Artículo producto de la investigación

Red inalámbrica universitaria de área amplia: implementación de una solución de acceso a los servicios de red en áreas geográficamente dispersas

Jorge Eduardo Hincapié Vargas[1]

Resumen

La Universidad Nacional Abierta y a Distancia (UNAD) es la Universidad más grande de Colombia en número de sedes y estudiantes.[2] Cuenta con sesenta sedes en Colombia y las distancias que existen entre ellas pueden llegar a los miles de kilómetros. Este artículo describe cómo la Gerencia de innovación y desarrollo tecnológico de la UNAD preparó e implementó una solución para resolver un problema típico de las organizaciones que tienen sedes en áreas geográficamente dispersas, consistente en el acceso a los servicios de red. La solución diseñada involucra los niveles de acceso, comunicación y gestión y garantiza las características de configuración, seguridad y disponibilidad de elementos de red para todos los usuarios, independientemente de su movilidad por las sedes.

Palabras clave: Redes inalámbricas, computación en la nube, gestión de redes, soporte a usuarios.

1 Gerente de Innovación y Desarrollo Tecnológico, Universidad Nacional Abierta y a Distancia (UNAD). Master in Business Administration. Especialista en Gerencia de proyectos. Ingeniero Telemático. Grupo de investigación GIta. E-mail: jorge.hincapie@unad.edu.co. Colombia.

2 De acuerdo con los datos reportados por el Ministerio de Educación Nacional (MEN) http://www.mineducacion. gov.co/cvn/1665/article-156678.html, http://www.mineducacion.gov.co/observatorio/1722/article-212743.html, http://www.mineducacion.gov.co/sistemasdeinformacion/1735/w3-article-212353.html

A wireless wide area university network: deploying an access solution to network services in geographically scattered areas

Abstract

The National Open and Distance University (Universidad Nacional Abierta y a Distancia, —UNAD—) is the biggest one in Colombia because of its number of venues and students. Its sixty campus are spread over the Colombian territory; in some cases, separated among themselves by thousands of kilometers. This paper describes how UNAD's innovation and technological management office prepared and developed a solution to resolve a typical problem into the geographically separate organizations, namely the access to web services. This solution includes the access and communication levels, and it warrants the features related to the configuration, security and availability of the web elements for all the users, independently of their mobility among its facilities.

Keywords: Wireless network, cloud computing, network management, user support.

Recibido: 1 Diciembre de 2010
Aceptado: 8 Abril de 2011

Introducción

Las organizaciones que se encuentran dispersas geográficamente en áreas amplias, por ejemplo a través de un país o una región, tienden a crear redes inalámbricas (López, 2003; Ocura, 2005) que pueden atender a sus usuarios más próximos o a los de su área de influencia. A estos usuarios se les configuran los servicios habituales de una red móvil entre los que se encuentran el perfil de usuario, la asignación de recursos y las configuraciones técnicas.

El perfil de usuario permite que al conectarse a la red inalámbrica se le asigne una dirección IP y una red de área local virtual (vlan) específica para garantizar que la información del usuario solo sea vista por el grupo de usuarios que tiene su mismo perfil. Con esto se proporciona un nivel de seguridad (Hefferan, 2003)

y de accesibilidad a los recursos a los que el usuario tiene derecho. Ejemplos pertinentes serían: un usuario administrativo tiene derecho al almacenamiento en servidores de la organización pero un visitante no; un usuario corporativo puede acceder a los recursos de la intranet pero un visitante no; un visitante puede ver las páginas del periódico local y esto tal vez no se le permita a un usuario de la organización.

La asignación de recursos y configuraciones técnicas se relaciona con el hecho de que cada usuario que se conecta a la red inalámbrica tiene derecho al uso de ciertos recursos y por tanto, es necesario configurarle algunos parámetros de red. Entre estos recursos y parámetros tenemos: correo, intranet, servidor de almacenamiento, impresoras, servicios de voz sobre el protocolo de internet (voIp), servidores de protocolo dinámico de configuración de host (dhCp), servidores de autenticación, servidores de nombre de domino (dnS), página de inicio, etc.

Problema

Tal vez la forma más común de resolver el problema de acceso a los servicios de red en las organizaciones geográficamente dispersas es creando reservas de direcciones en donde a la dirección de control de acceso al medio (MaC) de cada equipo se le asigna una dirección Ip y a esta se asigna una vlan y a esta vlan o grupos de direcciones se asignan listas de control de acceso (Muller, 2000). Adicionalmente se dan permisos de acceso a los recursos, de acuerdo con el perfil de usuario. Esta es una solución viable en una empresa u organización pequeña donde para implementarla se instalan Puntos de Acceso (ap) y se usa un controlador de dominio o un *router* para hacer las veces de servicio de autenticación.

Si se utiliza la misma solución en una organización con sesenta sedes distribuidas en un país con 60.000 potenciales usuarios, el resultado obtenido es muchas horas-hombre de trabajo, una red casi imposible de controlar, una serie de islas en cada ciudad o sede y una limitada movilidad de los usuarios en las redes inalámbricas.

Adicionalmente, el problema se agudiza en temas como la administración que requiere una alta inversión en hardware para tener un número elevado de controladores de dominios o de servidores de autenticación como wLan (redes inalámbricas locales). El número de ap se multiplica, la variedad de fabricantes y marcas tiende a crecer y la compatibilidad de equipos y su administración se torna más compleja.

Si a estos inconvenientes de administración tecnológica se suman las limitaciones al usuario para tener los recursos de la red en su dispositivo móvil, la organización tendrá una solución pequeña y efectiva para una organización pequeña, pero convertida en un problema grande para una organización grande.

Cubrimiento geográfico de la Universidad Nacional Abierta y a Distancia, UNAD, http://www.unad.edu.co/boletin/comunad/pages/boletin-marzo-1/la_megauniversidad.htm

Desarrollo

En el momento de enfrentar el problema, la UNAD contaba con sesenta sedes y más de cien redes inalámbricas locales. Cada sede tenía una o más redes inalámbricas (Lo &Lin, 1998; Franklin, 2005) instaladas y cada red inalámbrica se conectaba a la red de datos local, permitiendo la salida a Internet de los usuarios. Todas las sedes de la Universidad se encontraban interconectadas a través de una nube formada por una red con enrutamiento MpLS, lo que permitía que las sedes se pudieren ver entre sí y tuvieran salida a Internet.

Adicionalmente, la UNAD contaba con un datacenter conectado a la misma nube, lo que daba la posibilidad de centralizar servicios y pensar en servicios de red inalámbrica administrados y gestionados de una forma centralizada (figura 1).

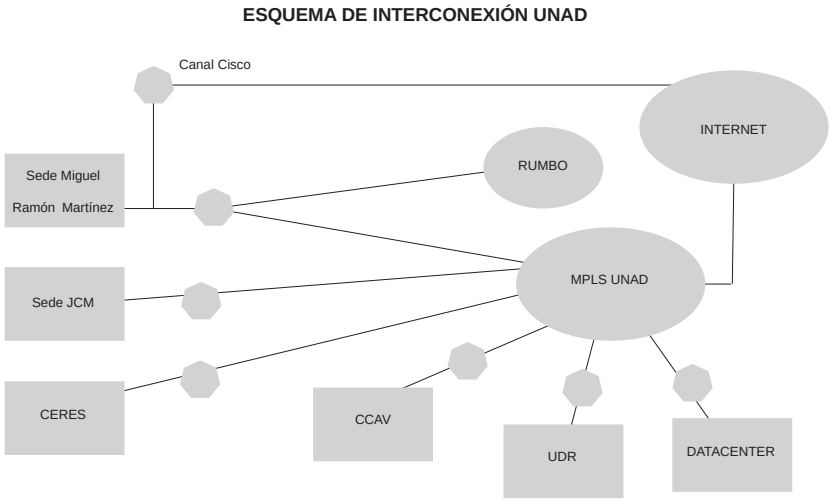

Figura 1. Esquema de interconexión de la UNAD antes de la implementación de la solución wLan

La solución se planteó como respuesta al problema de gestión y administración y se inició obteniendo una tipificación de usuarios y sedes. Esta buscaba obtener datos sobre el número potencial de usuarios, los perfiles que se requerían y los recursos técnicos con los que se contaba.

La tipificación proporcionó los siguientes datos relevantes:

a) La definición de cuatro categorías de perfiles de usuario: visitantes, estudiantes, empleados de planta y grupo de ingeniería. A cada perfil se le asignó una matriz de recursos a los que podía acceder.

b) La validación en campo de la cantidad de vLan a crear y las características de los equipos a implementar. Se encontró que en las sedes había equipos ap que soportaban conexiones bajo diferentes estándares de redes inalámbricas como 802.11a, 802.11b y 802.11g.

c) Los perfiles de las sedes a conectar, definidas en cuatro categorías: sedes principales con canales de datos robustos, servidores y administradores de red locales; sedes intermedias con canal y recursos de servidores; sedes pequeñas con enlaces vía radio y sin recursos de servidores y sedes vía satélite con canales de 512kb.

d) La cantidad de usuarios en cada una de las sedes, cuyo número promedio no es lineal o proporcional con los perfiles de las sedes, dado que una sede intermedia puede tener más usuarios tipo estudiante conectados que una sede principal donde haya más usuarios tipo empleado o funcionario administrativo.

e) El tipo o perfil de los usuarios que más recursos de red consumen. Los usuarios tipo administrativo consumen más frente a los usuarios tipo estudiante, quienes consumen por ráfagas. La proporción entre empleados de planta y estudiantes es de 1 a 20.

f) El tipo de puertos que requiere la solución, los protocolos que se usan y los servicios a los que se accede.

g) El inventario, el *hardware*, los servicios y los enlaces que podrían utilizarse para implementar la solución y las restricciones propias como la ampliación de canales.

Luego de realizada esta tipificación se tuvo la información básica para el planteamiento de la solución, aunque en la búsqueda de ella es frecuente partir de soluciones tecnológicas ya creadas por los fabricantes y, luego, tratar de adaptarlas a los requerimientos de las organizaciones o al tipo de solución que se busca.

Por ello se validaron otras soluciones que tuvieran características similares a las requeridas para la UNAD, visitando sitios web de diferentes universidades del mundo que mostraran la implementación de soluciones inalámbricas. En especial se buscaron en Suramérica y Norteamérica por la afinidad con el tipo de red que se podría llegar a instalar.

Identificado el problema y recolectada la información relevante, se diseñó una solución dividida en tres niveles: a) nivel de acceso, donde estaría todo lo relacionado con los ap, frecuencias de trabajo en cada sitio, ubicación e instalación de equipos en terreno, cableado de los puntos de acceso al *backbone* local; b) nivel de comunicación, donde se ubicaría lo que tiene que ver con los enlaces wan, la conexión a la nube, la definición de vLan a comunicar a nivel nacional, los sistemas de autenticación, la comunicación entre AP, la gestión del tráfico en la nube MpLS; c) nivel de gestión, que con el software necesario ubicado en el datacenter, permita desde cualquier centro a un administrador o desde la sede nacional al responsable de redes, hacer tareas de gestión catalogadas como de rutina, tales como el apagado o encendido de un radio en los ap, cambios de frecuencia, detección de colisiones, configuración de potencia de la señal emitida, enrolamiento de un usuario, entre otras.

Se evaluó el manejo del perfil de usuario y el sistema de autenticación y se planteó integrarlo al Directorio Activo (ad) a través del protocolo de autenticación kerberos para lograr manejar el ciclo completo de ingreso a la red desde los equipos físicos hasta los usuarios.

Finalmente, como parte de la solución, se tomaron en consideración las mejores prácticas definidas por la Biblioteca de Infraestructura de Tecnologías de Información (ItIL) frente a las cuales la gerencia de innovación de la UNAD está alineada, y los referentes de gestión de proyectos del Instituto de gerencia de proyectos (pMI). Así, antes de plantear la solución y una vez identificado y documentado el problema, se dejó definido el alcance de la solución a implementar considerando las restricciones de tiempo y costo.

Descripción de la solución implementada en la Unad

La solución implementada cumple con las siguientes premisas:

a) Una infraestructura de red inalámbrica con cobertura en las sesenta sedes de la UNAD. b) Gestión desde un nivel central de la totalidad de los ap.

c) Un único sistema de autenticación de usuario y contraseña que opere en todo el país.

d) Perfiles de tipos de usuario accesibles desde cualquier red inalámbrica.

e) Facilidad al usuario para acceder a los recursos de red, independientemente del sitio donde se conecte.

f) Baja carga de tráfico de red adicional en las sedes conectadas vía satélite.

Para lograr la cobertura inalámbrica, en cada una de las sedes de la unad se instalaron equipos de red de la siguiente forma:

a) Cincuenta y siete ap con características técnicas que podríamos llamar de tipo 1, que permiten a los usuarios conectarse a la red y reenviar el tráfico hasta la controladora y los servidores de autenticación. Estos equipos con características que se pueden denominar básicas, aunque robustos para manejar un gran número de usuarios, fueron instalados en las sedes donde la anchura de banda de los canales a la nube MpLS de la UNAD no representaba un problema si se le agregaba tráfico.

b) Cuarenta y siete ap con características técnicas que denominaríamos de tipo 2, que realizan *switching* local para evitar que cuando el tráfico de datos se realiza con servidores o aplicaciones que se encuentran publicadas dentro de las mismas sedes, este flujo de información llegue hasta el data center ubicado en Bogotá. Estos equipos se destinaron a las sedes principales donde el nivel de usuarios, y por lo tanto, el volumen del tráfico de datos es mayor, en comparación con las sedes regionales.

En la anterior distribución de ap los criterios de selección fueron la anchura del canal de conexión a la nube MpLS y el costo del ap. En este caso, los criterios obedecieron a la cantidad de aplicaciones en servidores locales que serían consultados por la red inalámbrica.

c) Dos controladoras que realizan la gestión de la red inalámbrica desde el data center, conectando estos dos equipos en *cluster* para tener redundancia. Las controladoras tienen características de equipos de alta disponibilidad y se conectaron por cuatro puertos diferentes a la red principal, buscando con todos estos mecanismos garantizar una alta disponibilidad de la solución central.

d) Siete ap con características técnicas de tipo 3, incluyendo características de equipos controladores que permiten autenticación y control de los AP que se conecten a ellas. Esta solución con características menores que las controladoras ubicadas en el *data center* pero que ofrecen mayores beneficios que un AP básico, fueron destinadas para las sedes con conectividad satelital donde la anchura de banda es un elemento crítico.

e) La distribución de la totalidad de los equipos tipo 1 y 2 se realizó de tal forma que se cumpliera con los criterios mencionados con anterioridad, dándose el caso de sedes con los dos tipos de equipos instalados.

La arquitectura quedó basada en tres componentes principales: ap, controladoras inalámbricas o wireless, switch y plataforma de administración centralizada con *software* para la gestión de la red inalámbrica. Los ap ofrecen la conectividad bajo los estándares 802.11a, 802.11b y 802.11g y con encriptación a través de wpa2, definido a nivel de las controladoras.

Las controladoras publican los identificadores de servicios (SSId) de las redes que a su vez publican los ap, y los SSId coinciden con los perfiles de usuario.

Los perfiles quedan definidos en las controladoras y cuando un usuario se conecta a un SSId, realmente está desde ese momento definiendo con qué perfil entra a la red. La autenticación se realiza contra los servidores RadIuS ubicados en el *data center*, los cuales a su vez, usan las bases de datos de usuarios de la unad para conceder los respectivos permisos.

Los ap no guardan ningún tipo de configuración ni imagen; solo tienen configurada la dirección Ip, las direcciones Ip de las controladoras y el *gateway* de la sede donde quedaron instalados. La configuración de la red como tal, la adquieren de las controladoras una vez las encuentran en la red y se conectan a ella. La solución establece un esquema de alta disponibilidad en el que los ap dependen de dos controladoras (primaria y secundaria), de tal manera que en caso de falla de la controladora primaria, los ap seguirán conectados a la secundaria para ofrecer el servicio de acceso inalámbrico; adicionalmente, las controladoras tienen fuente de potencia redundante y doble conexión a la red alambrada.
Para la gestión de la red se instaló una aplicación comprada al fabricante de los controladores y que corre sobre una plataforma con sistema operativo Microsoft. Esta aplicación permite aprovisionamiento, configuración, cambio de parámetros, monitoreo de ap y de usuarios, niveles de señal y generación de reportes de manera centralizada. Este *software* de gestión quedó habilitado para manejar hasta 10 controladoras inalámbricas, permitiendo así un crecimiento futuro de la red y, en un modelo de gestión posterior, descentralizar algunas funciones para administradores locales.

Los ap de la red inalámbrica gestionada por medio de controladoras inalámbricas se tipificaron de dos formas: conectados directamente a la controladora o distribuidos. En el primer caso, los ap se conectan a la controladora a través de otros equipos de red como s*witches* y *routers* usando alimentación con red regulada y adaptadores o con inyectores de poE (Adaptadores para suministrar energía con el cable de la red de datos) [9]. En el caso de la solución implementada en la unad, se instalaron ap distribuidos, ya que estos no están conectados directamente a una controladora. Por tratarse de una red donde existe *firewall* y se manejan parámetros de seguridad a nivel de aplicaciones y puertos (Huston,2001), fue necesario generar un piloto que al monitorear la red, identificara todos los puertos involucrados en las diferentes transacciones de red y simulara la operación desde el aprovisionamiento

de un usuario hasta la conexión e intercambio de información entre dos usuarios conectados a la red inalámbrica en dos sedes diferentes. Con la información del piloto se establecieron políticas de seguridad que permiten el flujo de información a través de los puertos requeridos sin abrir brechas de seguridad en la red.

Para realizar la autenticación (Brykczynski and Small, 2003), (Higby and Baile, 2004) de los usuarios cuando necesiten ingresar por medio de la red inalámbrica, se implementó un sistema aaa RadIuS de Microsoft mediante el servicio npS (de los servidores Windows 2008), usando la base de datos de directorio activo.

Conclusiones

Basados en una problemática común para las organizaciones que se encuentran dispersas geográficamente y según el análisis de las soluciones comúnmente implementadas, la Gerencia de innovación y desarrollo tecnológico de la unad planteó una solución que involucraba los elementos tradicionales organizados, de tal forma que se aprovecha la infraestructura de red existente y no se incurre en los problemas de típicas instalaciones descentralizadas. A la implementación de esta solución se le sumó la aplicación de metodología como la establecida por el pMI y las buenas prácticas sugeridas por ItIL, logrando así la construcción de una red inalámbrica exitosa.

Tabla 1. Situación antes y después de aplicar esquema de red inalámbrico

Situación antes de aplicar el nuevo esquema de red inalámbrico	Situación después de aplicar el nuevo esquema de red inalámbrico
Variedad de ap en marcas, velocidades y configuraciones de alta complejidad en la gestión y administración.	Homogeneidad en configuraciones, control de las velocidades en los ap, facilidad en la administración y gestión.
Seguridad distribuida y difícil de controlar, variedad de vLan, sin control de tráfico y acceso.	Seguridad centralizada, vLan separadas, control de acceso y de tráfico.
No se detectan ap fuera de servicio en ciudades distantes y se requiere desplazamiento de técnicos a sitio para ajustar configuraciones.	Detección de ap fuera de servicio, detección de ap no autorizado y posibilidad de configuraciones remotas.
Inventarios, actualización de equipos, soporte y garantía con alto grado de complejidad y gestión administrativa.	Inventarios, actualización de equipos, soporte y garantía con baja complejidad.

Referencias bibliográficas

Brykczynski, B. and Small, S. (2003). Reducing Internet-Based Intrusions: Effective Security Patch Management. *IEEE Software*, 20(1), 50-52.

Franklin, T. (2005). *Wireless Local Area Networks in Education* [en línea].York: TeachLearn. Disponible en: http://www.techlearn.ac.uk [2011, 30 de junio].

Gutiérrez, J., Naeve, M., Callaway, E., Bourgeois, M., Mitter, V. and Heile, B. (2001). 802.15.4: A developing standard for low-power low-cost wireless personal area networks. *Network*, 15(5), 12-19.

Hefferan, R. (2003). *Information Security Management*, [en línea]. Institute of Scientific & Technical Communicators. Disponible en: http://www.istc.org.uk/map.htm [2011, 7 de abril].

Higby, Ch. and Baile, M. (2004). *Wireless security patch management system*, [en línea]. Utah: Brigham Young University. Disponible en: http://0-delivery.acm.org.millenium.itesm.mx/10.1145/1030000/1029575/p165-higby.pdf?ip=200.34.202.242&CFID=29882587CFTOKEN=82364802& [2011, 30 de junio].acm=1308641782_c0be4083d9efc59ac763c02f775000db

Himmelsbach, V. (2005). Wireless LANs. *Computer Dealer News*, 13(15), 7.

Huston, G. (2001). TCP in a wireless world. *Internet Computing*, 5(2), 82-84.

López, A. (2003). *Evaluating organization and connectivity in ad-hoc wireless networks.*

Lo, Ch. and Lin M. (1998, febrero). QoS Provisioning in Handoff Algorithms for Wireless LAN, Broadband Communications. Actas del Seminario Internacional de Zurich, Suiza.

Monterrey: Instituto Tecnológico y de Estudios Superiores de Monterrey.

Muller, N. (2000).Wireless Data Networking. Boston. MA: Artech House Publishers.

Ocura, E. (2005). *Clusterización en redes Ad Hoc de gran escala.* Trabajo de grado, Maestría en Ciencias en Ingeniería Electrónica con especialidad en Telecomunicaciones, Instituto Tecnológico y de Estudios Superiores, Monterrey.