



Red Inalámbrica

Fco. Javier Fernández Landa
Universidad Pública de Navarra



Agenda

- Presentar la red inalámbrica de la Universidad Pública de Navarra.
- Describir su implantación.
- Aspectos de gestión de red.
- Modos de conexión.
- Siempre teniendo en cuenta, lógicamente, la seguridad.

La Universidad Pública de Navarra



- Fundada en 1987
- 5 centros, 20 departamentos, 24 titulaciones
- 800 PDI, 350 PAS y 8500 alumnos
- Un campus (Arrosadia) con 23 edificios
- Un edificio (Ciencias de la Salud) remoto

Red inalámbrica – Evolución

- Desde el año 2002 a mayo de 2005
 - 5 APs. Servicio bajo demanda. 250 usuarios
 - 2 enlaces de troncal
- Año 2004: Proyecto red inalámbrica
 - Concurso público. Pliego de prescripciones técnicas
 - Adjudicación en noviembre de 2004
- En producción desde mayo de 2005
 - 900 usuarios (800 estudiantes, 100 PAS/PDI) hasta la fecha
- Anuncio a la comunidad universitaria en septiembre de 2005

Puntos básicos del proyecto

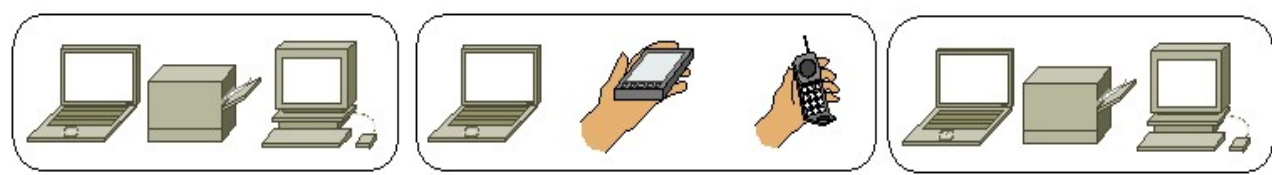
- Parte física
 - Diseño físico de red determinando localización de APs, antenas, canales y potencias de acuerdo a medidas de campo con herramientas especializadas.
 - Replanteo con nuevas medidas tras la instalación de los APs.
 - Únicamente cobertura interior.
- Parte lógica
 - Gestión específica de APs y red inalámbrica.
 - Sistema de autenticación de red RADIUS.
 - Múltiples escenarios de acceso y servicio.
 - Elementos adicionales de seguridad o acceso.

Fases de implantación

- Fase 1 – Piloto (Dic. 2004 – Mayo 2005)
 - Solamente 3 edificios del campus. 13 APs de un total de 93.
 - Completar todos las tareas del proyecto (física y lógica).
 - Formación.
 - Al final de la fase red totalmente operativa.
- Fase 2 – Despliegue (Marzo – Julio 2005)
 - 14 edificios en dos grupos de 7.
 - 60 APs.
- Fase 3 – Finalización (Octubre – Noviembre 2005)
 - Últimos 7 APs.

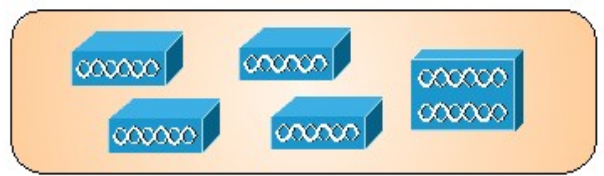


La red de la Universidad



USUARIO

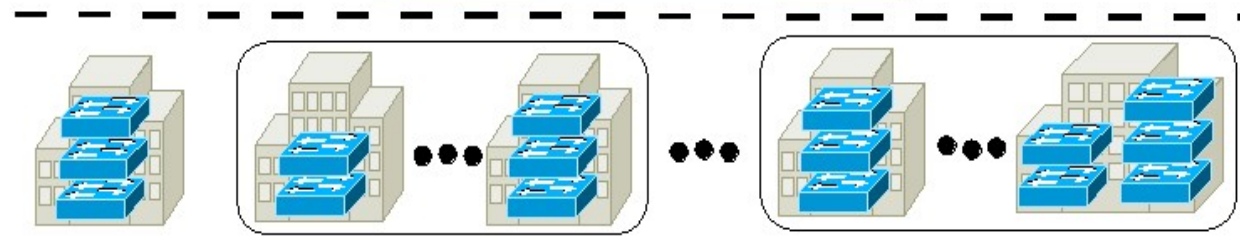
- 1600 dispositivos WIFI
- 890 usuarios WIFI



ACCESO WLAN

- 16 Edificios Campus + 1 Remoto
- 75 Puntos de acceso b/g
- 18 Puntos de acceso a/b/g

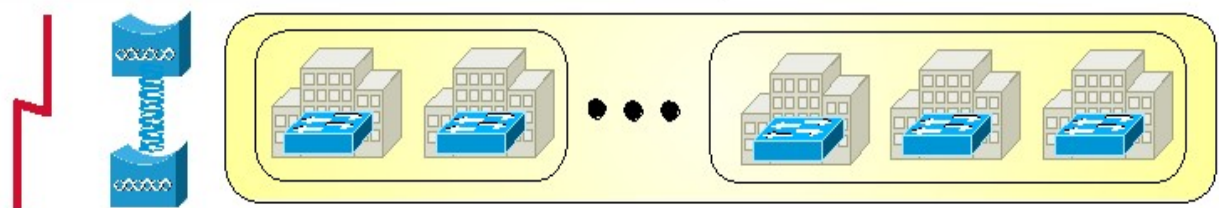
93 FastEthernet PoE



ACCESO LAN

- 18 Edificios Campus + 1 Remoto
- 41 Armarios distribución
- 33 Armarios aulas y laboratorios
- 151 Switches FastEthernet

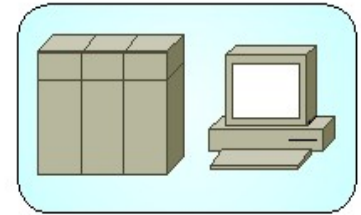
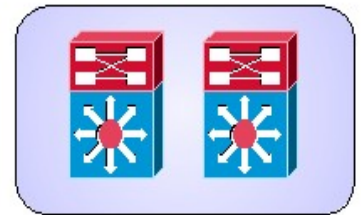
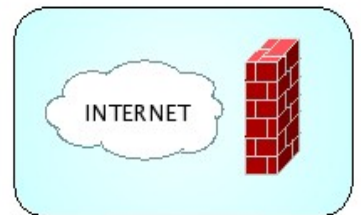
117 Gigabit Ethernet
2 Inalámbricos



DISTRIBUCION

- 12 Edificios
- 20 Switches Gigabit
- 9 Grupos de redundancia
- 1 Enlace inalámbrico

40 Gigabit Ethernet
1 WAN (LAN2LAN)



CORE - CPD

- CPD
- 2 x C6500
- SERVICIOS: Internet - Intranet
- SEGURIDAD

Mediciones de cobertura

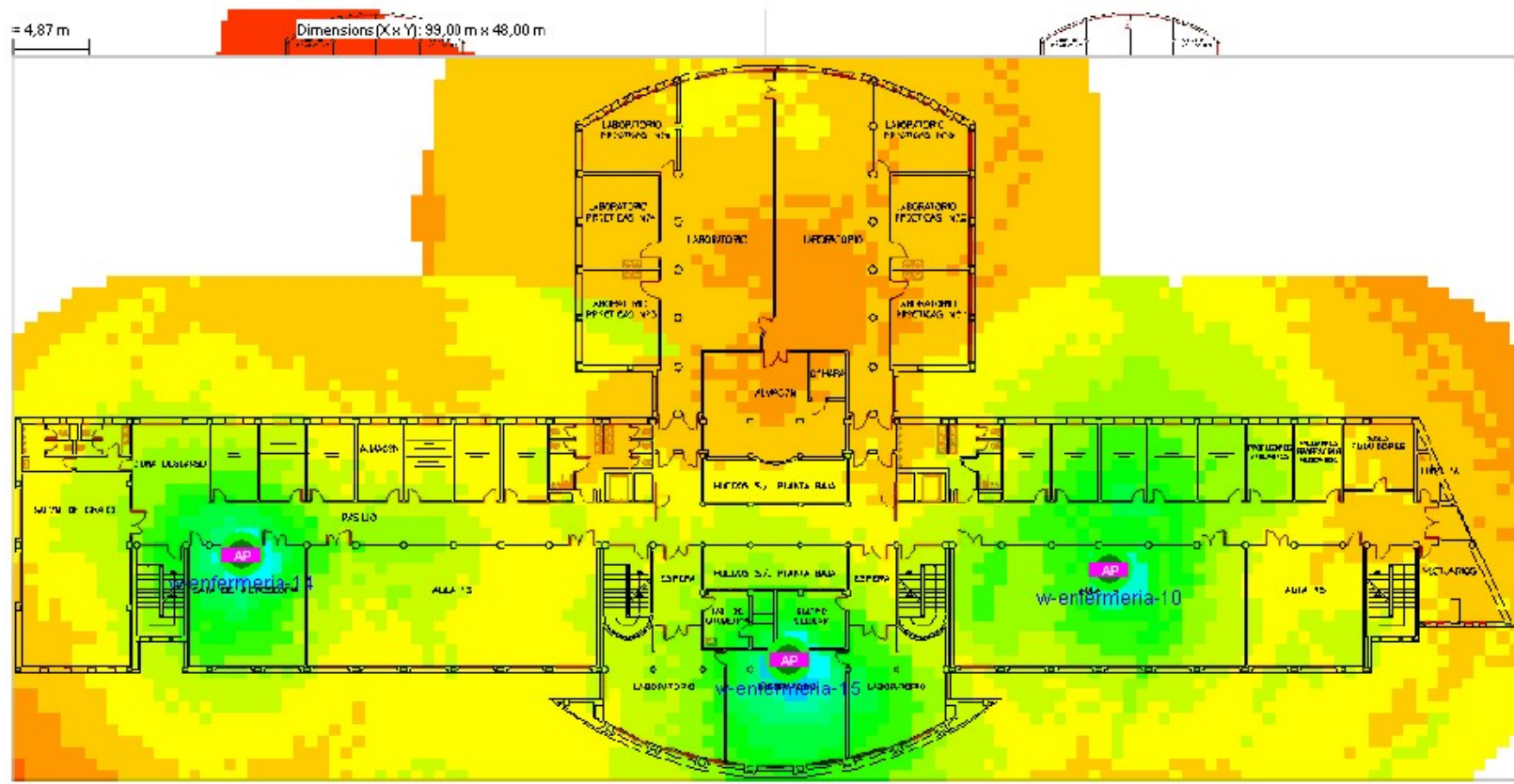
- Diseño
 - Zonas prioritarias: aulas, salas de reuniones, salones, bibliotecas, zonas de uso común en general.
 - 2 APs. Medidas 802.11g.
 - Factores a determinar: ubicación de APs, orientación de antenas, canales y potencia.
 - Herramienta usada: AirMagnet Survey.
- Replanteo
 - Nuevas medidas de campo tras instalación de APs (a/b/g).
 - Ajustes en canales y potencia. Detección de rogue APs.
 - Herramientas usadas: AirMagnet Survey y Cisco WLSE.
 - Ubicación APs de fase 3.

Plano de cobertura

Signal/Noise Distribution

Overall Coverage Report by AP

AirMagnet Surveyor



Instalación de AP

- APs Cisco 1200 (93)
 - 802.11g y 802.11b
 - 18 con el módulo 802.11a
- Cableado estructurado CAT 5e
- Alimentación 802.3af
 - Power Injectors
 - PoweDsine (6 y 12 en 1U)
- Medidas antirrobo

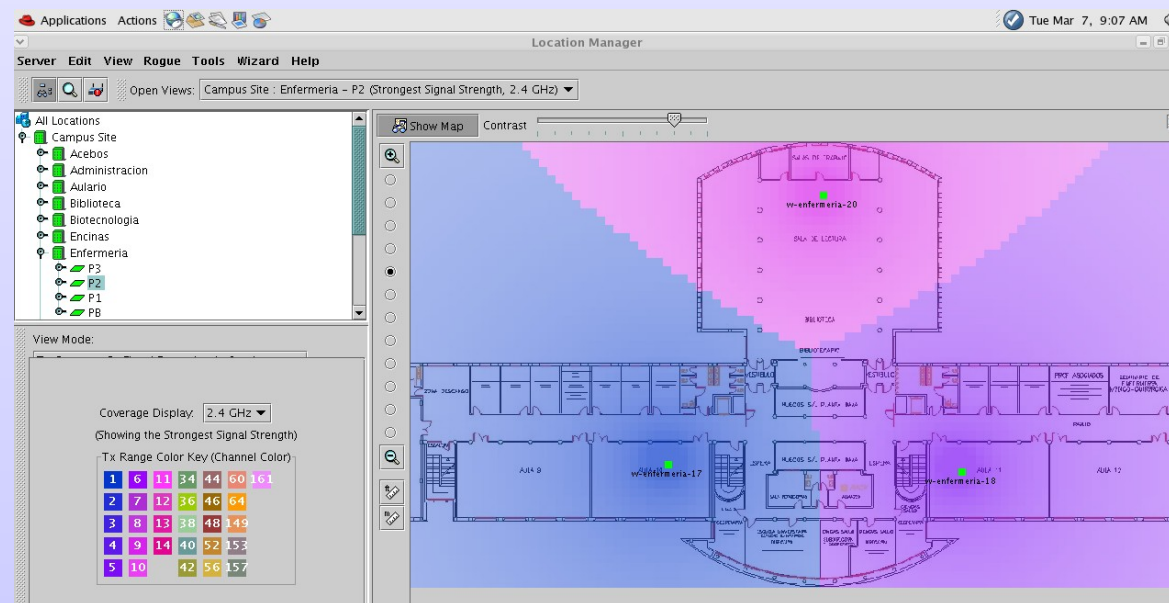
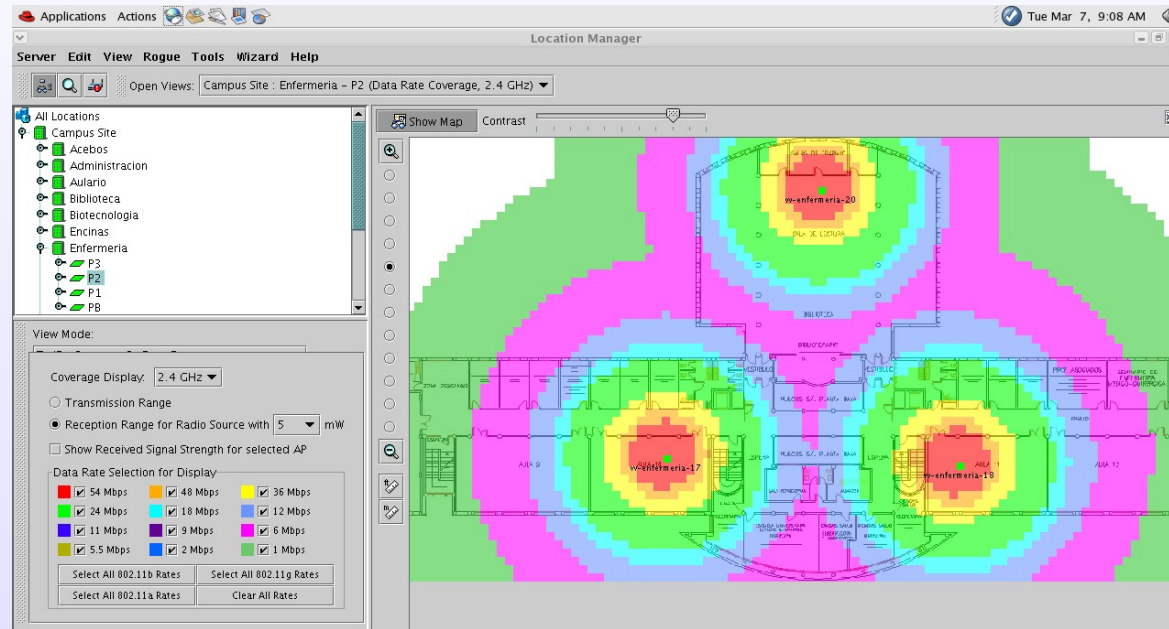


Herramientas de gestión

- Cisco WLSE
 - 2 APs dedicados a WDS
 - Gestión y seguridad RF
 - Planos
 - Gestión de elementos: configuraciones, IOS
 - Alarmas
- Airwave AMP
 - Complementaria
 - Se integra con NoCat, ACS, WLSE, switches y routers
 - Especialmente útil para helpdesk, reports y estadísticas



WLSE – Planos de cobertura



Airwave AMP

Applications Actions Fri Mar 10, 12:30 PM
 endrino.red.unavarra.es - Mozilla Firefox
 File Edit View Go Bookmarks Tools Help
 https://endrino.red.unavarra.es/root?

endrino.red.unavarra.es NoCat Gateway Status: Universidad... Condiciones
Airwave New Devices: 0 Up: 99 Down: 0 Mismatched: 4 Rogue: 22 Users: 48
 Home Groups APs/Devices Users Reports System Device Setup AMP Setup RAPIDS
 Overview Search License

Welcome to the AirWave Management Platform™

Number of Users

Bits Per Second Out Bits Per Second In

System Overview

System Name: endrino.red.unavarra.es Current Time: 3/10/2006 12:30 PM
 Organization: UPNV Uptime: 42 days 3 hrs 13 mins
 Hostname: endrino.red.unavarra.es Software Version: 4.1
 IP Address: 172.17.0.17 Operating System: Fedora Core release 3

Monitoring Status

0 of 99 devices are [Down](#)

Latest Reports

- [Device Summary](#)
- [Wireless Network Usage](#)
- [Device Uptime](#)
- [Inventory](#)
- [User Sessions](#)
- [All Reports](#)

Quick Links

- [Help](#)
- [Supported Devices and Features](#)
- [Configure default credentials.](#)
- [Discover new devices on your network.](#)
- [Upload AP firmware.](#)
- [Poll routers and switches.](#)
- [Configure alert thresholds.](#)

Latest System Events

Time	User	Type	Event
Fri Mar 10 12:24:43 2006	System	System	Wireless station 00:13:CE:86:9B:CF deauthenticated via RADIUS Accounting
Fri Mar 10 12:19:39 2006	System	System	Wireless station 00:16:6F:40:6A:8C deauthenticated via RADIUS Accounting
Fri Mar 10 12:14:49 2006	System	System	Wireless station 00:80:5A:27:DA:64 deauthenticated via RADIUS Accounting
Fri Mar 10 12:09:40 2006	System	System	Wireless station 00:0E:35:55:38:3A deauthenticated via RADIUS Accounting
Fri Mar 10 11:49:48 2006	System	System	Wireless station 00:14:A4:67:9A:E0 deauthenticated via RADIUS Accounting

[View Event Log](#)

© 2001-2006 AirWave Wireless, Inc. - <http://www.airwave.com/>
 AirWave Wireless, Inc. is not connected, affiliated or related to Airwave O2 Limited in any way whatsoever.

Last day

Number of Users

Last week

Number of Users

Last month

Number of Users

Last year

Number of Users



Seguridad RF

- Detección de rogue APs
 - A través de los interfaces de radio
 - A través de la red cableado
 - Localización en red cableada de APs detectados por radio
- Detección de redes ad-hoc
- Detección de ataques y anomalías en el medio inalámbrico
 - MAC spoofing, EAPOL flooding
 - Fallos de encriptación
 - Tramas de gestión excesivas



Autenticación RADIUS

- Dos servidores Cisco ACS
- Credenciales de autenticación en servidor LDAP corporativo
- PEAP-GTC
- Dos perfiles de usuario:
 - Estudiante. Sólo permite autenticación desde NoCat
 - PAS/PDI. También permite autenticación desde APs
- Servidor freeradius para incorporación a eduroam



Modos de acceso (I)

- Acceso restringido seguro
 - Reservado para PAS/PDI.
 - WPA y WPA2. Autenticación PEAP-GTC usando credenciales corporativas.
 - Permite acceso a servicios exclusivos de intranet.
 - Equipo de usuario registrado y cumpliendo requisitos de conexión.
- Acceso abierto autenticado
 - Cualquier miembro de la comunidad universitaria.
 - No cifrada. Autenticación por portal web (NoCat).
 - Acceso únicamente a servicios públicos de la universidad y a Internet.



Modos de acceso (II)

- Pantallazo del portal cautivo (NoCat)

The screenshot shows a Mozilla Firefox browser window displaying a captive portal for the University of Navarra's wireless network. The browser's address bar shows the URL: `https://wls.unavarra.es/cgi-bin/login?redirect=http%3a%2f%2ffedora%2eredhat%2ecom%`. The page features a "wifi" logo and a "red inalámbrica hari gabeko sarea" header. A central section titled "Ayuda y condiciones de uso" (Laguntza eta erabiltzeko baldintzak) provides instructions for users. To the right, there is a login form with fields for "Usuario / Erabiltzailea:" (containing "javier.fernandez") and "Contraseña / Pasahitza:" (containing "*****"), along with an "Entrar / Sartu" button. The footer contains contact information for the University of Navarra, including the phone number 948 169 090 and the email address `sistemas@unavarra.es`. The system tray at the bottom shows the user "root@j6614:~" and the "Universidad Publica de Nav" application.



Modos de acceso (III)

- Invitados
 - Desactivado por defecto en toda la red.
 - Se activa previa petición en los APs que dan cobertura al lugar de celebración de un congreso, reunión, etc. durante su periodo de duración.
 - Abierta y no cifrada. El invitado debe aceptar las condiciones de uso de la red de la Universidad.
 - Acceso a Internet y servicios públicos de la Universidad.
- eduroam
 - WPA y WPA2. TTLS-PAP y PEAP-GTC.
 - Acceso a Internet y servicios públicos de la Universidad.



Seguridad de red

- Para los modos de acceso por portal cautivo, invitados y eduroam.
 - Política de seguridad equivalente a la del tráfico desde Internet. Pasa por el cortafuegos de red perimetral.
 - Ningún control sobre el equipamiento de usuario. Recomendaciones de seguridad.
 - Direccionamiento privado con NAT dinámico.
- Para el modo de acceso restringido y seguro.
 - Política de seguridad específica con acceso a servicios de intranet aplicada en cortafuegos interno.
 - Requerimientos específicos para el equipamiento de usuario.



A partir de ahora

- Cobertura interior completa.
- Cobertura exterior.
- Optimización del roaming.
- Servicios móviles. VoIP.

Conclusiones

- Las redes inalámbricas están aquí para quedarse.
- Paso adelante en la consolidación de infraestructuras de autenticación para el acceso a red.
- Campo abierto para avanzar y mejorar en la gestión del medio inalámbrico y su seguridad.
- Nuevas necesidades en seguridad de red.





Muchas gracias

Fco. Javier Fernández Landa
Universidad Pública de Navarra

javier.fernandez@unavarra.es

