Javier Rodríguez e Ismael Senés-k idatzia
Astelehena, 2013(e)ko urtarrila(r)en 28-(e)an 10:18etan

There are no translations available.



Uno de los problemas mayores que nos estamos encontrando a la hora de implantar redes WIFI en los centros docentes es el de la elección de la tecnología. En muchos casos se han instalado puntos de acceso "domésticos" que son aptos para un entorno de baja demanda, pero que no son válidos para su uso en redes escolares debido al número de equipos que deben conectarse a cada punto de acceso y el consecuente solapamiento de canales.

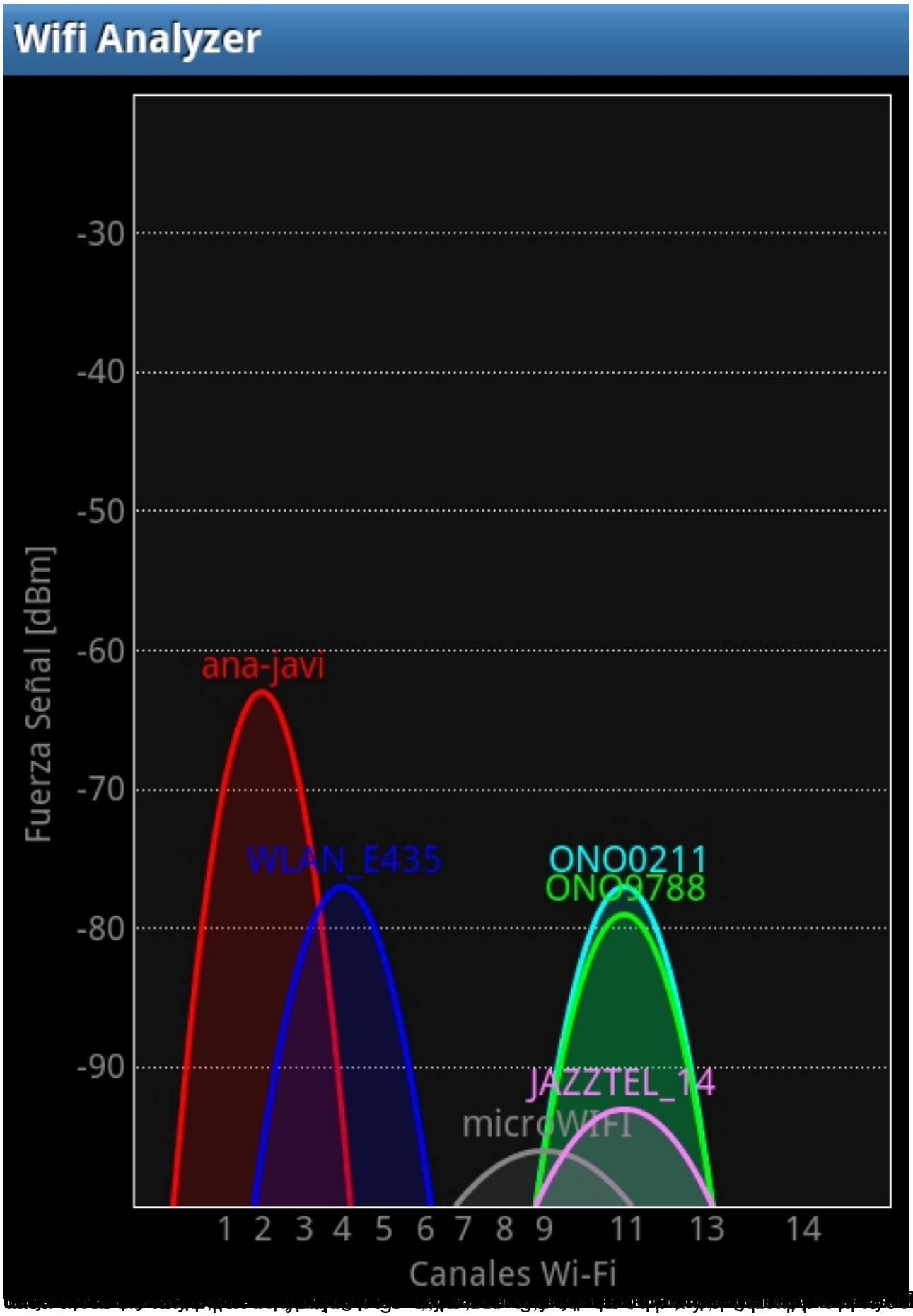
No es objeto de este artículo ver en detalle el funcionamiento de las redes inalámbricas, por lo que únicamente se dará una breve introducción para posteriormente, centrarse en las wifis con una gestión avanzada, capaces de solucionar los problemas de conectividad WIFI en los centros docentes.

Para más información de esta tecnología, existe un monográfico disponible en el Observatorio Tecnológico en la siguiente dirección:

http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi

Como todos sabemos, una red wifi es una red de datos que utiliza la señal de radio como soporte de transmisión, conformando por ejemplo una red de ordenadores que se conectan entre sí por una red inalámbrica, normalmente utilizando la banda de los 2.4 GHz, y cada día más, también la de los 5 GHz según la norma usada en cada caso.

Hasta hace poco hemos estado utilizando las normas 802.11b/g, que trabajan sobre la banda de 2.4GHz. Dicha banda está dividida en 13 canales de comunicación, el problema es que dichos canales están solapados, y pueden interferir en la comunicación entre varias redes inalámbricas, empeorando la calidad en la comunicación.


Wifi Analyzer
-30
-40
-50
-60
-70
-80
-90
Fuerza Señal [dBm]
ana-javi
WLAN_E435
ONO0211
ONO9788
JAZZTEL_14
microWIFI
1 2 3 4 5 6 7 8 9 11 13 14
Canales Wi-Fi

Soho de uso profesional

Soho es la contracción del término “Small Office – Home office”. Este término se utiliza habitualmente para indicar que un determinado hardware o elemento, está diseñado para un uso doméstico o de pequeña oficina, pero no a un nivel profesional, ya que tiene ciertas limitaciones que podrían hacer caer su rendimiento o incluso inutilizarlo en el caso de usos intensivos, las redes wifi actuales se ven en muchos casos infradimensionadas, demandando capacidades de conexión y funcionalidades para las que no fueron creadas.

Comentado esto, quizá el lector vaya tomando conciencia de la problemática actual de las redes wifis. La sensación generalizada es que la red wifi no funciona como la cableada. En muchas ocasiones hemos tenido que escuchar la frase de “la wifi funciona a ratos” o “se cuelga muy a menudo y deja de funcionar hasta que reseteamos los puntos”.

Esto no sucede porque los puntos de acceso sean malos, es porque hemos tratado de utilizar un hardware que tenía unas limitaciones y nos las hemos saltado.

Por ejemplo, en algunos entornos, como pudiera ser un centro educativo, en el que se han montado redes inalámbricas con este tipo de dispositivos, en un primer momento, todo funciona, ya que pocas personas conocen la clave de acceso a la red inalámbrica, y la usan con moderación, siempre dentro de las limitaciones marcadas por el fabricante.

Con el tiempo, la conectividad wifi comienza a dar problemas, ya que la clave se ha extendido rápidamente y el número de dispositivos ha aumentado de manera considerable. En la actualidad, casi todos llevamos un terminal wifi en el bolsillo, nuestro teléfono móvil por ejemplo.

¿Qué sucedería si nada más entrar al centro educativo todos activáramos nuestra wifi para conectar a las antenas del centro?, que en la mayoría de los casos saturamos los dispositivos hasta el punto de dejarlos colgados o en el mejor de los casos, que cuando llegan a su límite, no aceptan más conexiones inalámbricas y se produzca una denegación de servicio.

Para tratar de paliar esta problemática surgen las redes wifi profesionales, y como evolución de éstas, las redes wifi con gestión avanzada los puntos, objeto de este artículo.

La evolución, Wifis de gestión avanzada

Hasta la aparición de esta tecnología, la configuración de las redes era muy rudimentaria, dejando a la destreza del instalador gran parte del buen o mal funcionamiento de la red inalámbrica. En muchas ocasiones no se ha realizado un estudio de coberturas previo, de canales ya utilizados, etc., lo que hace que el rendimiento de la red caiga y no sea óptimo, como ya se ha comentado.

Con las wifis de gestión avanzada, son los dispositivos los que toman capacidad de determinadas decisiones, incluso para modificar su configuración, con el consiguiente aumento de rendimiento. Los puntos de acceso y posibles controladores (que trataremos más adelante) se comunican entre sí a nivel 2 del protocolo OSI (OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones), por lo que son capaces de ponerse de acuerdo entre todos y establecer una configuración óptima, incluso teniendo en cuenta la configuración de otras redes cercanas y que pudieran interferir con la nuestra.

Además, esta “inteligencia” del hardware, le permite protegerse de ataques, de determinados dispositivos no deseados en nuestra red o de caídas de algunos de los puntos de acceso.

Veamos algunas de las funcionalidades que nos ofrecen:

Diferentes tipos de redes

Con un solo punto de acceso, es posible crear diferentes redes que serán difundidas como si se trataran de un grupo de puntos de acceso convencionales. Es decir, que con el mismo hardware, podemos hacer que se difundan tres redes inalámbricas diferentes:

-

Red de trabajadores: Desde la que tendremos acceso a todos los servicios de red de la empresa o centro educativo, sin limitaciones.

-

Red de telefonía: Que tendrá una mayor prioridad a la hora de enrutar los paquetes, ya que serán marcados con una calidad de servicio alta, lo que garantizará que los paquetes viajen en tiempo real y sean priorizados frente a otro tipo de tráfico, evitando así los cortes de voz.

-

Red de invitados: En la que únicamente se permite la navegación básica y con un caudal muy limitado para evitar abusos y que influya en la calidad de red de las dos anteriores.

Banda preferente

Se puede elegir la banda que utilizaremos para la emisión de radio. Si todo nuestro hardware de red es más bien moderno, podemos utilizar la banda de 5 GHz, con las ventajas que ya se han comentado.

En caso de tener un parque informático un poco más antiguo, es posible que las tarjetas de red inalámbrica no soporten esa banda, teniendo que utilizar la de 2.4 GHz, o incluso dejar abierto a que se establezca la banda en cada caso concreto, priorizando el utilizar la banda superior en caso de que sea posible su uso.

Elección del canal más adecuado

Un sistema wifi de gestión avanzada es capaz de hacer su propio estudio de uso de canales y frecuencias, y adaptarse al más óptimo en cada caso. Incluso algunos puntos de acceso tienen la capacidad de aumentar o disminuir su potencia para no influir en zonas donde tienen visibilidad con otros puntos, evitando de esta forma interferencias entre ellos.

Métodos de autenticación

Uno de los mayores problemas de las redes wifis era el logado masivo de dispositivos a nuestra red, lo que hacía que los puntos se colapsaran o dejaran de prestar servicio una vez llegado a su límite. Para evitar este problema, aparecen diferentes formas de autenticar a las máquinas que pueden utilizar nuestra red inalámbrica, impidiendo los accesos no autorizados a la red. Las más conocidas son:

-

Captive portal: Quizá el más conocido, ya que es el adoptado en la mayoría de wifis de hoteles o zonas de ocio. En este caso, se pueden establecer unos tickets o pares usuario/clave para uso y disfrute de la red. La wifi parece abierta, pero una vez estamos conectados y comenzamos la navegación, nos aparece una web que nos pide la autenticación para permitirnos el acceso a Internet.

-

Autenticación por MAC: Todo equipo electrónico susceptible de conectarse a una red de datos, tiene asociado un número único que lo identifica, la llamada MAC Address. Es posible permitir el acceso únicamente a los dispositivos que estén registrados con su número de MAC en el sistema, impidiendo al resto cualquier actuación con la red.

-

Por tipos de dispositivos: Quizá se está pensando en eliminar de la lista de dispositivos autorizados los teléfonos móviles personales, en este caso es posible limitar hasta el detalle de prohibir determinadas marcas o modelos de terminales. Por ejemplo, si tenemos un problema de accesos no permitidos desde los teléfonos móviles de los alumnos, podemos prohibir las conexiones generadas desde una BlackBerry, iPhone, SmartPhones de Samsung, etc.

-

Certificados: Utiliza el concepto de certificados, como el usado en las páginas web seguras. Podríamos autenticar los accesos, en lugar de con usuario y clave, directamente con su DNI electrónico, por ejemplo.

-

Radius: Uno de los protocolos más extendidos en el caso de haber algún sistema de facturación por tráfico, aunque también muy extendido en las sistemas con directorio activo o ldap.

VLANs

Cuando el parque informático es grande, si todos los equipos estuvieran conectados a la

misma red, determinados paquetes de difusión podrían perjudicar el rendimiento, es por esto, que se hace necesaria una segmentación de la misma, evitando las colisiones de un gran número de equipos tratando de acceder al mismo medio de comunicación.

Al igual que en las redes cableadas, en las inalámbricas tenemos la capacidad de crear diferentes redes locales virtuales (Vlans = Virtual Local Area Network), organizando nuestra red e incluso, dando diferentes permisos de acceso a determinados recursos dependiendo de la vlan a la que nos conectemos.

Detección de intrusos

Todos sabemos que con determinado software, es posible sacar algunas claves de redes inalámbricas, lanzando ataques sobre los puntos de acceso.

El hardware de wifis de gestión avanzada es capaz de detectar estos ataques y protegerse de ellos, obviando todos los paquetes que provienen de la máquina atacante, de tal forma que no sea posible obtener la clave por los métodos convencionales. Por tanto, redes más seguras y eficientes, ya que evitamos usos indebidos de las mismas.

Filtrado de contenidos

Es posible la generación de un listado de páginas web prohibidas, o lista negra, y el propio sistema se encargará de que ningún terminal conectado pueda acceder hasta ellas. También al contrario, se puede prohibir toda la navegación a excepción de las webs autorizadas mediante lista blanca.

Este sistema puede suponer un duro trabajo de recopilación de páginas web susceptibles de ser prohibidas, además de su categorización. Para hacer esto más sencillo, en Internet hay grupos de trabajo que ya han hecho gran parte de esta catalogación, pudiendo utilizar sus listas negras y mejorarlas con el día a día.

Filtrado de conexiones por protocolo

En muchas ocasiones se ha logrado prohibir un determinado tráfico de descargas cerrando los puertos más utilizados. Por ejemplo, podemos cerrar los puertos del protocolo TCP 4661, 4662 y UDP 4665 y 4672 para evitar descargas con Emule o similares, pero estos programas tienen

la capacidad de poder configurar el puerto, siendo muy complicada la detección de su funcionamiento en una red, a no ser por el consumo de ancho de banda.

En las wifis de gestión avanzada, es posible prohibir por tipo de tráfico, pase por el puerto que sea, o incluso permitirlo, pero con un consumo moderado de la red. Se podría llegar a dejar abierto el uso de programas de descargas tipo Emule, pero limitarle el tráfico a un 5% del total de nuestra red.

¿Es necesario un controlador?

En la mayoría de estos sistemas, se hace necesaria la inclusión de un nuevo elemento, el controlador. Este hardware suele ser una máquina, u ordenador, con la misión de controlar todos los puntos de acceso que hay en el sistema y aportarles algunas de las funcionalidades comentadas anteriormente.

Estos controladores dan acceso a un gran número de funcionalidades adicionales:

-

El acceso remoto a cualquiera de las redes que difunde nuestro sistema wifi. Es posible conectarse por VPN hasta el controlador y desde ahí saltar a cualquiera de las redes que estén configuradas en el sistema.

-

Estadísticas de uso a unos niveles de detalle muy altos, hasta el punto de saber los consumos de red de cada usuario, las horas a las que se conecta, qué tipo de tráfico genera (vídeo, descargas, audio, etc) y su historial de navegación entre otros.

-

Control más exhaustivo de la configuración de los puntos de acceso, pudiendo incluso ser de diferentes marcas, siempre que soporten determinadas funcionalidades.

-

Gestión de todo el sistema desde cualquier parte, incluso con la posibilidad de una consola centralizada para varios controladores conectados a ella, por lo que sería viable la gestión y mantenimiento de muchos centros de una forma cómoda y sin desplazamientos. Algunos sistemas sin controlador también lo permiten, pero con limitaciones en las funcionalidades.

-

Posibilidad de caché en local, optimizando el acceso al exterior. Si un alumno entra a la web del INTEF, el controlador descarga esta información en local, sirviéndola desde aquí al resto de peticiones, sin utilizar las líneas de ADSL o fibra hacia el exterior, y con el consiguiente aumento de la velocidad de navegación.

El inconveniente en este caso, es que un sistema con controlador, hace que el precio suba considerablemente, lo que en muchos casos lo convierte en inviable.

Por esta razón, comienzan a estar disponibles sistemas en los que el controlador es virtual, y su potencia está distribuida entre los puntos de acceso, que al comunicarse entre sí, son capaces de realizar una gran parte de las funcionalidades que aportaría un controlador, con un nivel de exigencias inferior, pero suficiente para muchos de los entornos.

Conclusiones

Las wifis des gestión avanzada no sólo nos aportan un mayor ancho de banda por el aumento en la velocidad del tráfico que son capaces de gestionar, si no que además, añaden los mecanismos suficientes para poder optimizar los consumos y moldear las necesidades y permisos en cada caso concreto.

Por contra, es necesaria una mínima gestión de estos sistemas, pudiendo vigilarse de forma centralizada o no.

Al igual que con anteriores tecnologías, es vital un primer estudio en el que poder detectar e implantar la mejor configuración posible para obtener el máximo rendimiento. Un sistema bien configurado puede soportar 30 terminales con vídeo en tiempo real y de alta definición (en red

local o Internet dependiendo del ancho de banda de salida y la caché local) sobre el mismo punto de acceso.

Aunque son redes mucho más potentes, también tienen sus limitaciones, por lo que antes de adquirir un sistema u otro, habrá que fijarse bien en las características técnicas del equipamiento. Todas las marcas tienen varias gamas de productos de cuarta generación, por lo que habrá que prestar especial atención a qué nos permite cada dispositivo y las diferencias entre unos y otros.