

Desafíos para asegurar la calidad del servicio de internet inalámbrico en la Universidad Francisco Gavidia

Challenges to ensure the quality of wireless internet service at the Francisco Gavidia University

Mario Rafael Ruiz Vargas

Ingeniero en Ciencias de la Computación y
Máster en Informática Aplicada a Redes,
Universidad Francisco Gavidia, El Salvador.
Máster en Ciencia y Tecnología Informática y
Doctor en Ciencia y Tecnología Informática,
Universidad Carlos III de Madrid, España.

Director de Tecnología y Sistemas en la Universidad Francisco Gavidia
mario@ufg.edu.sv

RESUMEN

El proyecto "Aseguramiento de la conectividad de la red inalámbrica y calidad en el acceso al servicio de internet", contempla el desarrollo de una solución a las necesidades de conectividad WiFi en la Universidad Francisco Gavidia. La UFG a partir del año 2008 instaló la primera infraestructura que permitió ofrecer el servicio de internet inalámbrico en su campus. Sin embargo, se tuvo que superar grandes desafíos para ofrecer un servicio que permita abarcar el mayor número de usuarios con un nivel aceptable de servicio y que contara con medidas de seguridad apropiadas para una institución de educación superior.

Palabras clave: Internet inalámbrico, gestión de la conectividad, arquitectura WLAN, autenticación de red, perfiles de usuario de red inalámbrica.

ABSTRACT

The project: "Securing of the connectivity wireless network and quality in the access Internet service", includes the development of a solution to the connectivity needs in the Francisco Gavidia University from El Salvador. The UFG since 2008 installed the first infrastructure, which allowed wireless service on its campus. However, there were many challenges to offer a service allowing include as many users, with an acceptable level of service and that has appropriate security measures for an institution of higher education.

Keywords: Wireless internet, connectivity management, WLAN architecture, network authentication, user profiles wireless network.

Introducción

La Universidad Francisco Gavidia, con el objetivo de mejorar los servicios que brinda a sus estudiantes, ha definido entre sus líneas estratégicas la satisfacción permanente del estudiante y el apoyo de proyectos encaminados a cumplir este objetivo; por esta razón desde el año 2008 puso oficialmente a disposición en todo el campus la conexión a la red inalámbrica.

En sus inicios, el internet inalámbrico en el campus era un servicio que se ofrecía como valor agregado. Pero con el pasar del tiempo, comenzó un crecimiento en la demanda de una conexión a internet inalámbrica dedicada. Para llegar a ofrecer una buena experiencia al usuario, primero se tuvieron que vencer diferentes obstáculos y se probaron distintas soluciones para lograr satisfacer la necesidad actual y anticiparnos a las necesidades futuras.

Entre los resultados obtenidos con la implementación del proyecto, se tiene la mejora significativa del acceso y la calidad del servicio de internet inalámbrico que la Universidad ofrece a sus usuarios académicos y administrativos, la gestión de perfiles de usuarios y la integración con otros sistemas; privilegios asignados por categorías de usuarios, permitiendo simplificar la gestión de las credenciales para el acceso al servicio de internet inalámbrico.

La solución actual, es un servicio que conlleva componentes estratégicos de planeación, determinación de las necesidades de los estudiantes, docentes y demás personal de la Universidad, así como satisfacción de dichas necesidades y proyección de recursos

informáticos. Dicha solución permite ofrecer un servicio de internet inalámbrico con una experiencia de usuario satisfactoria; para ello nos valemos de una administración centralizada de los diferentes perfiles de usuarios, herramientas de monitoreo y seguridad, y optimización del ancho de banda.

El proyecto se considera que puede ser replicado por otras instituciones que deseen ofrecer un servicio de internet inalámbrico o estén enfrentándose a problemas y desafíos similares a los que se enfrentaron, que nuestra institución superó hasta lograr satisfacerlos.

1. Antecedentes

Inicialmente, en el año 2008, se dispuso de 15 equipos de red inalámbrica que sirvieran como puntos de acceso (AP) y se colocaron aproximadamente uno por cada dos niveles en cada uno de los edificios de clases; además, se colocaron 10 AP en los edificios administrativos. Para ese año, el tráfico de la red inalámbrica no era tan representativo respecto al resto de tráfico de la red cableada, por ello se tenía un ancho de banda unificado para ambos servicios. Durante los dos años siguientes el servicio funcionaba relativamente bien, brindando conexiones a los usuarios ocasionales que en momentos específicos necesitaban utilizar la red inalámbrica.

En vista de que el servicio de internet inalámbrico se ofrecía como un valor agregado, no recibía quejas o incomodidades, pues el servicio no se consideraba algo indispensable. El método de autenticación que se utilizaba era WEP, que es el nivel más bajo de seguridad por clave compartida para una red inalámbrica;

sin embargo en su momento, este tipo de autenticación ofrecía la mayor compatibilidad con los diferentes dispositivos de los usuarios (Curran & Smyth, 2006). La clave de acceso a la red inalámbrica pronto fue del dominio público entre los estudiantes e incluso los negocios aledaños a la institución.

Con el paso del tiempo, los dispositivos móviles fueron haciéndose más populares entre nuestros estudiantes, y a la vez que aumentaban las capacidades de estos dispositivos, también lo hacía la demanda de ancho de banda por conexión. El aumento en el uso de computadoras portátiles por parte de la población universitaria y la motivación cada vez mayor a utilizar los sistemas y servicios en línea de la institución, tendían irreversiblemente hacia una demanda de conectividad cada vez mayor.

Además, era imperativo contar con un sistema de autenticación que permitiera asegurar la conectividad exclusivamente a los miembros de la institución y ser capaces de regular el acceso al contenido no académico.

Algunos de los problemas que se solventaron con el proyecto fueron la cantidad insuficiente de equipos para proveer conectividad a todos dispositivos que requerían conexión y la inauguración de un nuevo edificio en el año 2013, que no contaba con la cantidad suficiente de equipos que brindaran acceso a la red inalámbrica. Los equipos no eran capaces de responder a todas las solicitudes, por lo que comenzaban a denegar los intentos de conexión y era necesario reiniciarlos.

Entre otras cosas, los miembros de la comunidad universitaria comenzaron a utilizar, además de

sus computadoras portátiles, tabletas y teléfonos inteligentes, multiplicando por un factor de 3 las necesidades de conectividad. En ese entonces no existía una herramienta que gestionara el acceso a la red inalámbrica, sino que la autenticación se realizaba por medio de WEP, y aunque posteriormente se utilizó WPA, casi cualquier persona podía conectar sus dispositivos a la red con solo conocer la contraseña.

Se tenían vulnerabilidades que podrían ser explotadas, pues la red inalámbrica se separaba de la red cableada únicamente por VLAN. No se contaba con un método específico para autenticar a los visitantes que necesitaran acceso a la red inalámbrica. El servicio de internet inalámbrico era provisto como un “valor agregado”, por lo que no existía un contrato basado en un acuerdo de nivel de servicio SLA (*Service Level Agreement*) con el proveedor de servicios de Internet ISP (*Internet Service Provider*), para asegurar la disponibilidad del servicio, y no existía un ancho de banda dedicado exclusivamente al servicio de internet inalámbrico. Otro de los puntos importantes era utilizar canales que no interfirieran con los equipos de red inalámbrica de las empresas cercanas o entre sí mismos, ya que provocaba una señal atenuada.

1.1. Población meta

En la actualidad la red inalámbrica implementada brinda el servicio al 100% de la población en la Universidad Francisco Gavidia. Esto incluye:

- Personal administrativo: directores, coordinadores y empleados (más de 300 personas).

- Usuarios académicos: estudiantes de nuevo ingreso, carreras de Pregrado y Postgrado, decanos y docentes (más de 15,000 personas).

Es importante destacar que cada usuario está autorizado para conectar a la red inalámbrica hasta tres dispositivos de forma simultánea.

1.2. Área de desarrollo

La Universidad Francisco Gavidia de El Salvador posee dos sedes, la Sede Central localizada en la capital San Salvador, principal campus de la institución educativa; además, un Centro Regional en el Occidente del país específicamente en la ciudad de Santa Ana. El servicio de internet cableado e inalámbrico está disponible para la comunidad educativa en general, sin importar la sede geográfica a la que pertenezca. Desde hace algunos años la UFG ha integrado casi todos sus sistemas informáticos, plataformas y servicios para ingresar mediante un único portal web conocido como WebDesktop, esto permite que los usuarios utilicen una sola credencial para ingresar a diferentes sistemas. La credencial de acceso al WebDesktop es también utilizada como método de autenticación en la red inalámbrica de la institución. Sin importar el campus en que se encuentre el usuario, puede hacer uso del servicio y utilizar los beneficios asociados a su perfil.

1.3. Propósito

Proveer una solución a las necesidades de conectividad inalámbrica que tienen los miembros de la comunidad universitaria. Asegurar la cobertura en las diferentes áreas que componen la institución y brindar un servicio

estable, todo esto soportado por un ancho de banda para suplir la demanda del contenido consultado a través del internet inalámbrico.

Definir un sistema de autenticación de usuario de la red inalámbrica, que permitiera asegurar el acceso únicamente a los miembros de la comunidad universitaria y, además, incluir el componente de seguridad necesario para ofrecer un acceso a las actividades e interacciones en internet de forma confiable.

Contar con un sistema de monitoreo capaz de proveer información dinámica sobre la cantidad de usuarios conectados, el consumo en el ancho de banda dedicado a la red inalámbrica, detectar cualquier actividad irregular en la red y manejar otros datos estadísticos.

2. Desarrollo e implementación del proyecto: Aseguramiento de la conectividad a la red inalámbrica y calidad de servicio

Alrededor de 15 mil estudiantes de la Universidad Francisco Gavidia tienen a su disposición el acceso a una red inalámbrica como herramienta para el desarrollo de sus actividades académicas. Para poder conectarse a la red inalámbrica los estudiantes emplean las mismas credenciales de su WebDesktop, que integra los sistemas y servicios en línea que posee la institución.

Contar con una red inalámbrica en todo el campus hace posible que la comunidad universitaria conecte a internet sus dispositivos móviles y computadoras portátiles, desde auditorios, aulas, bibliotecas, cafeterías y zonas de esparcimiento. La comunidad universitaria tiene a su disposición una gama

de servicios institucionales en línea, acceso a libros de texto completos, investigaciones y repositorios electrónicos e internet por medio de una conexión segura. A la vez que es posible monitorear la actividad de los usuarios en la red inalámbrica, el rendimiento de esta y definir roles, permisos y restricciones, así como un control granular del contenido, para asegurar un óptimo nivel de rendimiento/uso de la red inalámbrica, rúbricas/directrices que brindan información en tiempo real o mediante registros históricos, todo ello a través de una conexión segura sobre internet inalámbrico.

2.1. Factores determinantes en la elección de la solución

Para diseñar y poder implementar una solución de red inalámbrica que especialmente fuera utilizada por todos los miembros de la institución educativa, fue necesario considerar los objetivos de mejora continua de los servicios y procesos de la institución, así como hacer énfasis en las líneas estratégicas de la institución: excelencia académica, satisfacción permanente, crecimiento integral y proyección institucional. Ello permitió trazar el objetivo final de este proyecto.

En el ámbito técnico buscábamos implementar una solución capaz de mejorar la calidad del servicio, asegurar la conectividad de los usuarios y la gestión de los accesos a la red inalámbrica. Dicha solución debería ser capaz de automatizar la inclusión de nuevos usuarios y tener el potencial para heredar los roles de los usuarios a nivel institucional. La infraestructura debía ser capaz de adaptarse a las necesidades y crecer para los requerimientos futuros.

Gracias a la implementación de esta solución de red inalámbrica se hizo posible aumentar el uso de los servicios en línea en todo el campus. En vista de este incremento de uso de dispositivos móviles, se diseñaron versiones móviles de los sistemas para los diferentes sistemas móviles; ahora, al ingresar al internet inalámbrico de la UFG los estudiantes tienen la oportunidad de utilizar estas herramientas en un formato ajustado a sus dispositivos y realizar sus actividades utilizando una conexión segura.

2.2. Fases previas a la planificación de la nueva solución

En el año 2004 se designaron puntos de acceso de red inalámbrica para algunas bibliotecas del campus. Se utilizaban 5 AP Cisco Aironet 1231. En aquel entonces los estudiantes se sentían cómodos haciendo uso de internet inalámbrico en las bibliotecas pues lo utilizaban únicamente en sus computadoras portátiles. Sin embargo, con el pasar de los años, el uso de computadoras portátiles se fue incrementando y con ello la necesidad de acceder a internet desde las aulas. Inicialmente, la seguridad no era una de las mayores preocupaciones, por lo que la autenticación a la red inalámbrica se realizaba por medio de una clave WEP.

Cada AP tenía la capacidad para gestionar 2048 direcciones MAC. Sin embargo, dados que el AP es un medio compartido y que funciona como un concentrador inalámbrico, el desempeño de cada usuario disminuye a medida en que aumenta el número de usuarios en un AP individual. Idealmente, no más de 24 clientes deben asociarse con el AP, ya que el desempeño de procesamiento del AP se reduce con cada cliente que se asocie

con el mismo; por lo tanto, la capacidad que se tenía era de 120 clientes. En cada salón de clase existe por lo menos un punto de red cableada y los docentes estaban habituados a portar un cable de red para hacer uso de la misma. No obstante, se percibía la necesidad de brindarles acceso a internet también a los estudiantes.

Durante los años 2008 a 2010 se lanzó el primer proyecto que buscaba ofrecer acceso a internet mediante una red inalámbrica que abarcara también las aulas. Para ese efecto se destinaron 25 puntos de acceso a la red inalámbrica, 19 en la sede de San Salvador y 6 para la sede de Santa Ana. Los equipos que se utilizaban eran ZyXel Prestige 334, TP-LINK 701ND, D-Link 2360 y Aironet 1242AG. Durante un tiempo se cubrió la demanda de conexiones, pero únicamente se brindaba el servicio en los edificios de clases y no se brindaba cobertura completa a las aulas, pues los puntos de acceso estaban al centro de cada nivel de los edificios de aulas, así que los usuarios debían colocarse cerca del centro para asegurarse una mejor señal. Se tenía capacidad para atender 600 conexiones. (Ver Figura 1).

Con el propósito de ofrecer una mejor conexión a la red inalámbrica de la institución, en el año 2012 se desarrollaron esfuerzos para incrementar el número de AP en las aulas, iniciando así el primer proyecto que contemplaba una cobertura para todo el campus. Para ello se consideraron 34 nuevos equipos de acceso entre los que se contaban con FAT AP modelos GoNet 2100, 1100, 510 y modelos thin/Thick AP 160 (Soni & Mendiratta, 2008). Estos se distribuyeron de tal forma que se brindara cobertura a la mayor área posible. Los modelos 2100 y 1100 soportaban hasta 150 usuarios cada uno y el resto

un promedio de 20, y se tenía una capacidad para 1,720 usuarios. Cabe mencionar que la tecnología GoNet fomentaba la creación de una malla de WiFi para grandes áreas físicas, como se puede observar en la Figura 1.

Por primera vez la Universidad Francisco Gavidia ofrecía cobertura de acceso a la red inalámbrica en todo el campus. Sin embargo, el crecimiento exponencial en el uso de dispositivos móviles y la disponibilidad de la red fomentó el crecimiento en la demanda de conexiones. Provocando un escenario en el que teníamos cobertura en todo el campus, pero no éramos capaces de asegurar la estabilidad en las conexiones de los usuarios. En las horas pico algunos usuarios eran desconectados o simple y sencillamente los equipos se congelaban y era necesario reiniciarlos.

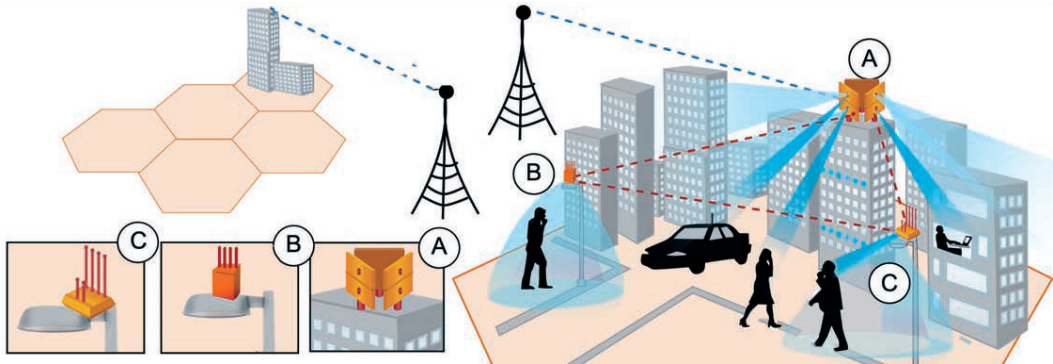
Además, junto con una gran área de cobertura se incrementó la cantidad de usuarios haciendo uso de la red inalámbrica, y aunado a esto, debido al uso de una autenticación bajo una sola contraseña, era posible que diferentes personas ajenas a la institución hicieran uso de nuestra red incrementando el tráfico y consumo del ancho de banda. En este escenario era muy difícil obtener información de los usuarios de la red y determinar su pertenencia a la institución o establecer perfiles de usuario, lo que impedía definir restricciones de forma particular.

3. Implementación del proyecto de servicio de red inalámbrica

En el segundo semestre del año 2014 la Universidad Francisco Gavidia tomó a bien ampliar la infraestructura de red inalámbrica, con

Figura 1

La tecnología GoNet promovía el uso de una red tipo malla para grandes áreas de cobertura (A. MBW 2000 base de alto rendimiento con cobertura omnidireccional y multi-radio. B. MBW 1100, estación base para una efectiva cobertura a nivel de calle. C. MBW 500 dispositivo para el despliegue de redes ad hoc y cubrir necesidades baja demanda Wi-Fi.).



Fuente: Ilustración tomada de: http://www.go80211.com/products/GO_MBW1000_WLP1100.pdf.

el afán de fomentar el uso de la Tecnología, la Innovación y la Calidad, poniendo este servicio a disposición de todos sus estudiantes, docentes, personal administrativo y visitantes.

3.1. Análisis de las necesidades y definición de requerimientos

Con este proyecto se buscaba obtener una solución de red inalámbrica con tecnología WiFi a diferentes ISP, que ofreciera cobertura a todo el campus universitario. Junto con un proveedor de servicio se realizaron diferentes visitas para inspeccionar el campus y los salones de clase, se contabilizaron las capacidades de los salones y se estimó la cantidad de conexiones inalámbricas.

Se transformó el enfoque, pasamos de pensar en áreas de cobertura a pensar en la calidad del servicio y por ello se consideró una

cantidad mayor de equipos de acceso. Por esta misma razón era necesario definir un equipo Controlador Central que hiciera posible difundir políticas de navegación, desplegar configuraciones, seguridad, aplicar métricas de optimización en un mismo SSID y poder configurar la funcionalidad de Roaming al desplazarse de un área a otra entre Puntos de Acceso. Debido a la mayor cantidad de puntos de acceso debía considerarse la potencia de los equipos, la frecuencia y los canales a utilizar, para evitar la interferencia entre señales (Sarddar, Jana, Patra, Biswas, & Naskar, 2010).

El estándar utilizado al implementar redes inalámbricas es el IEEE 802.11, conocido como WiFi, IEEE 802.11b e IEEE 802.11g, que operan en la banda de 2.4 GHz; la versión IEEE 802.11a opera en la banda de 5GHz y el estándar IEEE 802.11n opera en ambos rangos de frecuencia (Hiertz *et al.*, 2010; Ni, 2005).

3.2. Tecnología a utilizar

Se determinó utilizar puntos de acceso del tipo *Thin Access Point*, los cuales están conectados a un controlador inalámbrico encargado de la gestión y el tráfico de la red; este tipo de AP permite ahorrar tiempo y dinero, ya que la configuración se realiza en la controladora. La decisión de utilizar este tipo de equipos tomó en cuenta casos de éxito conocidos anteriormente (Sou, 2014). Algunas de las funcionalidades de estos equipos que vale la pena destacar son estas:

Balanceo de carga. Permite distribuir el tráfico de manera más eficiente entre los AP y las bandas de frecuencia disponibles. El controlador utilizado permite los siguientes tipos de balanceo: “Access Point Hand-off”, que indica a un cliente la posibilidad de conectarse a un AP más cercano dependiendo de la carga máxima que este pueda soportar; y el tipo “Frequency Hand-off”, este permite al controlador administrar el uso de las bandas de 2.4 GHz y 5 GHz indicando al cliente la frecuencia con menos uso.

Automatic Radio Resource Provision (ARRP). Utilizado para evitar la interferencia entre los AP. Cuando se activa un perfil de AP se mide la utilización y la posible interferencia en los canales disponibles, seleccionando el canal más apropiado para cada AP. La medición puede repetirse periódicamente para responder a algún cambio del medio.

Roaming. O itinerancia, que permite a los usuarios desplazarse por las zonas de cobertura e irse registrando en los diferentes puntos de acceso; de esta forma el usuario tiene la sensación

de no perder la conexión mientras se desplaza entre diferentes zonas físicas del campus.

Sistema de Prevención/Detección de Intrusos. Detección y supresión de AP Rogue, que realiza escaneos periódicos para detectar puntos de acceso no autorizados. (Ver Figura 2).

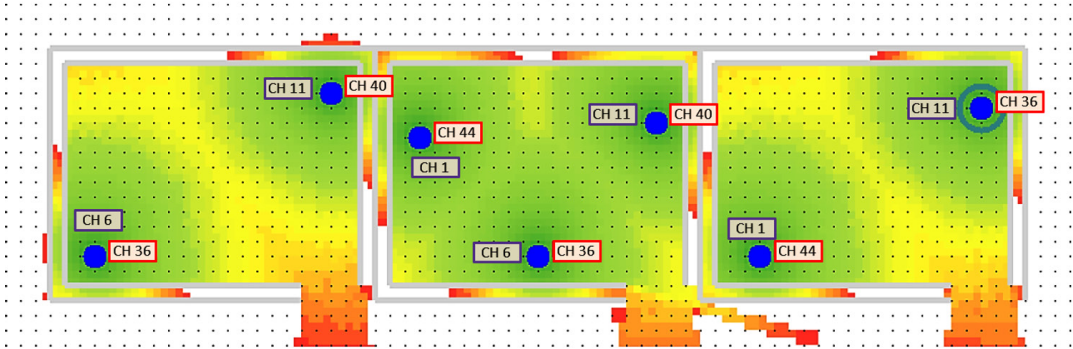
IEEE 802.11e y QoS basado en aplicaciones. Para que la implementación de la solución funcionara en 2 frecuencias simultáneamente, se determinó utilizar los canales 1,6 y 11 del rango de frecuencias que opera a 2.4GHz en arreglos de hasta tres AP por salón de clase, para evitar colisión en la frecuencia de los canales. Los mismos equipos utilizados hacen posible la conexión en el rango de frecuencia de 5GHz, para los cuales se han considerado los canales 36, 40 y 44 en el mismo arreglo y con los mismos equipos, hasta tres AP por salón de clase. En la Figura 2 se puede observar una simulación por computadora de las áreas de cobertura en la frecuencia de 2.4 GHz. También en la Figura 2 se puede observar una simulación por computadora de las áreas de cobertura en la frecuencia de 5 GHz; la única diferencia es una leve disminución en la amplitud de la señal (Sarddar *et al.*, 2010). Posteriormente al estudio se llegó a la cifra de 385 AP para satisfacer las necesidades de la institución. Con esto fue posible tener la capacidad para ofrecer el servicio de internet inalámbrico a un promedio de 11,550 dispositivos simultáneamente.

3.3. Autenticación de usuarios

Se definieron las reglas bajo las cuales se realiza la autenticación de acceso a la red inalámbrica. Para conseguir la autenticación de las credenciales se empleó un método conocido como REST,

Figura 2

Configuración del área de cobertura de los AP colocados dentro de las aulas. Rango de frecuencia 2.4 GHz: canales 1, 6 y 11; para la frecuencia de 5 GHz: canales 36, 40 y 44.



mediante el cual se verifica la identidad de quienes pretenden ingresar al sistema a través de un portal captivo, se genera una solicitud de POST y se recibe una respuesta JSON.

La red de autenticación inalámbrica aparentemente está abierta; pero cuando se conecta el usuario, el servidor RADIUS solicita ingresar las credenciales de acceso mediante una conexión HTTPS. En la Figura 3, se muestra el diagrama de flujo del proceso de autenticación. (Ver Figura 3 y 4).

Perfiles

Se crearon diferentes perfiles de usuario con el objetivo de proveer distintos beneficios dependiendo de los perfiles de control de aplicación definidos para cada uno de los grupos solicitados por las autoridades de la UFG; así:

- Decano-Director
- Docentes
- Estudiantes
- Estudiantes de Postgrados

- Administrativos
- Visitas

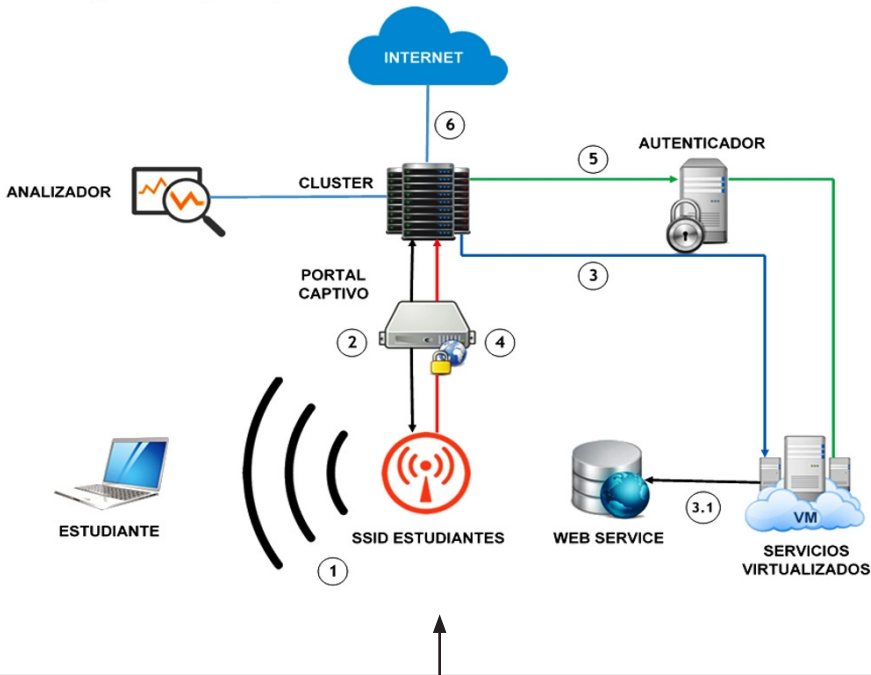
3.4. Autenticación de visitas

Para los visitantes, es decir personas que no poseen credenciales de acceso a los sistemas o servicios en línea de la UFG, se ha definido una dinámica de autenticación, que consiste en crear un usuario temporal que será asociado a la cuenta de un usuario institucional. La Figura 5 es una captura del WebDesktop de un usuario que está autorizado para brindar acceso a visitantes. (Ver Figura 5).

Dentro del escritorio virtual en línea WebDesktop, con el ícono Wifi – Visitas, los usuarios autorizados acceden a la Administración de Usuarios Invitados. En dicho entorno se podrán observar los usuarios que han sido creados anteriormente y se podrá crear un nuevo usuario con una duración temporal. La Figura 6 muestra el panel de administración para usuarios invitados. Al crear un usuario invitado, este podrá

Figura 3

Esquema para la autenticación de la nueva solución inalámbrica.



1. El usuario se conecta a SSID UFG-WiFi con un método abierto de seguridad.
2. La controladora Wireless muestra el portal cautivo de autenticación. La Figura 4 muestra el portal que se despliega a los usuarios.
3. El Clúster (servidor de aplicaciones) recibe los datos que ingresó el usuario (carnet y contraseña).
 - 3.1. El servidor de aplicaciones realiza una consulta al Web Service para validar el estatus del usuario y proporcionar los permisos de navegación si el usuario está activo.
4. El usuario envía las credenciales a la controladora Wireless, las cuales han sido validadas.
5. La controladora recibe las credenciales y son validadas por la plataforma de autenticación.
6. Se permite o no la navegación hacia internet.

Figura 4

Pantalla de autenticación del portal captivo para el acceso a la red



Figura 5

Los usuarios autorizados pueden brindar acceso a internet inalámbrico a los visitantes, para ello tienen en su WebDesktop el ícono llamado Wifi Visitas.



conectarse a la red con SSID UFG-Visitas y tendrá que autenticarse con las credenciales que su “patrocinador” le envíe por correo electrónico. (Ver Figura 6.

Parte complementaria de la implementación de la nueva infraestructura es su difusión dentro de la comunidad universitaria. Por ello, junto con la implementación del proyecto, se lanzó una campaña para informar a los estudiantes sobre el nuevo recurso que estaría a su disposición.

En la Figura 7, se muestra uno de los volantes que se distribuyó de forma física y digital en la comunidad universitaria, para proveer de indicaciones sobre la autenticación y motivar a los estudiantes en el uso de los beneficios que tienen a su disposición. (Ver Figura 7).

4. Resultados obtenidos con la implementación

En la actualidad los usuarios pueden conectarse a la red inalámbrica desde cualquier dispositivo compatible con la tecnología WiFi. La autenticación de usuarios se realiza gracias a la comunicación que se estableció entre las bases de datos de acceso a los sistemas en línea de la Universidad (a través del WebDesktop) y la base de datos del servidor de autenticación que permite utilizar las mismas credenciales de los servicios en línea para conectarse a la red inalámbrica, heredando el perfil, roles del usuario y asignarle permisos en base a estos. La red inalámbrica de la UFG se conecta a internet por medio de un enlace dedicado de 110 Mbps que es independiente del ancho de banda destinado a la red cableada de la institución.

La autenticación de usuarios en la red inalámbrica se realiza por medio de una

controladora centralizada que permite, además de autenticar a los usuarios, monitorear el tráfico y el uso que hacen de la red. Se han definido políticas de bloqueo para sitios no académicos, función que es provista por el *firewall* de la controladora. Además, con el objetivo de brindar mayor seguridad al navegar, únicamente se han habilitado los puertos necesarios para navegar por internet y ejecutar los clientes de correo electrónico más utilizados por nuestros usuarios.

Otro aspecto importante es que la controladora provee un sistema de información dinámico con reportes de consumo de ancho de banda y estadística de los equipos, entre otros. Los equipos inalámbricos cuentan con la función de selección del mejor Access Point adyacente, lo que permite asegurar el buen desempeño del servicio en la red inalámbrica de la UFG. En la controladora se han definido reglas a nivel de *firewall* para que los servicios en línea internos, como por ejemplo el sitio web institucional, el WebDesktop y Sistema Bibliotecario para que puedan ser utilizados sin autenticarse en la red inalámbrica.

Gracias a la implementación de este proyecto hemos podido satisfacer las necesidades de cobertura y la calidad del servicio de red inalámbrica, haciendo posible que la comunidad universitaria cuente con acceso a internet inalámbrico en todo el campus. Como muestra la Figura 8, en el año 2014 se produjo un considerable incremento en la cantidad de puntos de acceso disponibles, y consecuentemente se incrementó en gran manera la cantidad de usuarios simultáneos que pueden acceder al servicio de internet inalámbrico. (Ver Figura 8).

Figura 6

Panel de administración de usuarios invitados y campos que deben llenarse para dar de alta a un usuario invitado.

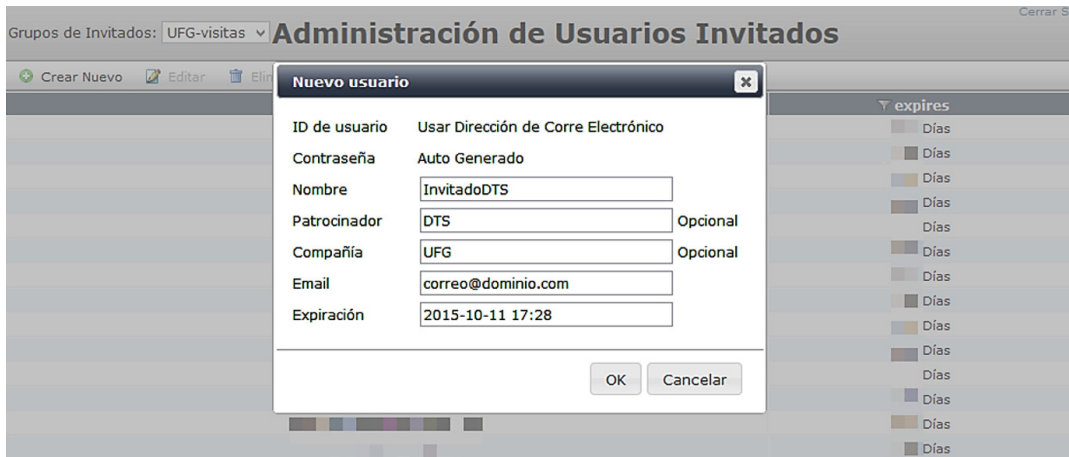


Figura 7

Panel de administración de usuarios invitados y campos que deben llenarse para dar de alta a un usuario invitado.



Sin lugar a dudas, la inversión en infraestructura tecnológica nos ha permitido satisfacer la demanda de conectividad que se requiere para acceder a contenidos actualizados e interactuar en la web en tiempo real desde los salones de clase.

4.1. Monitoreo y estado del servicio

El proyecto implementado incluye un sistema de información dinámico que brinda un conjunto de herramientas de monitoreo que provee información sobre la cantidad de datos transferidos a través de la red inalámbrica, el número usuarios conectados y activos por hora, reportes por SSID respecto al uso del ancho de banda para cada uno y la cantidad de tráfico para cada aplicación.

Junto a las herramientas de monitoreo utilizadas se genera una serie de informes gerenciales con información; por ejemplo, un listado de los usuarios que más sesiones han realizado y el ancho de banda que han demandado, los sistemas operativos y dispositivos más utilizados, los correos electrónicos con mayor tráfico, las categorías de sitios web y los sitios web más visitados. Así mismo, es posible obtener informes sobre los usuarios que han hecho mayor uso del ancho de banda. La Figura 9 muestra un reporte sobre el usuario específico que en un periodo de tiempo determinado ha hecho el mayor consumo del ancho de banda en la red inalámbrica. (Ver Figura 9).

Otros de los reportes disponibles tienen que ver con los usuarios invitados o el perfil de Visitas. Es necesario conocer la cantidad de usuarios invitados creados y por quiénes fueron generados, así como también los Access Point utilizados por estos usuarios y los sitios web visitados.

Parte importante para el buen desempeño de la red inalámbrica es el monitoreo del hardware. Con el Analizador es posible determinar el estado de cada uno de los AP y un registro histórico de los eventos, como por ejemplo cuando alcanzan el límite de usuarios conectados o de paquetes retransmitidos. En este mismo contexto es posible monitorear el uso de CPU de los equipos de red, el uso de memoria, ancho de banda y a la vez obtener un reporte histórico de estos datos. Con el fin de evaluar el rendimiento del equipo, la cantidad de información que puede almacenarse en registros históricos depende únicamente de la capacidad de almacenamiento de la controladora.

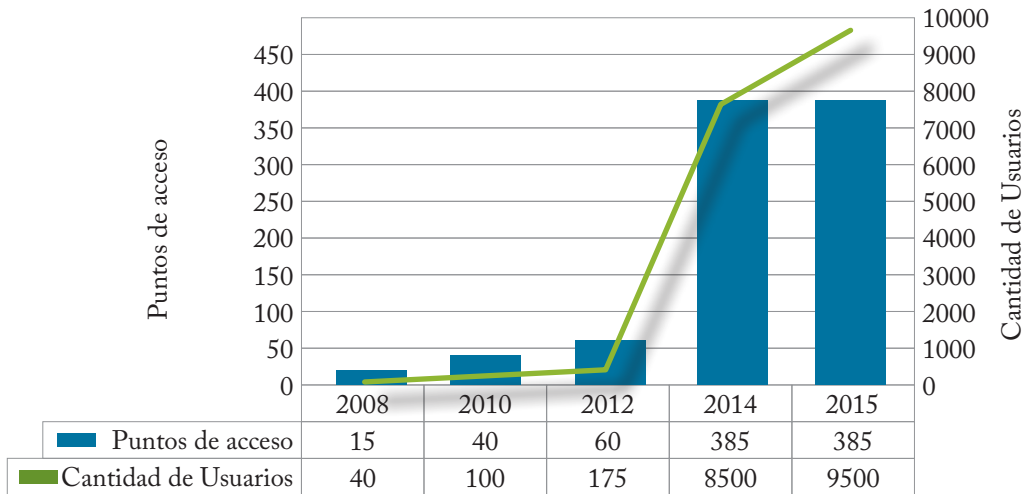
5. Conclusiones

El acceso a internet se ha convertido en una necesidad inherente en la educación; en el pasado podría decirse que abarcaba aquellas ramas afines a las TIC y a la investigación, sin embargo, en la actualidad todas las ramas del conocimiento pueden beneficiarse de este recurso. No obstante, ofrecer un servicio de internet inalámbrico en el ámbito educativo, puede suponer un reto como fue en nuestro caso. Un elemento fundamental para poder ofrecer un servicio que compensara las demandas de la comunidad universitaria, fue cambiar el punto de vista que se tenía sobre la red inalámbrica, dejando de considerarla solo un valor agregado, sino considerarla o valorarla como una parte integral en el desarrollo de nuestras actividades académicas.

El uso de credenciales por los usuarios facilita en gran medida el control que se tiene sobre la actividad que se lleva a cabo con la red inalámbrica, y además es de mucho valor tener la

Figura 8

Evolución de la relación entre puntos de acceso a internet inalámbrico y la cantidad de usuarios conectados simultáneamente por años.



capacidad de integrarlas con las credenciales que los usuarios utilizan para acceder a los servicios y plataformas en línea que posee la institución.

Una de las lecciones aprendidas a lo largo de este proceso fue el hecho de identificar que, aunque exista cobertura de una señal de red inalámbrica y se posea la clave de autenticación, esto no asegura la conectividad a la misma ni mucho menos la calidad del servicio. En el año 2012 teníamos unos equipos que abarcaban una gran área física, pero que, sin embargo, rápidamente eran saturados por la cantidad de usuarios que se conectaban. Además, el incremento de puntos de acceso es una decisión que requiere de un diseño y análisis de las necesidades; de lo contrario se corre el riesgo de tener interferencias entre canales o puntos de acceso en desuso. Al hacer disponible un recurso como el servicio de internet inalámbrico, también es necesario

configurar las políticas de seguridad y restricción de acceso a sitios no académicos, pues se desea que este recurso sea utilizado para propósitos académicos. Contar con herramientas de análisis, monitoreo y reportes tiene un papel muy valioso para conocer el uso que se da a este recurso y poder tomar decisiones basadas en los datos que generan los sistemas de información dinámicos de la red inalámbrica.

Figura 9

Reporte del consumo de ancho de banda y actividad en la red inalámbrica para un usuario específico.



Referencias

Curran, K., y Smyth, E. (2006). Demonstrating the Wired Equivalent Privacy (WEP) Weaknesses Inherent in Wi-Fi Networks. *Information Systems Security*, 15(4), 17–38. Recuperado desde: <http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=22287937&site=ehost-live>.

Hiertz, G. R., Denteneer, D., Stibor, L., Zang, Y., Costa, X. P., y Walke, B. (2010). The IEEE 802.11 universe. *IEEE Communications*

Magazine, 48(1), 62–70. doi: 10.1109/MCOM.2010.5394032.

Ni, Q. (2005). Performance analysis and enhancements for IEEE 802.11e wireless networks. *IEEE Network*, 19(4), 21–27. doi: 10.1109/MNET.2005.1470679.

Sarddar, D., Jana, T., Patra, T., Biswas, U., y Naskar, M. K. (2010). Fast handoff mechanism in WLANs based on neighbor graph information. En 2010 1st International Conference on Parallel, Distributed and

- Grid Computing, PDGC – 2010, 334–338. doi: 10.1109/PDGC.2010.5679972.
- Sou, A. (2014). PROTUR Hotels Chooses Fortinet to Secure Wireless Network. Reuters, U.S. Recuperado desde: <http://www.reuters.com/article/2014/07/21/idUSnMKWN3nQva+1e4+MKW20140721>
- Soni, V., & Mendiratta, R. (2008). Next-generation wlan architecture for high performance networks. IET International Conference on Wireless, Mobile and Multimedia Networks, ICWMMN 2008, 125–129. ISSN 0537-9989.