Red Inalámbrica Universitaria

Enrique de la Hoz de la Hoz
enrique@aut.uah.es

Universidad de Alcalá de Henares

14 de noviembre de 2006

Índice

Antecedentes

- Especificaciones técnicas establecidas desde la Universidad de Alcalá

Antecedentes

- Especificaciones técnicas establecidas desde la Universidad de Alcalá
- Necesidad de proporcionar acceso a Internet a los usuarios de la Ciudad Residencial Universitaria de la Universidad de Alcalá

Antecedentes

- Especificaciones técnicas establecidas desde la Universidad de Alcalá
- Necesidad de proporcionar acceso a Internet a los usuarios de la Ciudad Residencial Universitaria de la Universidad de Alcalá
- Acceso limitado a HTTP y HTTPS con un ancho de banda mínimo por usuario equivalente al ofrecido por un ADSL de 256 kbps.

Escenario

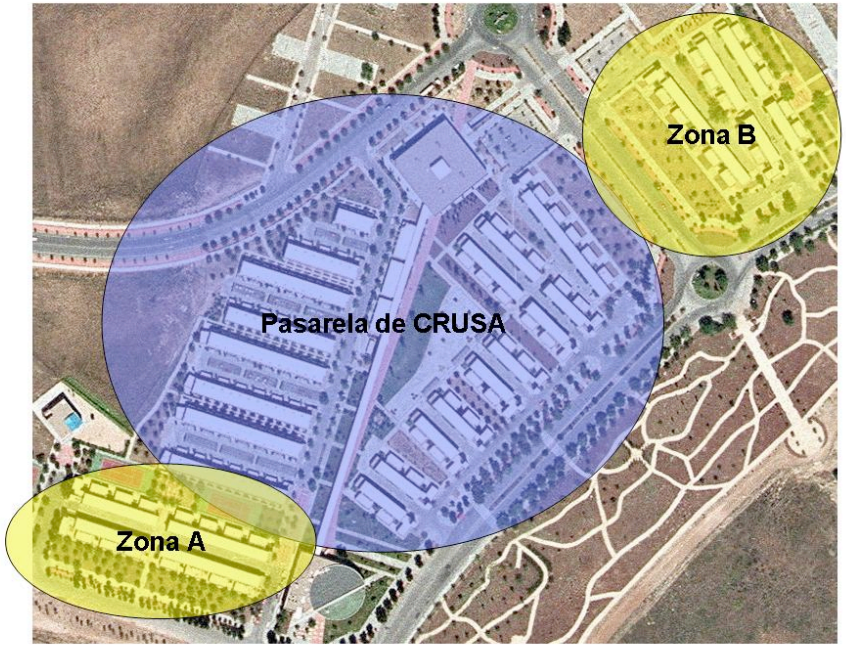


Figura: Vista satélite de CRUSA

Escenario

- Complejidad de desplegar una infraestructura de red cableada
  Caro y molesto para los residentes

Escenario

- Complejidad de desplegar una infraestructura de red cableada
  Caro y molesto para los residentes
- Decisión de emplear comunicaciones inalámbricas basadas en el estándar IEEE802.11

Premisas

- Desarrollo de un sistema radio para dar cobertura global a toda la zona de las residencias

Premisas

- Desarrollo de un sistema radio para dar cobertura global a toda la zona de las residencias
- Desarrollo de una plataforma para proporcionar el servicio empleando software libre en concreto Linux

Etapas

- Se plantea un desarrollo en dos fases:
  - En una primera fase, se pide un despliegue rápido de la red sin requisitos de calidad de servicio sobre un ADSL de 1Mbps

Etapas

- Se plantea un desarrollo en dos fases:
  - En una primera fase, se pide un despliegue rápido de la red sin requisitos de calidad de servicio sobre un ADSL de 1Mbps
  - En la segunda fase, se plantea ofrecer los requisitos adecuados con una plataforma segura y gestionable

Desarrollo de la Fase I

- Problemas con el despliegue de los puntos de acceso

Desarrollo de la Fase I

- Problemas con el despliegue de los puntos de acceso
- Estudio de puntos de acceso de marcas comerciales: Senao, D-Link, Linksys

Esquema de red de la Fase I

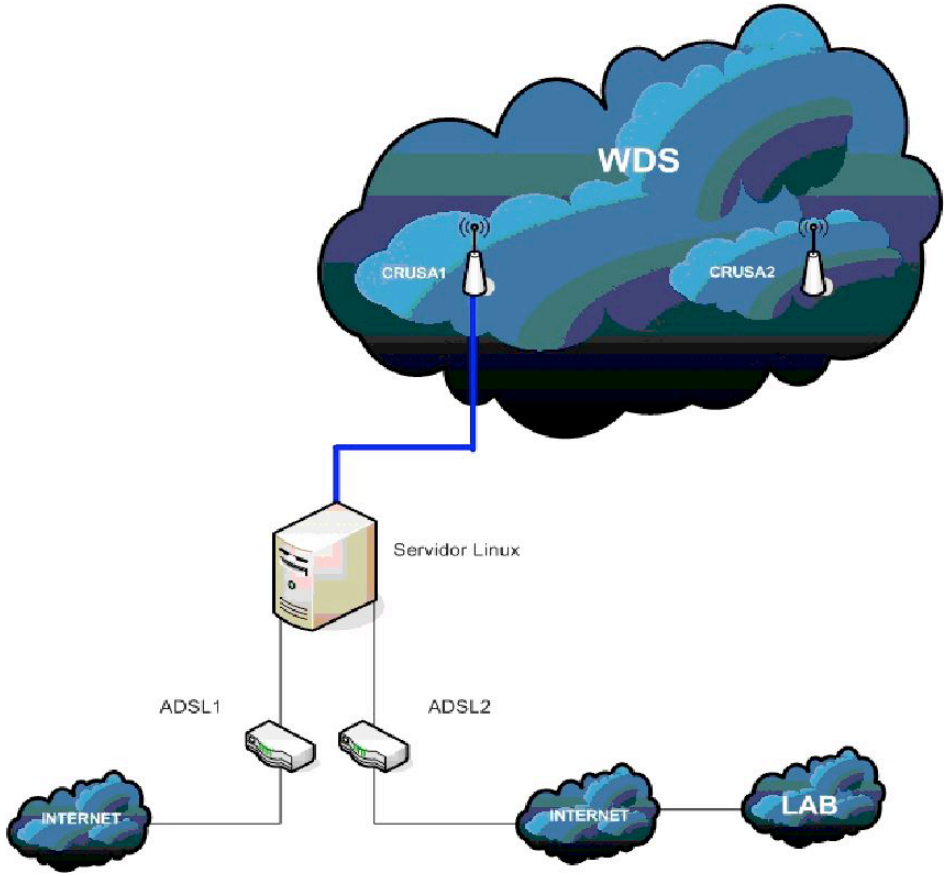


Figura: Esquema de la Fase I

Ejecución de la fase I

- Se despliegan dos puntos de acceso en WDS ubicados en sendas torretas determinando la áltura óptima a la que situarlos para ofrecer la máxima cobertura
- Se opta por los puntos de acceso Linksys Wireless-G Broadband Router sustituyendo el firmware por la distribución dd-wrt basada en Linux
- Toda la infraestructura de red se basa en Debian GNU/Linux
- Para la gestión se emplean SARG y AWSTATS para monitorizar accesos al proxy, y MRTG para monitorizar el estado el acceso de la red.
- Se despliega una infraestructura de seguridad basada en SNORT y un firewall con iptables

Conclusiones

- Realimentación de la información de monitorización para corregir errores de configuración
- Selección de los AP Linksys WRT54G por soportar monitorización SNMP y de firmware basada en Linux
- Limitación del sistema impuesta por el escaso número de APs empleados
- Necesidad de un despligue de un sistema para garantizar calidad de servicio

Esquema de red de la Fase II

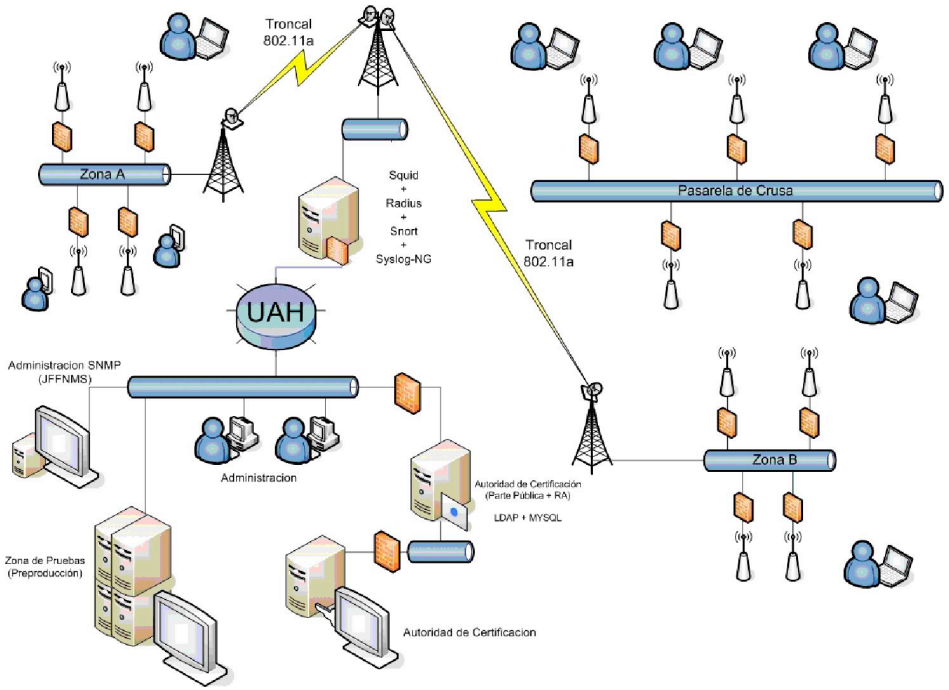


Figura: Esquema de la Fase II

Puntos de acceso

- Se realiza un estudio de cobertura para situar 22 puntos de acceso Linksys en modo router segmentando la red con su propio firewall basado en Iptables

Puntos de acceso

- Se realiza un estudio de cobertura para situar 22 puntos de acceso Linksys en modo router segmentando la red con su propio firewall basado en Iptables
- Todos los APs se unen mediante un troncal bien ethernet o mediante enlaces troncales IEEE802.11a (tsunamis y subscriptores en modo bridge, Proxim 5054-BSU-SU) donde no llega el cable

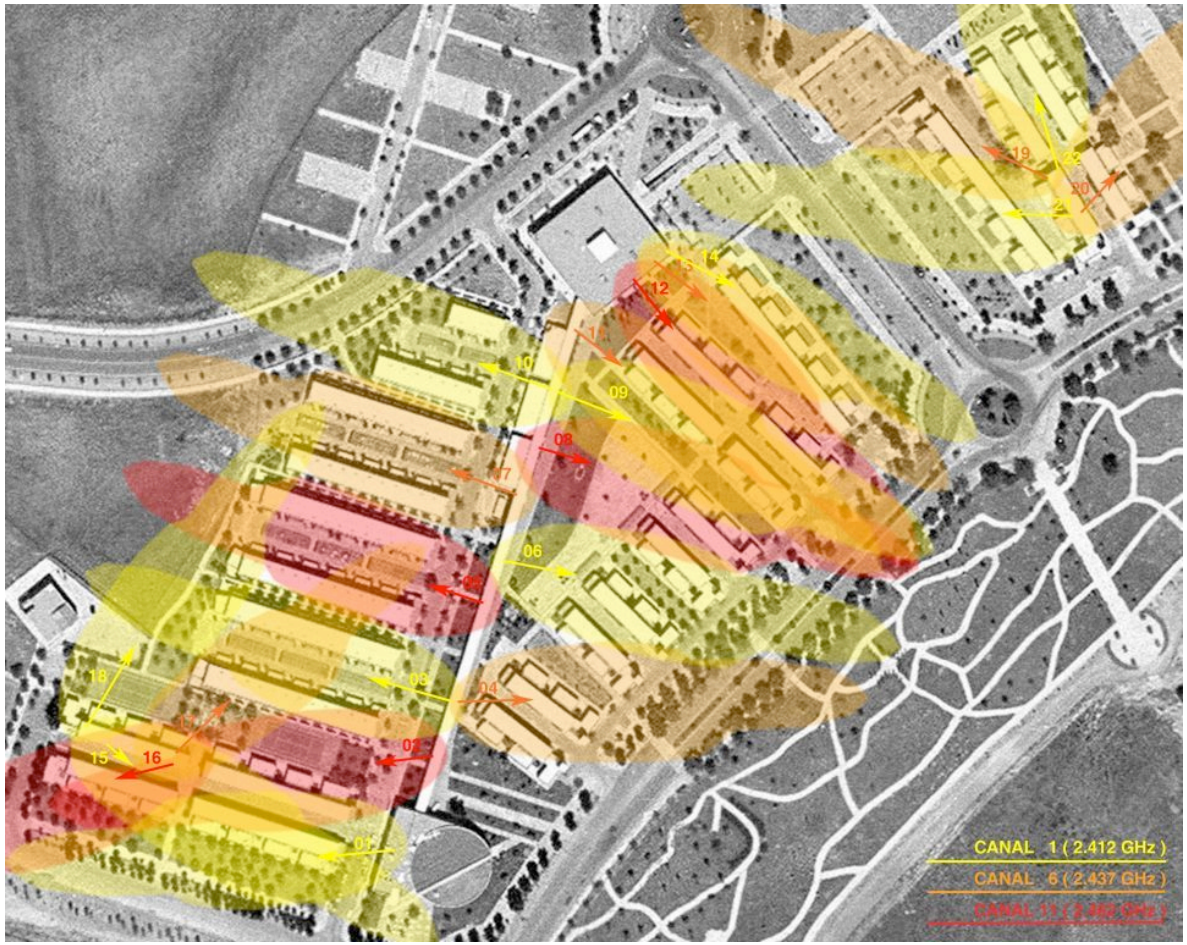
Puntos de acceso

- Se realiza un estudio de cobertura para situar 22 puntos de acceso Linksys en modo router segmentando la red con su propio firewall basado en Iptables
- Todos los APs se unen mediante un troncal bien ethernet o mediante enlaces troncales IEEE802.11a (tsunamis y subscriptores en modo bridge, Proxim 5054-BSU-SU) donde no llega el cable
- Cargados con el firmware Linux dd-wrt.vv prefinal 5 y distribuidos en los canales 1, 6 y 11

Puntos de acceso

- Se realiza un estudio de cobertura para situar 22 puntos de acceso Linksys en modo router segmentando la red con su propio firewall basado en Iptables
- Todos los APs se unen mediante un troncal bien ethernet o mediante enlaces troncales IEEE802.11a (tsunamis y subscriptores en modo bridge, Proxim 5054-BSU-SU) donde no llega el cable
- Cargados con el firmware Linux dd-wrt.vv prefinal 5 y distribuidos en los canales 1, 6 y 11
- La distribución de los APs permite que todos los usuarios lleguen a un mínimo de dos APs, zonas más ocultas incluídas

Distribución de puntos de acceso



Servidor Proxy

- Se incluye un proxy-cache para gestionar las peticiones de los APs

Servidor Proxy

- Se incluye un proxy-cache para gestionar las peticiones de los APs
- Se emplea un servidor Linux y se centraliza ahí también el cortafuegos, el sistema de detección de intrusiones y el sistema de calidad de servicio

Proxy-Caché

- Se emplea Squid 2.5.9 como proxy y caché de HTTP, proxy de SSI, aceleración de HTTP, control de acceso por IP y filtrado de contenido dinámico

Proxy-Caché

- Se emplea Squid 2.5.9 como proxy y caché de HTTP, proxy de SSI, aceleración de HTTP, control de acceso por IP y filtrado de contenido dinámico
- Se consigue un ahorro de ancho de banda en torno al 25-30 por ciento

Proxy-Caché: estadísticas

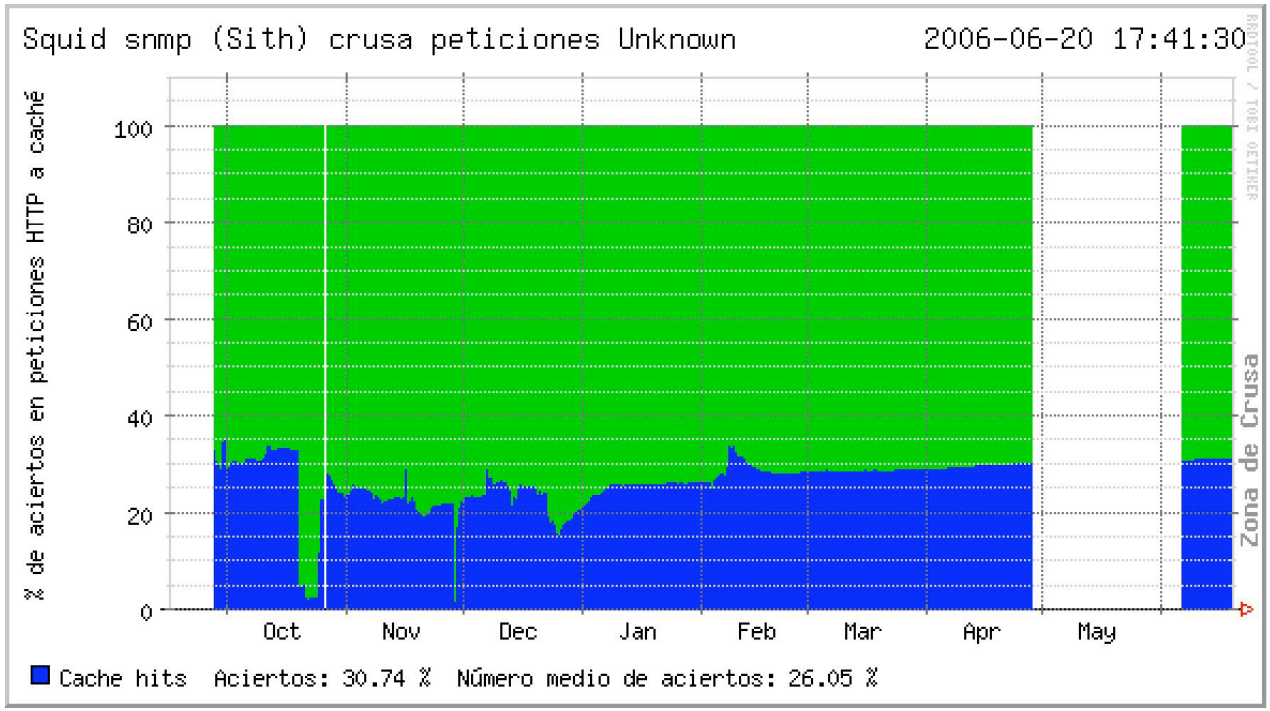


Figura: Eficiencia del Proxy

Calidad de Servicio

- Se diseña un sistema de QoS basado en los diagramas de colas del kernel de Linux mediante tc

Calidad de Servicio

- Se diseña un sistema de QoS basado en los diagramas de colas del kernel de Linux mediante tc
- El objetivo es repartir dinámica y equitativamente el ancho de banda disponible

Calidad de Servicio

- Se diseña un sistema de QoS basado en los diagramas de colas del kernel de Linux mediante tc
- El objetivo es repartir dinámica y equitativamente el ancho de banda disponible
- Como disciplinas de colas se emplean HTB para reservar ancho de banda y ESFQ y SFQ para repartirlo equitativamente

Calidad de Servicio

- Se diseña un sistema de QoS basado en los diagramas de colas del kernel de Linux mediante tc
- El objetivo es repartir dinámica y equitativamente el ancho de banda disponible
- Como disciplinas de colas se emplean HTB para reservar ancho de banda y ESFQ y SFQ para repartirlo equitativamente
- Se determina un conjunto de clases de tráfico donde el tráfico de usuario está en los últimos lugares garantizando por encima el tráfico de soporte necesario de la red .

Calidad de Servicio

- Se diseña un sistema de QoS basado en los diagramas de colas del kernel de Linux mediante tc
- El objetivo es repartir dinámica y equitativamente el ancho de banda disponible
- Como disciplinas de colas se emplean HTB para reservar ancho de banda y ESFQ y SFQ para repartirlo equitativamente
- Se determina un conjunto de clases de tráfico donde el tráfico de usuario está en los últimos lugares garantizando por encima el tráfico de soporte necesario de la red .
- Se parchea tc para emplear ESFQ, iptables para el marcado de paquetes y la creación de dispositivos virtuales de red y el kernel de Linux para soportar ESFQ

Calidad de Servicio

- Para el acceso a Internet se crean tres colas finales:
  - Cola de max prioridad para paquetes de mínimo retardo

Calidad de Servicio

- Para el acceso a Internet se crean tres colas finales:
  - Cola de max prioridad para paquetes de mínimo retardo
  - Cola para paquetes con los bits "Max Throughput.º "Max Reliability.ªctivos
- En la interfaz Wifi definimos diez colas finales donde el tráfico http ocupa la mínima prioridad

Calidad de Servicio

- Para el acceso a Internet se crean tres colas finales:
  - Cola de max prioridad para paquetes de mínimo retardo
  - Cola para paquetes con los bits "Max Throughput.º "Max Reliability.ªctivos
  - Cola de mínima prioridad para el tráfico de usuario
- En la interfaz Wifi definimos diez colas finales donde el tráfico http ocupa la mínima prioridad

Monitorización de red

- Se emplea la aplicación JFFNMS para monitorizar la red

Monitorización de red

- Se emplea la aplicación JFFNMS para monitorizar la red
- Es un front-end de la RRDTool

Monitorización de red

- Se emplea la aplicación JFFNMS para monitorizar la red
- Es un front-end de la RRDTool
- Sistema monitorización sobre SNMP visual y sencillo

JFFNMS

- Se ha ampliado la funcionalidad de JFFNMS con un sistema de alertas vía correo o SMS

JFFNMS

- Se ha ampliado la funcionalidad de JFFNMS con un sistema de alertas vía correo o SMS
- Se han fijado problemas de la aplicación y se ha documentado la misma

Seguridad

- Se propone un sistema para el despliegue masivo de la red inalámbrica en la Universidad de Alcalá

Seguridad

- Se propone un sistema para el despliegue masivo de la red inalámbrica en la Universidad de Alcalá
- Autentificación de usuarios basada en certificados digitales con control de acceso basado en 802.1x

Seguridad

- Se propone un sistema para el despliegue masivo de la red inalámbrica en la Universidad de Alcalá
- Autentificación de usuarios basada en certificados digitales con control de acceso basado en 802.1x
- Creación de una autoridad de certificación propia basada en OpenCA

Seguridad

- Se propone un sistema para el despliegue masivo de la red inalámbrica en la Universidad de Alcalá
- Autentificación de usuarios basada en certificados digitales con control de acceso basado en 802.1x
- Creación de una autoridad de certificación propia basada en OpenCA
- Empleo de token criptográficos para almacenar las credenciales de los usuarios

802.1x y Protocolo RADIUS

- Sistema de generación de claves dinámicas para el medio para cada usuario

802.1x y Protocolo RADIUS

- Sistema de generación de claves dinámicas para el medio para cada usuario
- Se despliegan los sistemas de autenticación EAP-MD5, EAP-TLS y EAP-TTLS

802.1x y Protocolo RADIUS

- Sistema de generación de claves dinámicas para el medio para cada usuario
- Se despliegan los sistemas de autenticación EAP-MD5, EAP-TLS y EAP-TTLS
- Se decide emplear el servidor FreeRadius sobre Debian Linux
  - Problemas con el soporte de SSL
  - Se comprueba la configuración como proxy Radius de cara a poder integrarlo en proyectos como Eduroam

Esquema de autenticación con el protocolo Radius

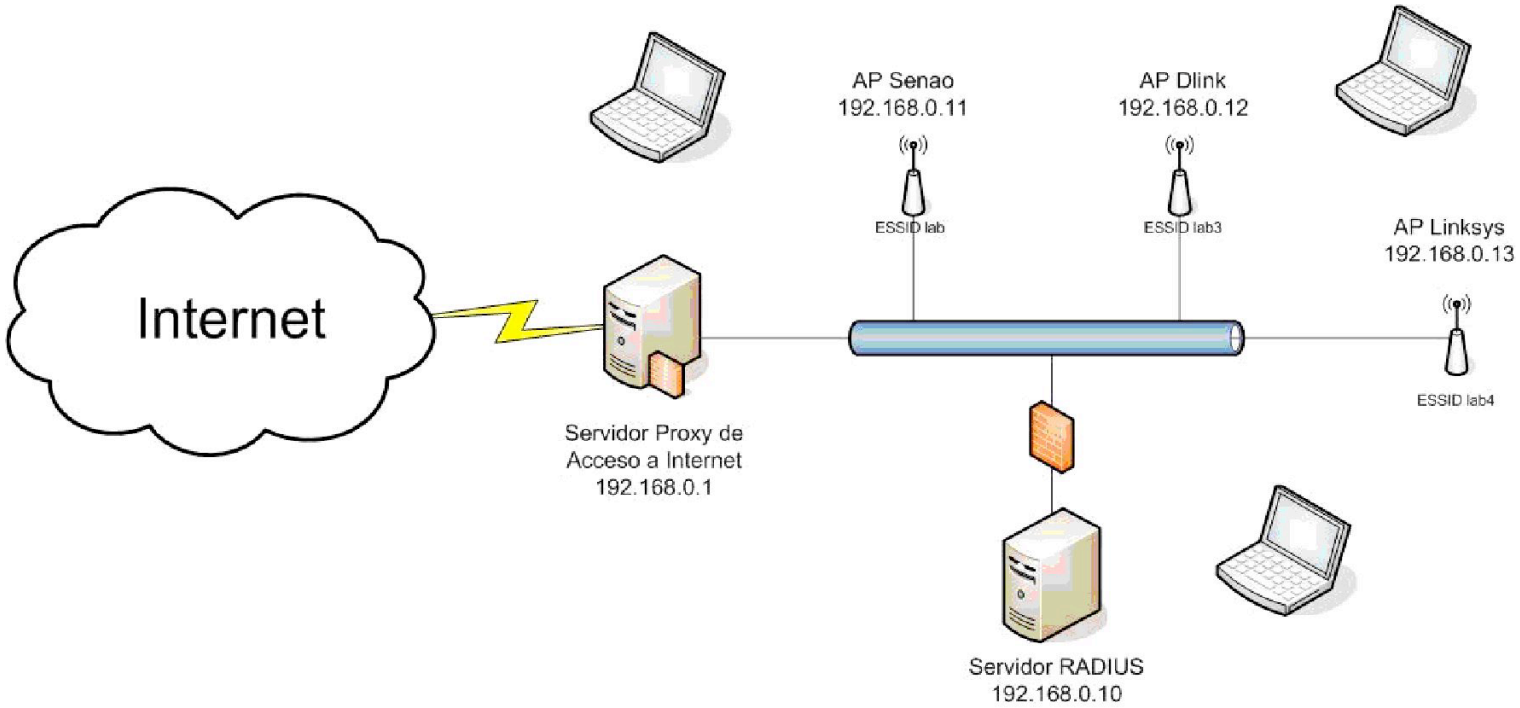


Figura: Radius

Configuración

- Se opta por emplear EAP-TLS: autenticación vía certificados digitales

Configuración

- Se opta por emplear EAP-TLS: autenticación vía certificados digitales
- Configuración de los puntos de acceso

Configuración

- Se opta por emplear EAP-TLS: autenticación vía certificados digitales
- Configuración de los puntos de acceso
- Empleo del WPA Supplicant con front-end desarrollado en Java

Certificados digitales en eToken

- La forma más segura de almacenar las claves privadas de los usuarios es dentro de dispositivos criptográficos

Figura: eToken

Certificados digitales en eToken

- La forma más segura de almacenar las claves privadas de los usuarios es dentro de dispositivos criptográficos
- Se despliega una prueba piloto de autenticación empleando Aladdin eToken

Figura: eToken

Prueba piloto

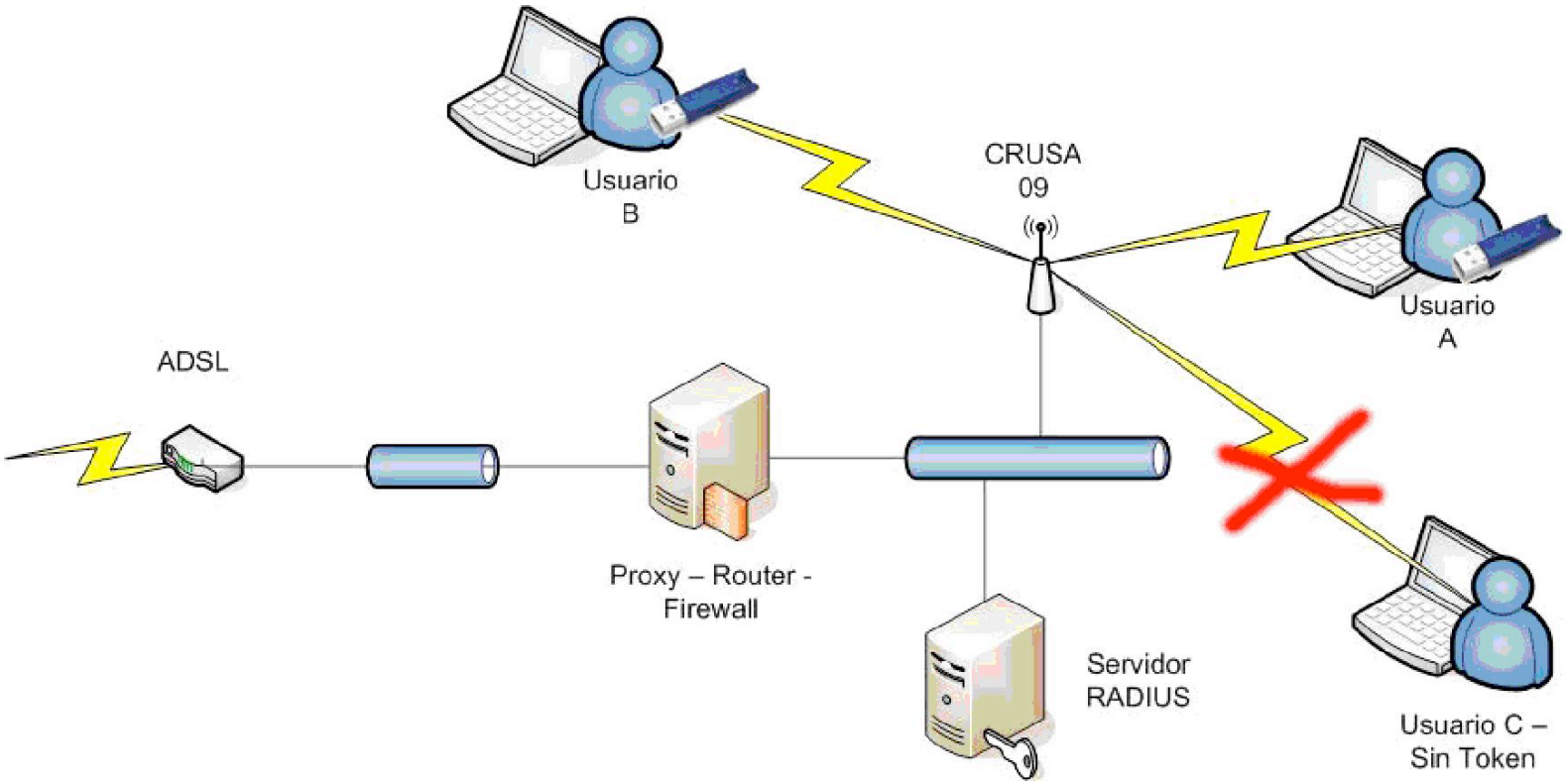


Figura: Prueba piloto

Autoridad de Certificación

- Se diseña una autoridad de certificación para su empleo en toda la universidad de Alcalá

Autoridad de Certificación

- Se diseña una autoridad de certificación para su empleo en toda la universidad de Alcalá
- Se emplea OpenCA 0.9.2 con soporte de OCSPD
  - Se traduce el paquete a Castellano

Resultados

- El sistema es capaz de proporcionar el servicio según los requisitos acordados
  - Se ha llegado a un máximo de 200 usuarios conectados simultáneamente
  - Los puntos de acceso han llegado a 25 usuarios simultáneos
- El sistema de gestión funciona adecuadamente y no afecta de modo apreciable al rendimiento de la red
- Queda pendiente el despliegue en toda la red del sistema de autenticación con certificados digitales

Estadísticas

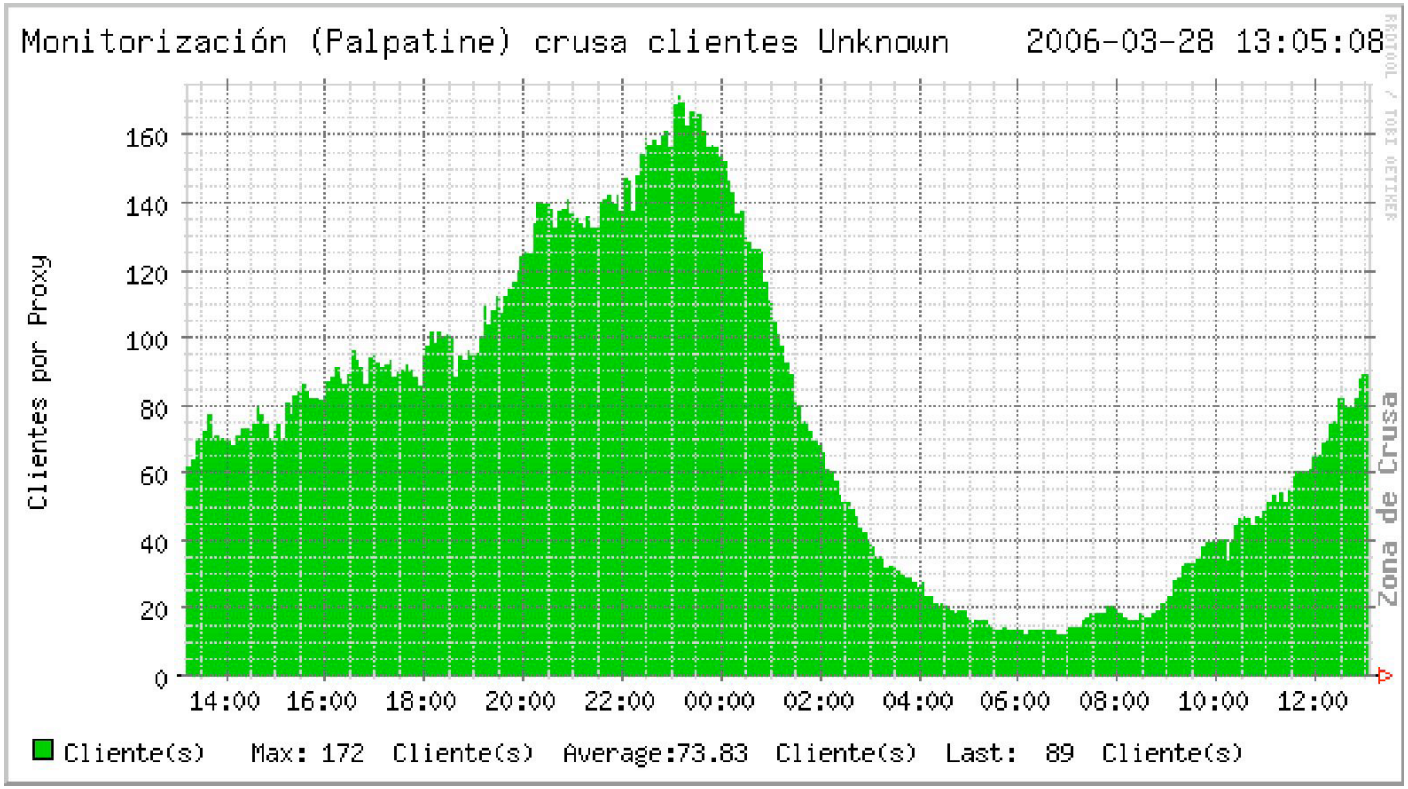


Figura: Usuarios simultáneos

Equipo de trabajo

- Alicia Caminero
- Antonio García
- Daniel Hernanz
- Enrique de la Hoz
- Miguel López
- Pablo Navas

Muchas gracias

- Muchas Gracias

Muchas gracias

- Muchas Gracias
- ¿Preguntas?