) Stop Auto

Last cleared: Mar 10 - 03:18:36

Tree Depth: off

Traffic Class Name	Report	Class Hits	Policy Hits	Current (bps)	1 Min (bps)	Peak (bps)	Guar. Rate Failures	Pkt Exch (ms)	Partition Min-Max	Policy Type (Pri.) Guar.-Limit	Top User Analysis
YahooGames		46	NA	404	260	59k	0	172			
Battle.net		0	NA	0	0	0	0	NA			
Mensajes				3.5M	3.4M	23.0M	0	NA			
IRC				60k	59k	441k	0	NA			
IRC-S-OUT		1216	NA	60k	58k	441k	0	183			
IRC-S-IN		122	NA	0	7	2079	0	2			
Lotus-IM		138150	NA	2.9M	3.0M	4.4M	0	536			
MSN-Messenger		32034	NA	303k	94k	779k	0	141			
Windows-POPUP		243032	243032	0	0	0	0	NA		Discard	
YahooMsg		993	NA	136	125	44k	0	92			
AOL-AIM-ICQ		991	NA	130k	138k	19.9M	0	34			
Multimedia				6.3M	5.1M	29.0M	0	NA			
GoogleEarth		144	NA	1.3M	693k	2.5M	0	11			
MPEG-Audio		396	NA	676k	676k	14.2M	0	31			
MPEG-Video		1032	NA	160k	389k	27.7M	0	28			
Ogg		6	NA	0	0	792k	0	17			
QuickTime		132	NA	39k	357k	13.9M	0	21			
RadioNetscape		0	NA	0	0	0	0	NA			
Real		4295	NA	818k	787k	8.1M	0	92			
RTP-I				0	359	210k	0	NA			
RTP-I-1016		0	NA	0	0	0	0	NA			
RTP-I-G722		0	NA	0	0	0	0	NA			
RTP-I-G723		0	NA	0	0	0	0	NA			
RTP-I-G729		0	NA	0	0	0	0	NA			
RTP-I-GSM		0	NA	0	0	0	0	NA			
RTP-I-H261		0	NA	0	0	0	0	NA			
RTP-I-H263		0	NA	0	0	0	0	NA			
RTP-I-PCMU		0	NA	0	0	0	0	NA			
RTP-I-QCELP		0	NA	0	0	0	0	NA			
Default		22	NA	0	359	210k	0	NA			
Shoutcast		12	NA	0	177	911k	0	43			
WinampStream		1167	NA	1.4M	1.1M	2.3M	0	57			
WinMedia		40525	NA	1.9M	1.4M	15.4M	0	69			
RTSP		1517	NA	13k	4485	890k	0	123			
StreamWorks		333	NA	106	33	33k	0	129			

“Qué hacen” los Usuarios

Chequeando dirección IP 155.210.[redacted]

Reload

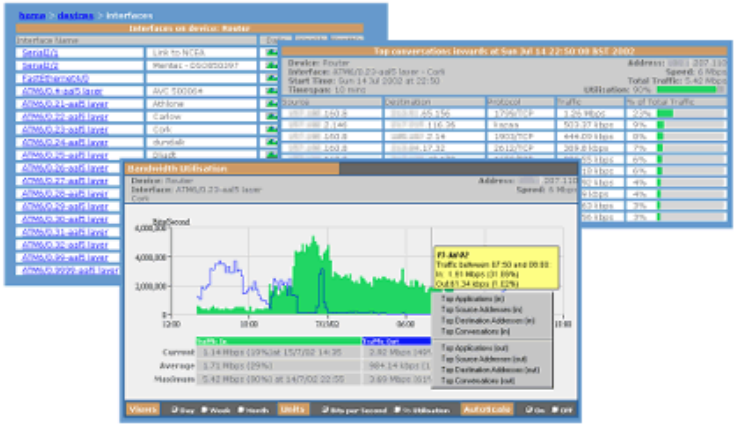
IDENT: Connection timed out (110)

WAN Flows

Resultado consulta: [128 Registros]

InAddr	InAddr Name	In Port	OutAddr IP	OutAddr Name	Out Port	Idle Time	Class In	Class Out	Service
155.210.[redacted]	155.210.[redacted]	4537	172.212.250.73	ACD4FA49.ipt.aol.com	7000	1m	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	84.48.130.237	237.84-48-130.nextgentel.com	17160	47s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	62.3.78.65	dsl-62-3-78-65.zen.co.uk	32879	0s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	64.3.150.52	w052.z064003150.sjc-ca.dsl.cnc.net	33160	4s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50743	1h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	84.181.232.56	p54B5E838.dip.t-dialin.net	58964	1m	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50424	1h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	83.112.238.111	ALagny-152-1-64-111.w83-112.abo.wanadoo.fr	4149	2h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	193.146.74.175	193.146.74.175	40248	0s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	4406	80.104.128.237	host237-128.pool80104.interbusiness.it	6882	1s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50291	3h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	3725	217.217.3.129	129.red-217-217-3.user.auna.net	16605	0s	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50880	3h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50222	2h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	88.101.19.154	154.19.broadband6.iol.cz	50018	2h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	63629	83.112.238.111	ALagny-152-1-64-111.w83-112.abo.wanadoo.fr	2765	3h	BitTorrent	BitTorrent	BitTorrent
155.210.[redacted]	155.210.[redacted]	3136	38.115.131.131	38.115.131.131	2240	3h	Soulseek	Soulseek	Soulseek

“Qué hacen” los Usuarios



- NetFlow 5

  Captura de Flows en una base de datos

- Ethereal

  Sólo como última opción y para casos extremos

Problemas de implantación/explotación

- Inicio : No retransmitíamos Multiples-SSID
- Máximo de AP por WDS
- Compatibilidad de las tarjetas de red con la red Eduroam
- Problemas puntuales que vamos resolviendo día a día

ROGUE ACCESS POINT

Cómo se haría:

- AP con SSID igual a uno de los existentes
- Copia de la página de petición de login o copia de la estructura existente
- Creación de un certificado con nombre similar al de la organización
- Una vez puesto en marcha, el AP nos capturaría usuarios y contraseñas

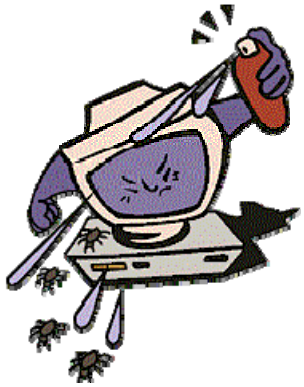
Cómo evitarlo:

- Detección de AP Rogue por medio del WLSE
- Buscar la posición de este AP lo antes posible y así poder parar el ataque
- Por parte de los usuarios: no confiando en nuevos certificados

Nota: Este tipo de ataque no lo hemos detectado en nuestra red

- En Eduroam-web:
  - TODOS
    - La red es completamente abierta
    - Falta de certificados en muchos servicios (Webmail, Pop3, Imap...)
    - La facilidad de uso de la misma hace que los usuarios la prefieran a la cifrada

- En Eduroam:
  - A nivel de cifrado NINGUNO, de momento…
  - A nivel de usuarios: virus, p2p …



¡Muchas gracias!

¿Dudas, comentarios o preguntas?