UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SOLUCIÓN DE ACCESO SEGURO BASADO EN CONTEXTO PARA USUARIOS DE RED DE LA UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

LENIN VERAMENDI SALAZAR

PROMOCIÓN

2009- I

LIMA – PERÚ

2013

SOLUCIÓN DE ACCESO SEGURO BASADO EN CONTEXTO PARA USUARIOS DE RED DE LA UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

Agradezco a mi madre y a mi padre por brindarme su amor, por haberme formado con valores desde niño y darme fuerza para afrontar los retos de la vida

SUMARIO

Este informe busca dar solución a los problemas de conectividad de usuarios de red y también a los problemas de gestión que afronta el departamento de TI de la Universidad Peruana de Ciencias Aplicadas, UPC. Como primer punto se revisará a detalle la problemática que se está viviendo actualmente, aquí detallaremos las principales preocupaciones tanto de los usuarios como de los administradores de red, además revisaremos el estado actual de la red de la UPC para poder entender a fondo las razones de los problemas. Una vez entendida la problemática, se pasará a analizar las posibles soluciones para poder elegir la solución más adecuada tanto en la parte técnica como económica, con esto plantearemos un diseño de red para la UPC y finalmente una propuesta económica.

Si bien este trabajo está centrado en el caso particular de una universidad, también podría servir como guía base para aplicarse a otras instituciones del sector educativo universitario.

ÍNDICE

INTRODUCCIÓN

En la actualidad las redes de comunicaciones IP forman cada vez más una muy importante parte en la vida de las personas, no sólo en sus aspectos personales sino también en aspectos formativos de educación. Es así que dichos medios juegan un papel sustancial en la educación superior, en la preparación de mejores profesionales y la creación de nuevos entornos de aprendizaje, entre otras cosas. Teniendo esto en mente, surge la necesidad de contar con una red IP preparada para entregar una calidad de experiencia óptima en entornos de educación superior tanto a estudiantes, docentes y trabajadores administrativos.

Si revisamos las tendencias tecnológicas actuales, podemos citar dos con fuerte presencia en los entornos educativos y que guían la evolución de las redes IP. La primera tendencia tecnológica es el video como medio de comunicación que cada vez se va haciendo más masivo, esto debido en gran parte al uso doméstico tipo youtube donde encontramos gran cantidad de contenido de video y otra gran parte debido al uso de video en entornos empresariales en formato de videoconferencia y telepresencia donde gracias al uso de video en alta definición podemos llegar a enriquecer la experiencia a tal punto de lograr una sensación de tener una reunión en una sala cuando en verdad las personas están distanciadas miles de kilómetros geográficamente. La segunda tendencia tecnológica es la movilidad, esto debido a la aparición de gran cantidad y variedad de dispositivos inalámbricos tipo laptops, tabletas y teléfonos celulares inteligentes los cuales pueden tener distintos sistemas operativos y de fábrica no cuentan con un puerto para cable de red sino que nacen para ser inalámbricos y así seguirán conectándose a la red, esto significa para los usuarios una flexibilidad nunca antes vista ya que no están atados a un cable ni a un espacio físico determinado sino que se pueden mover con total libertad sin perder la conexión a la red.

La adopción de estas tendencias dentro de los entornos educativos presenta nuevos retos para el departamento de TI ya que el uso de múltiples dispositivos y en su mayoría personales de estudiantes y docentes puede significar un hueco de seguridad por donde se filtre información por ello es primordial conocer quién se conecta a la red, en qué momento y mediante qué acceso (cableado inalámbrico o VPN) y de acuerdo a ello definir las políticas de acceso a información. El presente informe muestra cómo preparar las redes IP para que trabajen bajo un entorno seguro de acceso a información sin

comprometer la velocidad de comunicación y así la red esté lista para implementar las tendencias tecnológicas previamente descritas con el objetivo de mejorar el proceso de enseñanza en los entornos universitarios mediante el uso de la tecnología como facilitador de la información.

Es justamente con esta visión que la Universidad Peruana de Ciencias Aplicadas, UPC, una de las principales instituciones educativas superiores en el Perú manifiesta su preocupación por brindar un servicio de conectividad de alta velocidad a sus alumnos, profesores y empleados sin comprometer la seguridad y otorgando al usuario final la libertad de elegir el medio por el cual se conecta, sea cableado o inalámbrico, de elegir el dispositivo que prefieran y bajo una única política de seguridad aplicada de manera automática por la red IP. En resumen buscan una solución tecnológica para un entorno educativo superior que les permita brindar mejores servicios de conectividad a los usuarios finales y así usar la tecnología como un facilitador del proceso de enseñanza.

Dentro de las limitaciones que se tienen, podemos decir que no se cuenta con un laboratorio para probar esta solución por lo que se debe estar bien seguro de las funcionalidades a implementar y hacer las validaciones respectivas de la integración entre las plataformas consultando a los fabricantes.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1 Descripción del problema

El departamento de TI de la UPC se encarga de dar conectividad hacia internet y dentro de la universidad a profesores, estudiantes y trabajadores administrativos.

Actualmente la universidad tiene dos redes paralelas, una red llamada la red académica y otra llamada la red administrativa. Los estudiantes y profesores se conectan a la red académica y los trabajadores se conectan a la red administrativa. Ambas redes tienen switches y puntos de acceso inalámbricos desplegados a lo largo de todo el campus universitario de forma replicada, sin embargo hay zonas donde solo hay cobertura inalámbrica de una u otra red, o académica o administrativa. Todo el control que tiene el departamento de TI es sobre los equipos conectados a la red cableada que han configurado ellos mismos para el uso de los estudiantes, profesores y personal administrativo. Durante los tres últimos años se ha visto un crecimiento exponencial del uso de la red inalámbrica por parte de los estudiantes y profesores. Este crecimiento se debe al uso de dispositivos personales de los estudiantes y profesores; dispositivos tipo tabletas y teléfonos inteligentes son cada vez más comunes en la universidad y estos dispositivos solo usan la red inalámbrica para tener conectividad.

El estado actual de la red antes descrita presenta algunos aspectos negativos los cuales se indican a continuación:

- Para el departamento de TI es difícil tener control y visibilidad de los usuarios que acceden con múltiples dispositivos a la red inalámbrica.
- Al no poder controlar qué dispositivos se conectan a la red se optó por tener una red inalámbrica abierta y sin seguridad para toda persona que tenga un dispositivo dentro de la cobertura inalámbrica que inclusive puede ser de fuera de la universidad y así asegurar conectividad a cualquier estudiante sin embargo esto ocasiona que la red se sature por el acceso de personas indebidas e incluso se han llegado a detectar ataques a los servidores provenientes de dispositivos inalámbricos.
- Los usuarios perciben una navegación lenta cuando usan la red inalámbrica y algunos han optado por utilizar modem 3G. Esto genera malestar dentro de la comunidad estudiantil ya que significa un costo adicional que el estudiante debe cubrir por su cuenta.

- Los alumnos al tener una mala experiencia de navegación no pueden acceder de manera óptima al contenido de video que cada vez se hace más común entre los estudiantes y profesores ya que el material de enseñanza y de investigación muchas veces se encuentra en este formato ya sea a nivel de red local o a través de internet o incluso vía videoconferencias usando internet.
- Los profesores al tener una mala experiencia de navegación bajan su productividad ya que al momento de acceder a los servidores locales e internet a través de una conexión inalámbrica el rendimiento es pobre.
- No se tiene control de la información corporativa a la que acceden los estudiantes, docentes y trabajadores administrativos desde dispositivos personales dentro de la red inalámbrica de la universidad.
- Para el departamento de TI es difícil dar acceso de invitado a un proveedor o cualquier otra persona ajena a la universidad que los visita y necesita conectarse a la red ya que no cuenta con una mesa de ayuda ni con los recursos suficientes como para generar los accesos temporales para cada invitado.

En base a la problemática descrita anteriormente, enunciamos el siguiente problema, el cual debe ser resuelto a fin de cumplir con los objetivos estratégicos de la organización.

1.2 Formulación del problema

El departamento de TI de la UPC no tiene visibilidad de los usuarios ni los dispositivos que acceden a la red inalámbrica ni tiene control de la información a la que acceden, lo que ocasiona un hueco de seguridad y una mala experiencia de navegación para los usuarios.

1.3 Objetivos del trabajo

El objetivo de este trabajo es mejorar el entorno de aprendizaje y trabajo en la Universidad Peruana de Ciencias Aplicadas mediante el uso de herramientas tecnológicas que permitan tener control de las personas que acceden a la red para poder asignarles accesos adecuados a los recursos de información y realicen sus labores de manera eficiente.

Se busca mejorar la seguridad mediante el control de acceso de los estudiantes, docentes, trabajadores administrativos e invitados que se conectan a la red de la UPC ya sea que se conecten a través de red cableada o inalámbrica, en cualquier momento y lugar bajo una sola política establecida por el departamento de TI, el cual tenga visibilidad y control de los usuarios que se conectan y mediante qué dispositivo lo hacen.

Si bien este trabajo está centrado en un caso particular de una universidad, la solución puede servir como línea base para aplicarse a otros entornos del sector educativo universitario.

1.4 Evaluación del problema

Podemos dividir en tres partes el problema que se presenta en la UPC.

1.4.1 Red inalámbrica lenta

Los problemas con la conexión inalámbrica ocasionan mucho malestar en la comunidad universitaria y en especial en los estudiantes. Se realizó una encuesta corta a alumnos y trabajadores de la universidad en el campus de Monterrico y se obtuvieron los siguientes resultados:

- "A mi oficina casi no llega la señal wifi"
- "A mi oficina no llega el wifi. Red demasiado lenta por saturación de alumnos."
- "A veces falla el internet y la conexión WIFI es muy mala."
- "En muchas ocasiones me quedo sin internet y no puedo realizar mis tareas de los cursos."
- "En ocasiones lento y no hay buena cobertura de Wifi"
- "Falla la conexión a Internet"
- "Hay zonas donde la señal no llega y si debería funcionar bien (Pabellón L)"
- "No funciona el wifi en toda la universidad"
- "Está pésimo el servicio, es lento"

Esta limitación en la red dificulta la adopción de nuevas formas de enseñanza en la universidad tipo clases virtuales donde se usa mucho el video en vivo y/o en demanda ya que el video consume mucho ancho de banda. Más aun sería difícil poder hablar de clases con video en alta definición.

1.4.2 Falta de una política de seguridad para el acceso a la red

El control de acceso a información es un problema muy delicado ya que se puede llegar hasta tener robo de información lo cual ocasionaría un gran problema para la institución, desde malograr su imagen y credibilidad hasta poner en duda la seriedad de la calidad de su enseñanza. Pero el control de acceso a información empieza desde el acceso a la red y los permisos que se conceden al usuario que ingresa a la red, por ello es muy importante tener control de las personas que se conectan a la red y mediante qué dispositivo se conectan, en que momento y lugar intentan acceder y a través de qué tipo de conexión, red cableada, inalámbrica o acceso remoto, quieren acceder a los recursos de información. Estos parámetros, el quién, qué, dónde, cuándo y cómo definen lo que se conoce como el contexto de acceso a la red y es basado en este contexto que se debe plantear una solución para el control de acceso a información.

1.4.3 Falta de una plataforma de gestión de red

La gestión de red es el paraguas que cubre tanto la seguridad como el correcto desempeño de la red, sin una gestión que cubra la seguridad y el desempeño de la red es

como tener un gran submarino de última generación sin sonar que anda por el mar y puede ser hundido por cualquier ataque. Actualmente se cuenta con software poco especializado en cuanto a monitoreo de equipos de red y no se llegaría a tener integración con los equipos de seguridad. Además se tienen software de gestión distintos para red cableada y para red inalámbrica lo cual significa tener islas separadas mientras lo que se necesita es tener una sola red bajo una sola política de seguridad y de gestión.

1.5 Limitaciones del trabajo

La implementación de la solución que se plantee frente a la problemática estudiada dependerá solo de la universidad. No es posible modificar la configuración de los equipos en la red de la UPC para hacer pruebas piloto. Todo cambio va por responsabilidad del departamento de TI de la universidad en horarios que vean convenientes.

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1 Antecedentes del problema

En esta sección revisaremos la topología de la red LAN de la universidad para entender cómo los paquetes de información se transportan en la red. Además se revisará el tipo de despliegue y las capacidades de los puntos de acceso inalámbrico y el controlador. Para terminar veremos las políticas de control de acceso existentes de acuerdo a los tipos de usuario y contexto y la gestión de los equipos de red.

2.2.1 Estado Actual de la Red LAN

Actualmente la UPC divide el equipamiento de red existente en dos redes independientes que se interconectan en el core de ambas redes, dichas redes llevan por nombre red académica y red administrativa. La red académica es la red a la que se conectan estudiantes y docentes para acceder a internet y a los recursos internos de educación mientras que la red administrativa es la red a la que se conectan los trabajadores administrativos de la universidad para acceder a internet y a las aplicaciones de uso interno. La figura 2.1 muestra el despliegue actual de ambas redes.

Los problemas identificados son:

- Esta situación de tener dos redes paralelas, académica y administrativa, ocasiona problemas graves para la universidad ya que cuando se presentan problemas de red es muy difícil identificar donde se generaron debido a los posibles bucles que se podrían ocasionar, también se tiene duplicidad en la gestión de equipos y una seguridad de acceso muy difícil de definir.
- Los switches presentan VLAN duplicadas en ambas redes, se hace uso de la VLAN 1 como VLAN nativa y como VLAN de datos e incluso llega hasta los principales servidores de aplicaciones de la universidad lo cual representa una mala práctica y un hueco de seguridad para posibles ataques tipo VLAN hopping y/o switch spoofing.
- La VLAN 1 es usada por los servidores de la universidad lo cual aumenta el riesgo de que sean atacados por las razones mencionadas en el ítem anterior.
- La red LAN no cuenta con una política de priorización de tráfico o calidad de servicio QoS implementada ni para la voz ni para aplicaciones críticas lo cual podría mejorarse tan solo haciendo configuración de los equipos.

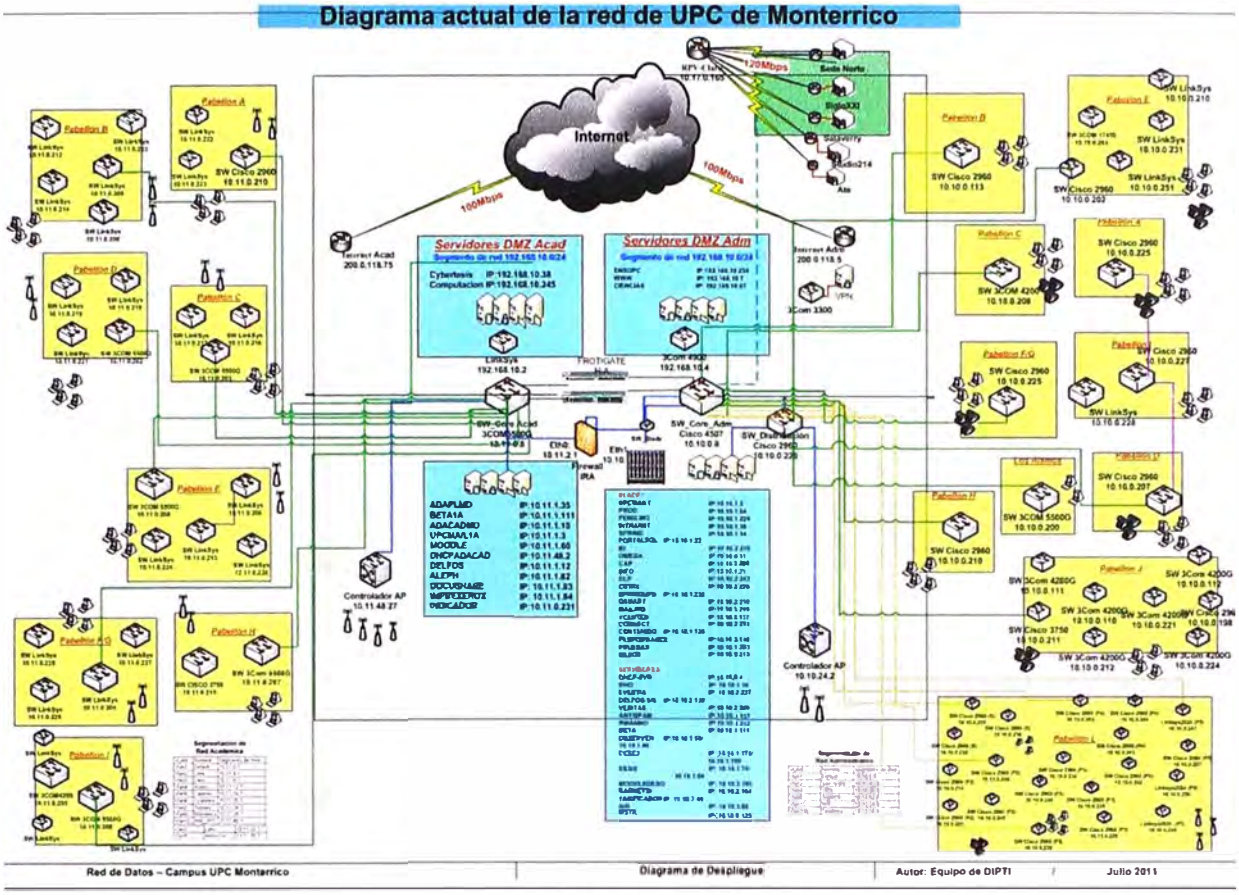


Fig. 2.1 Diagrama de la UPC, red académica en la derecha y red administrativa en la izquierda

Ambas redes cuentan con un diseño de red LAN jerárquico de 3 capas, es decir cuentan con una capa de core, otra de distribución y otra de acceso. En ambos casos cuentan con switches que en su mayoría son de la marca Cisco aunque también existen equipos antiguos de la marca 3com y otros más pequeños para oficinas pequeñas y laboratorios que son de la marca Linksys.

2.1.1.a) Capa de Core

Para la red académica se tiene como equipo de core un switch fixed de marca 3com, modelo 5500 que cuenta con 48 puertos Ethernet 10/100 Mbps y 4 puertos Ethernet 1Gbps con capacidades para hacer enrutamiento de paquetes en capa 3.

Los problemas identificados son:

- Cabe resaltar que este equipo usado como switch core de la red ya no cuenta con servicio de soporte y que actualmente la empresa 3com fue adquirida por Hewlett-Packard y ya no mantiene en venta ni soporte este equipo.
- Es un switch muy básico para ser el core de una red.

Para la red administrativa se tiene como equipo de core un switch modular de marca Cisco, modelo Catalyst 4507R+E, con modulo módulo supervisor de última generación y en redundancia que entrega 48Gbps de ancho de banda a cada uno de sus slot donde van módulos de puertos. En cuanto a los módulos de puertos vemos que se cuenta con 2

módulos de 48 puertos en cobre a 10/100/1000 Gbps y 2 módulos de 12 puertos de fibra a 1Gbps. Este switch tiene capacidades de enrutamiento en capa 3, realizar QoS avanzado y alta disponibilidad. En la figura 2.2 se puede ver una imagen de este switch de core.

Los problemas identificados son:

- Si bien el equipo de core presente en la red administrativa es un equipo bastante avanzado y con grandes prestaciones, solo existe uno y no tiene redundancia. Esto representa un punto de falla muy grave para la red ya que según las mejores prácticas y reglas de diseño se debe contar con un core en redundancia para asegurar la alta disponibilidad de la red y no tener cortes en el servicio de conectividad.
- Los módulos de 48 puertos este switch ofrecen una sobresuscripción de 2:1 mientras que el backplane podría ofrecer una sobresuscripción de 1:1.
- No se tiene configurado calidad de servicio ni seguridad.
- El switch cuenta con una versión de sistema operativo antigua.

Ambos switches de core se encuentran ubicados en el centro de datos de la universidad ubicado en el segundo piso del pabellón L, en el área de sistemas. Desde el centro de datos se tiene tendida fibra óptica multimodo y en redundancia hacia todos los edificios del campus universitario donde se conectan los switches de distribución.

Fig. 2.2 Cisco Catalyst 4500, es el switch core de la UPC

2.1.1.b) Capa de Distribución

Tanto para la red académica como para la red administrativa se cuentan con switches fixed de la marca Cisco, modelo Catalyst 3560G y 3560-X. Estos switches cuentan con capacidades de enrutamiento en capa 3, seguridad tipo listas de control de acceso y QoS básico para manejar VoIP entre otras aplicaciones. Los switches de distribución se conectan al core mediante interfaces de fibra óptica en velocidad de 1Gbps Ethernet y permiten agregar el tráfico de los switches de acceso hacia la capa de core.

Los problemas identificados son:

o Solo se tienen configurado capacidades básicas del switch como VLAN y telnet, lo cual significa una subutilización del equipo presente.

o No se tiene configurado calidad de servicio ni seguridad.

o La mayoría de los switches cuentan con una versión antigua de sistema operativo.

2.1.1.c) Capa de Acceso

Tanto para la red académica como para la red administrativa se cuentan con switches fixed de la marca Cisco, modelo Catalyst 2960G y 2960-S y otros de menos puertos y prestaciones de marca linksys.

A los switches de acceso van conectados los dispositivos finales como PCs, laptop, teléfonos IP y puntos de acceso inalámbricos. Los switches de acceso están distribuidos a lo largo del campus en los cuartos de telecomunicaciones de los distintos pabellones.

Los problemas identificados son:

o Se tienen switches con distinto sistema operativo y distinto licenciamiento lo cual complica una configuración coherente de los equipos y por tanto las prestaciones que ofrece la red.

o Existen switches no administrables que sólo brindan conectividad mas no capacidades avanzadas en el acceso.

o No se tiene configurado calidad de servicio.

o La mayoría de los switches cuenta con una versión de sistema operativo antigua.

2.1.2 Estado Actual de la Red Inalámbrica

En la red inalámbrica encontramos dos componentes a analizar: los puntos de acceso inalámbricos que están distribuidos a lo largo del campus y el controlador inalámbrico que se encarga de la configuración, gestión y manejo de radio frecuencia de los puntos de acceso.

2.1.2.a) Puntos de Acceso Inalámbricos

Los puntos de acceso inalámbricos desplegados a lo largo del campus universitario son todos de la marca Cisco, principalmente los modelos 1141, 1131 y recientemente los 3500 en su totalidad son 81 puntos de acceso. Estos puntos de acceso trabajan en modo "Lightweight Access Points" (Punto de Acceso Ligero) lo que significa que la gestión de los puntos de acceso, configuración, operación de RF, seguridad, calidad de servicio y demás políticas están centralizadas en un controlador al cual se conectan los puntos de acceso a través de la red de switches. La comunicación entre el controlador y los puntos de acceso se realiza mediante el protocolo LWAPP (protocolo propietario Cisco) y CAPWAP (RFC 4118), el primero se usa para los AP 1131 y el segundo para los AP 1141 y 3500.

Los problemas identificados son:

o Se ha observado que el despliegue de los puntos de acceso 1131 en su mayoría se ha realizado en forma errónea ya que la gran mayoría se encuentran orientados en forma vertical como se puede observar en las figuras 2.3 y 2.4.

Fig. 2.3 Puntos de Acceso desplegados en la UPC

Fig. 2.4 Puntos de Acceso desplegados en forma vertical

Esta orientación no es la más adecuada para los puntos de acceso inalámbricos ya que el patrón de radiación de la antena irradia en forma de dona teniendo como centro al punto de acceso inalámbrico en forma horizontal. Por lo tanto la orientación actual ocasiona que no se cubra en forma óptima el espacio del campus universitario.

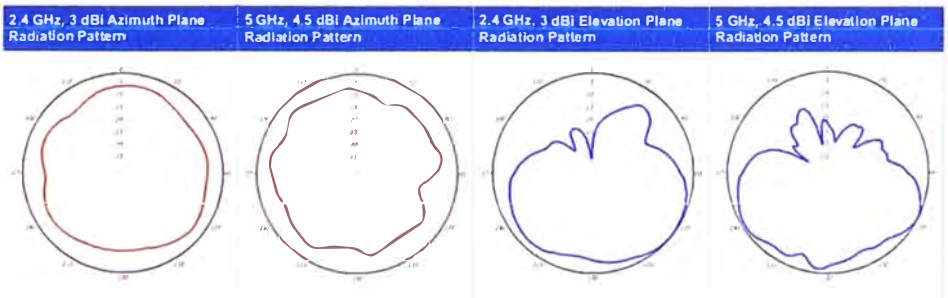


Fig. 2.5 Patrón de radiación de las antenas en los puntos de acceso

o Algunos puntos de acceso inalámbrico con elementos de antena externos cuentan solo con elementos de antena en la banda de 2.4 GHz y no con elementos de antena de 5GHz lo cual significa que los clientes que soportan 2.4GHz y 5GHz no podrán asociarse en la frecuencia de 5GHz y serán obligados a usar la banda de 2.4GHz la cual es muy

frecuente encontrar saturada por dispositivos antiguos que sólo trabajan en esta banda y se tendrá como resultado un canal de comunicaciones saturado y lento.

Fig. 2.6 Punto de acceso sin y con elementos de antena

- La velocidad que manejan los puntos de acceso inalámbricos presentes en la universidad trabajan bajo los estándares IEEE 802.11a/b/g con lo cual pueden llegar a velocidades máximas teóricas de 54Mbps y soportar a lo más 15 usuarios por punto de acceso. Teniendo en cuenta que actualmente la universidad cuenta con 5000 usuarios de red y 81 puntos acceso estaríamos hablando de aproximadamente 61 usurarios por puntos de acceso, lo cual se traduce en una saturación de las capacidades de los puntos de acceso inalámbrico.
- Debido a la gran cantidad de dispositivos que usan el aire para comunicarse y que son ajenos a la comunicación wifi, tipo hornos microondas de los cafetines, teléfonos fijos inalámbricos, cámaras de videovigilancia inalámbricos, etc., se obtiene un canal de comunicación inalámbrico muy cargado con interferencias lo cual hace que las comunicaciones tipo wifi vean comprometidas sus velocidades de transmisión.
- No se tiene una solución inalámbrica de radiofrecuencia que se adapte acorde a la demanda de los usuarios inalámbricos. Por ejemplo los puntos de acceso cercanos a los auditorios deberían orientar su cobertura hacia el auditorio cuando hayan conferencias o gran cantidad de usuarios inalámbricos y cuando no hayan usuarios ayudar a cubrir zonas fuera del auditorio.
- El tener una diversidad de modelos de puntos de acceso hace que los patrones de radiación sean distintos y por tanto la integración y el entendimiento entre puntos de acceso sea limitado.

2.1.2.b) El Controlador Inalámbrico

La universidad cuenta con dos controladores de redes inalámbricas. Un controlador de marca Cisco, modelo Wireless LAN Controller 5508 para la red académica el cual va conectado directamente al switch 3com del core académico y tiene puntos de acceso desplegados a lo largo del campus universitario. Y otro controlador de marca Cisco, modelo Wireless LAN Controller 2106 para la red administrativa el cual va conectado directamente al switch Cisco del core administrativo y tiene puntos de acceso desplegados en los edificios donde se encuentran las oficina administrativas.

El controlador Cisco 5508 cuenta con 8 interfaces de 1 Gigabit Ethernet cada una, actualmente solo tiene conectadas cuatro interfaces hacia el switch de Core de la red académica como se puede ver en la figura 2.7, estas cuatro interfaces están conectadas en modo agregación de puertos para dar balanceo de carga y redundancia, en caso de que falle una de las cuatro interfaces conectadas el trafico seguirá siendo enviado por las restantes interfaces activas.

Fig. 2.7 WLC Cisco 5508 con cuatro interfaces conectadas al core académico

El controlador Cisco 2106 cuenta con 8 interfaces de 10/100 Ethernet cada una, actualmente solo tiene conectadas una interface hacia el switch de Core de la red administrativa como se puede ver en la figura 2.8, en este controlador no se puede configurar agregación de puertos.

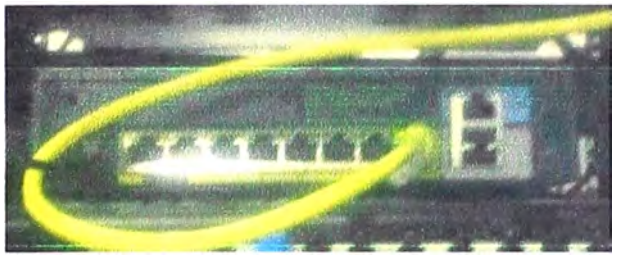


Fig. 2.8 WLC Cisco 2106 con una interface conectada al core administrativo

Los problemas identificados son:

- El controlador Cisco 5508 en la red académica presenta un cuello de botella para las comunicaciones de todos los usuarios que se conectan por la red inalámbrica ya que solo tiene cuatro interfaces activas, en total se tendría 4Gbps, lo que no es suficiente para toda la cantidad de usuarios que se conectan vía el medio inalámbrico.
- No se tiene visibilidad de las aplicaciones que usan el medio inalámbrico por lo tanto no se podría pensar en hacer reconocimiento de aplicaciones para priorización de tráfico y/o para filtrado.
- No se tiene alta disponibilidad de los controladores inalámbricos ya que cada uno es independiente. En el caso de que fallara un controlador, simplemente las antenas pertenecientes al controlador quedarían sin servicio y los usuarios inalámbricos no podrían conectarse vía wifi.
- Actualmente los puntos de acceso y los alumnos que se conectan a la red a través de cualquier SSID van por la VLAN 310, esto ocasiona congestión dentro de esta VLAN.
- El tener controladores independientes para cada red, académicos y administrativos, significa una doble gestión para el departamento de TI.

2.1.2.c) Redes Inalámbricas

Actualmente se tienen configurados 4 SSID que son irradiados a lo largo del campus universitario como se puede observar en la figura 2.9.

Fig. 2.9 Redes inalámbricas presentes en el campus universitario

Los dos primeros SSID, UPC-INVITADOS y UPC-WIFI-ADM, pertenecen a la red administrativa. Los siguientes dos SSID, UPC_Privada y upc-publica, pertenecen a la red académica. Para entregar direcciones IP a los usuarios inalámbricos se tiene un servidor DHCP corriendo sobre Windows server 2003.

Los problemas identificados son:

- El SSID upc-publica que usan los estudiantes para conectarse a la red, es una red inalámbrica totalmente abierta, no cuenta con ningún tipo de seguridad. Cualquier persona ajena a la universidad puede conectarse a esta red y ocasionar ataques a los recursos informáticos de la universidad o simplemente navegar por internet y causar congestión en la red.
- Si se quisiera dar acceso de invitado a los proveedores que visitan la universidad tendría que hacerse de forma manual, creando un usuario y contraseña y luego otorgarlo a la persona que está de visita. Este proceso manual es muy desgastante y difícil de controlar por el departamento de TI de la universidad.
- No se tiene control de los dispositivos que ingresan a la red inalámbrica ni a quién pertenecen.
- Se ha observado que existe duplicidad de IP en la red inalámbrica. Este problema ocasiona malestar a los usuarios que se conectan a la red inalámbrica debido a que el segundo dispositivo que se conecta nunca podrá comunicarse debido a que ya su IP ya estuvo comunicándose previamente por otros puertos.

o Existe pérdida de paquetes cuando los usuarios de red intentan acceder a internet y tienen navegación lenta para acceder a tráfico de video.

2.2 Bases teóricas

2.2.1 Diseño de red jerárquico

Idealmente, cuando se diseña una red se busca lograr un comportamiento predecible que permita lograr una alta disponibilidad y que no requiera mantenimiento de forma muy seguida. Por ejemplo, una red de campus necesita recuperarse de fallas y cambios de topología rápidamente y de una manera predeterminada. La red debe ser escalable, es decir debe soportar fácilmente ampliaciones y mejoras futuras. Con una amplia variedad de protocolos y distintos tipos de tráfico, la red debe ser capaz de conectar a los usuarios de manera eficiente a los recursos que necesitan, independientemente de su ubicación.

En otras palabras, se debe diseñar la red en torno a los flujos de tráfico en lugar de un tipo particular de tráfico. Lo ideal sería que la red se coloque de manera que todos los usuarios finales se encuentren a una distancia constante de los recursos que necesitan para su uso. Si un usuario en una esquina de la red pasa a través de dos switches para llegar a un servidor de correo electrónico, cualquier otro usuario en cualquier otra ubicación en la red también debería requerir de dos saltos para tener el servicio de correo electrónico.

A medida que la red va creciendo, con más edificios, más pisos y grandes grupos de usuarios, el número de switches de acceso aumenta. Como resultado, el número de switches de distribución aumenta. En redes grandes, también es posible llegar a punto de tener que agregar los switches de distribución. Esto se hace mediante la adición de una tercera capa de jerarquía, llamada la capa de core, como se muestra en la figura 2.10.

Los flujos de tráfico en una red de campus se pueden clasificar en tres tipos, según el lugar donde se encuentra el servicio de red o un recurso en relación con el usuario final. La tabla 2.1 enumera estos tipos de flujo de tráfico, junto con la extensión de red que se recorre al pasar de cualquier usuario hacia el servicio.

Se observa la facilidad con que se pueden describir las rutas de tráfico. Independientemente de donde se encuentra el usuario, la ruta de tráfico comienza siempre en la capa de acceso y continua en la distribución y tal vez en las capas de core. Incluso un camino entre dos usuarios en los extremos opuestos de la red se convierte consistente y predecible, acceso > distribución > núcleo > distribución > acceso.

Cada capa tiene atributos que proporcionan funciones de red físicos y lógicos en el punto apropiado de la red del campus. La comprensión de cada una de las capas y sus funciones o limitaciones es importante para aplicar correctamente cada capa en el proceso de diseño.

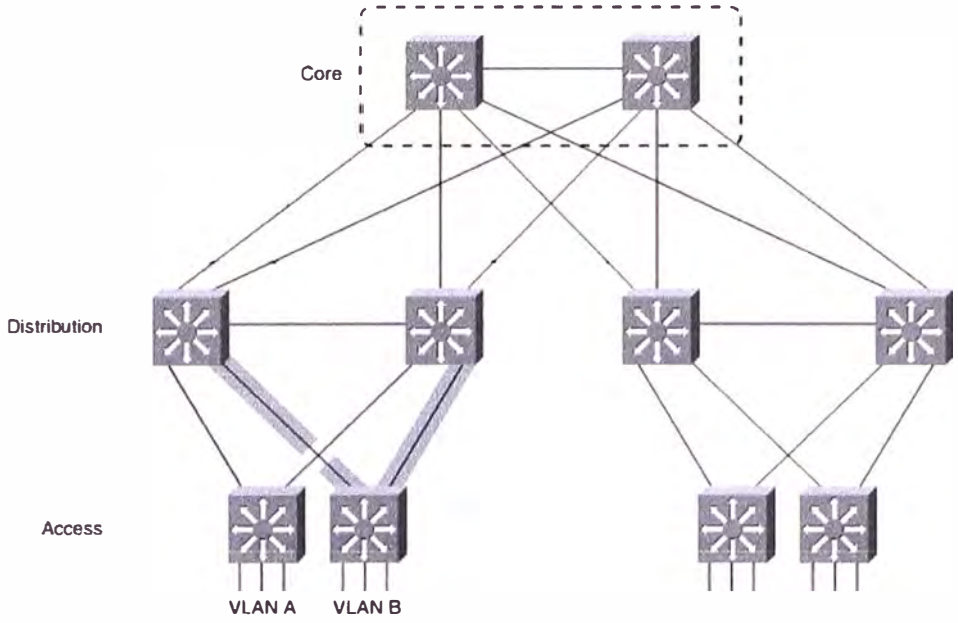


Fig. 2.10 Diseño de red de 3 capas

Tabla Nº 2.1 Tipo de servicios de red

TIPO DE SERVICIO	UBICACIÓN DEL SERVICIO	EXTENSIÓN DEL FLUJO DE TRAFICO
Local	Mismo segmento	Solo capa de acceso
Remoto	Diferente segmento	Capa de acceso a distribución
Empresarial	Atraviesa toda la red	Capa de distribución a core

2.2.1.a) Capa de Acceso

La capa de acceso está presente donde los usuarios finales están conectados a la red. Los switches de acceso suelen proporcionar conectividad de capa 2, dentro de una VLAN, a los usuarios finales. Los switches de esta capa, comúnmente se les llama switches de acceso, deben tener las siguientes características:

o Bajo costo por puerto.

o Alta densidad de puertos.

o Escalabilidad en lo enlaces de subida a las capas superiores.

o Funciones de acceso para usuario como VLAN, filtrado de protocolos y tráfico, y calidad de servicio (QoS)

o Redundancia y confiabilidad a través de múltiples enlaces hacia capas superiores.

2.2.1.b) Capa de Distribución

La capa de distribución proporciona la interconexión entre el acceso y la capa de core. Los switches de esta capa, comúnmente llamados switches de distribución, deben tener las siguientes características:

o Agregación de múltiples switches de la capa de acceso.

o Alto rendimiento para manejo de paquetes en capa 3.

o Funciones de conectividad basadas en políticas y seguridad a través de listas de acceso o filtrado de paquetes.

o Capacidades de Calidad de Servicio, QoS.

o Enlaces de alta velocidad, escalables y redundantes hacia el core de la red.

En la capa de distribución, se agregan o se juntan todos los enlaces ascendentes de todos los switches de acceso. Los switches de distribución deben ser capaces de procesar el volumen total de tráfico de todos los switches de acceso conectados. Estos switches deben tener una alta densidad de puertos de enlaces de alta velocidad para soportar el conjunto de switches de acceso.

Las VLAN y los dominios de broadcast convergen en la capa de distribución, por tanto se requiere enrutamiento de capa 3, filtrado y seguridad. Podemos decir que normalmente la capa de distribución es un límite de capa 3 donde se encuentra realiza el enrutamiento entre VLANs de la capa de acceso.

2.2.1.c) Capa de Core

Es la capa central de una red de campus y proporciona conectividad de todos los switches de distribución. El core, a veces referido como backbone, debe ser capaz de conmutar tráfico de la manera más eficiente posible. Los switches de la capa de core, comúnmente llamados switches de core, deben tener las siguientes características:

o Muy alto rendimiento en capa 3.

o No hay manipulaciones de paquetes innecesarias y tediosas (listas de acceso, filtrado de paquetes).

o Redundancia y confiabilidad mediante una alta disponibilidad

o Funciones de calidad de servicio avanzado, QoS avanzado.

Los switches en la capa de core o backbone deben estar optimizados para switching de alto desempeño. Debido a que la capa de core debe procesar gran cantidad de información proveniente de todo el campus, la capa de core debe ser diseñada teniendo en mente simplicidad y eficiencia.

2.2.2 Tipos de switches

2.2.2.a) Switches Fixed o de Puertos Fijos

Los fixed switches son normalmente usados para el acceso y distribución dependiendo de las capacidades de reenvío de tráfico que manejen; como el nombre lo indica, sus puertos son fijos y si se quisiera modificar los puertos tendría que reemplazarse todo el switch por otro con puertos acorde a la necesidad. Algunos modelos dentro de la marca Cisco son los Catalyst 2960 y Catalyst 3750. De la misma forma las capacidades en cuanto a memoria RAM y flash vienen fijas de fábrica y no se puede hacer upgrade.

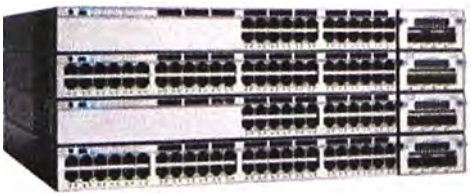


Fig. 2.11 Ejemplo de switch fixed

2.2.2.b) Switches Modulares

Los switches modulares generalmente tienen gran capacidad de reenvío de tráfico y son usados para el core de la red. Estos switches están conformados por un chasis al cual le vamos agregando tarjetas o módulos de puertos, linecards, dichos puertos pueden ser de diferente naturaleza dependiendo de las necesidades de conexión en un momento dado, por ejemplo se puede tener un módulo de 24 puertos Ethernet a 100Mbps instalado y luego al pasar del tiempo puede que este módulo ya no cumpla con los requisitos de conectividad por tanto se podría reemplazar este módulo por otro de 24 puertos Ethernet a 10Gpbs. Algunos switches modulares de gama alta aceptan módulos de servicios tipo firewall, IPS y otros.

Además de los módulos de puertos y de servicio, existe el módulo de control o supervisión que se encarga de definir la capacidad de troughput que entregará el switch a cada slot e incluso de características como cantidad de VLAN, tabla de enrutamiento, etc. Es muy recomendable tener este módulo en alta disponibilidad ya que si este módulo falla todo el switch dejaría de funcionar. En muchos casos a los módulos supervisores se les puede hacer upgrade de memoria RAM o flash para soportar nuevas versiones de software o nuevas capacidades.

Fig. 2.12 Ejemplo de switch modular

2.2.3 Acceso inalámbrico

Existen dos formas de despliegue de puntos de acceso inalámbricos para cubrir un área tipo campus. A continuación se detallan ambos despliegues.

2.2.3.a) Modo Autónomo

Tradicionalmente la infraestructura inalámbrica se centraba en torno a los puntos de acceso donde cada punto de acceso funcionaba como un hub entregando el servicio de conectividad inalámbrica a sus clientes asociados y localizados dentro de una celda de

cobertura. El tráfico desde y hacia cada cliente tenía que pasar por el punto de acceso para alcanzar cualquier parte de la red. El reto que se presentaba en este tipo de despliegues era que cada punto de acceso era autosuficiente y estaba relativamente aislado del resto de puntos de acceso; cada punto de acceso debía configurarse individualmente así hayan puntos de acceso con configuraciones muy similares y políticas idénticas. Al operar cada punto de acceso de forma independiente, cada punto de acceso debía elegir la radio frecuencia del canal en el que debía trabajar. Los clientes al asociarse al punto de acceso directamente estaban sujetos a las políticas de seguridad establecidas por el punto de acceso.

Para menos de 10 puntos de acceso este modo de operación podría ser útil sin embargo para despliegues con más de 10 puntos de acceso, la configuración de políticas de seguridad, la gestión de la radiofrecuencia y la calidad de servicio significan una labor manual muy pesada para el administrador de red, lo cual nos lleva a una red poco escalable, sin capacidad de soportar cambios y difícil de responder ante fallas.

Cada punto de acceso puede manejar múltiples SSID (Service Set IDentifier), y cada SSID se traduce a una VLAN en la red cableada, por tanto en un despliegue de puntos de acceso autónomos las VLAN podrían extenderse hacia cada uno de los puntos de acceso a través de todo el campus e incluso atravesar el core de la red lo cual va en contra de las reglas de diseño anteriormente revisadas, esto se puede apreciar en la figura 2.13.

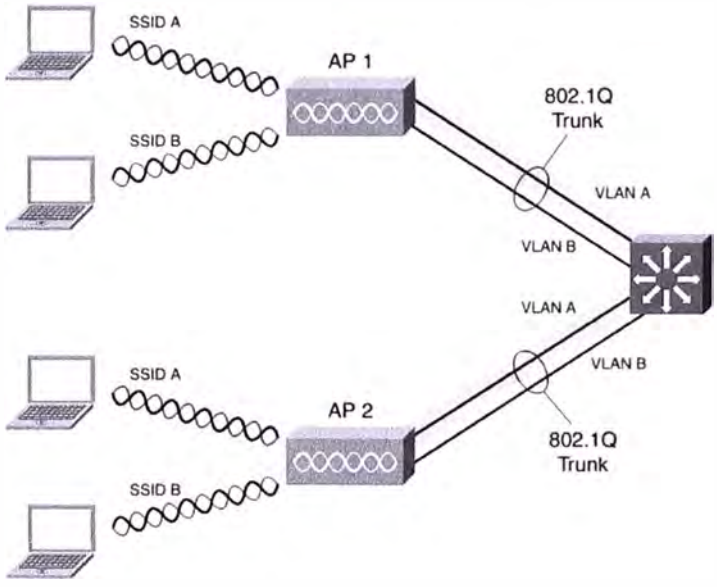


Fig. 2.13 Despliegue típico de un punto de acceso autónomo

2.2.3.b) Modo Centralizado

En este modo de despliegue se centraliza la seguridad, el control y la gestión de los puntos de acceso en un dispositivo central. Podemos decir que estas funcionalidades que eran realizadas por los puntos de acceso en el despliegue autónomo son ahora hechas de forma centralizada por un controlador.

Los puntos de acceso son ahora llamados LAP (Lightweght Access Point) y solo realizan las operaciones en tiempo real definido en 802.11. La designación de LAP se debe a que la imagen de software que corre es muy ligera en comparación con la imagen que corren los puntos de acceso autónomos, debido a que se le retira parte de las tareas al punto de acceso y se centralizan.

Las tareas de gestión son realizadas por el Wireless LAN Controller (WLC) que es común para todos los LAP. Los LAP solo realizan tareas en capa 1 y 2 donde se reciben y entregan las tramas del dominio de RF. Los LAP son totalmente dependientes del WLC para otras funciones de WLAN tales como autenticación de usuarios, gestión de políticas de seguridad, selección de canales de RF e incluso la potencia de la señal.

Esta división de trabajo se conoce como una arquitectura Split-MAC (División-MAC), donde las operaciones de MAC normales se separan en dos lugares distintos. Esto ocurre para cada LAP en la red, cada uno debe asociarse a un WLC para iniciar funcionamiento y dar conectividad a los clientes inalámbricos. El WLC se convierte en el hub central que soporta un número de LAP distribuidos en la red de switches.

Para que el LAP y el WLC empiecen a trabajar, ellos establecen primero un túnel para intercambiar información referente a 802.11 y luego un segundo túnel para la data de los clientes. El (los) LAP y el WLC pueden o no estar en la misma VLAN o subred IP, es más podrían estar en dos subredes IP totalmente distintas y en dos lugares distintos ya que el túnel hace esto posible al encapsular la data entre el LAP y el WLC, la data encapsulada luego puede ser conmutada (capa 2) o enrutada (capa 3) a lo largo de la red de campus.

El túnel se puede establecer usando el protocolo LWAPP (Lightweight Access Point Protocol) que es propietario de Cisco System o usando el protocolo CAPWAP (Control and Provisioning Wireless Access Points Protocol) definido en la RFC 4118.

Cualquiera que sea el protocolo que se use, se establecen dos túneles entre el controlador y los puntos de acceso. Por el primer túnel va tráfico de control encapsulado y encriptado; y por el segundo túnel va el tráfico de datos generado por los usuarios de forma encapsulada solamente (no encriptada) como se puede ver en la figura 2.14.

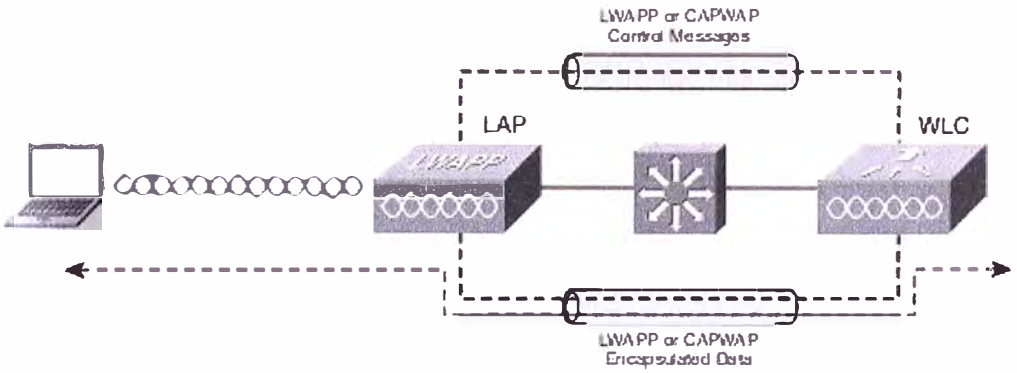


Fig. 2.14 Túneles creados entre un punto de acceso y un controlador

2.2.3.c) Funciones del WLC

El WLC permite solucionar muchos de los retos que presenta la arquitectura de AP autónomo. Dentro de las principales características podemos mencionar:

- Asignación dinámica de canales. El WLC elige y configura el canal de RF utilizado por cada LAP basándose en otros puntos de acceso activos en el área.
- Optimización de la Potencia de Transmisión. El WLC establece la potencia de transmisión de cada LAP basado en el área que se necesita cubrir. La potencia de transmisión también se ajusta automáticamente de forma periódica.
- Auto reparación de la cobertura inalámbrica. Si un LAP deja de funcionar, el agujero de RF será cubierto reajustando la potencia de transmisión de los LAP cercanos de forma automática.
- Roaming Flexible. Los clientes pueden hacer roaming ya sea de capa 2 o capa 3 con tiempos de transición muy rápidos.
- Balanceo de carga de clientes dinámico. Si dos o más LAP están en cubriendo la misma área geográfica, el WLC puede asociar a los clientes con el LAP menos utilizado. Esto distribuye la carga de clientes entre los LAP.
- Monitoreo de RF. El WLC al gestionar cada LAP realiza un escaneo de los canales para monitorear el nivel de uso de RF. Al escuchar en un canal, el WLC puede reunir de forma remota información sobre interferencia de RF, ruido, señales cercanas al LAP, y señales de puntos de acceso no autorizados.
- Gestión de seguridad. El WLC puede exigir a los clientes inalámbricos obtener una dirección IP de un servidor DHCP de confianza antes de permitirles asociarse y acceder a la WLAN.

2.2.4 Contexto de acceso a la red

En los entornos actuales de comunicaciones no solo basta identificar a los dispositivos que se conectan mediante el usuario y password de la persona que usa el dispositivo sino que también debemos tomar en cuenta otras variables para definir el contexto en el cual el usuario accede a la red. Por ejemplo no es lo mismo que un profesor universitario acceda a cambiar los registros de notas de sus alumnos usando un dispositivo personal, como una tablet, que usando una PC corporativa ya que el dispositivo personal está más propenso a ser usado por cualquier persona ajena a la organización que una PC corporativa dentro de una sala con accesos vigilados. También podríamos decir que si el profesor intenta acceder a cambiar los registros de notas de los alumnos a las 3 de la mañana probablemente se trate de una suplantación de identidad y sería conveniente que la red bloquee el acceso de este usuario a los recursos antes mencionados. Por tanto vemos que no es suficiente con una validación de usuario y password sino que debemos

definir un contexto de acceso a la red y que basado en este contexto se deben tomar decisiones de acceso a recursos de información.

El contexto de acceso a la red viene definido al responder 5 preguntas fundamentales, quién, qué, dónde, cuándo y cómo es que el usuario accede a la red. El quién identifica al usuario como tradicionalmente lo hacemos con el usuario y password, el qué define el dispositivo usado para acceder a los recursos de información que puede ser una tablet, un teléfono inteligente, una laptop, un teléfono IP, etc. El dónde define el lugar de la red desde donde accede el usuario, ejemplos de lugares son la oficina principal, una oficina remota e incluso un usuario desde su casa. El cuándo se refiere al tiempo en horas y minutos en que el usuario accede a la red. Finalmente el cómo se refiere a la tecnología utilizada para acceder a la red, ese decir si se usa un cable, si es medio inalámbrico vía wifi, o vía acceso remoto VPN (Virtual Private Network).

Fig. 2.15 Ejemplos de contexto de acceso a la red

Podríamos decir que el permitir o denegar el acceso a un recurso de información va depender del contexto en el cual el usuario se encuentre. En la figura 2.15 podríamos decir que Luis Veramendi con su laptop corporativa tiene acceso a los servidores de gestión de la red de la universidad mientras que con su tableta solo tiene acceso a internet.

Debido a que vivimos en un entorno con múltiples sistemas operativos como por ejemplo iOS, Android, Windows, Blackberry OS y otros más, podemos decir que una vez definido el contexto debe existir en la red un ente centralizado que pueda tomar la decisión y aplicar una política pre definida de acceso a los usuarios y sus dispositivos independientes del sistema operativo del dispositivo final. Este ente debe trabajar en conjunto con los equipos de red tipo switches y puntos de acceso inalámbricos ya que

estos equipos son la puerta de entrada de los usuarios y es desde aquí que debe empezar a permitir o denegar el acceso.

2.2.5 Control de acceso a la red

Control de acceso a red es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los usuarios y sus dispositivos, o sistema de autenticación, y reforzar la seguridad de la red de acceso.

El control de acceso a red es un concepto de ordenador en red y conjunto de protocolos usados para definir como asegurar los nodos de la red antes de que estos accedan a la red. Se puede integrar el proceso de remedio automático (corrigiendo nodos que no cumplen las normativas antes de permitirles acceso) en el sistema de red, permitiendo a la infraestructura de red como routers y switches trabajar en conjunto con el equipamiento informático del usuario final para asegurar que el sistema de información esté operando de manera segura antes de permitir el acceso a la red.

El objetivo del control de acceso a red es realizar exactamente lo que su nombre implica: control de acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos a los que pueden acceder en la red los usuarios y dispositivos y que pueden hacer en ella. Siendo más específicos, podemos decir que el control de acceso a la red busca cumplir los siguientes objetivos:

- Mitigar ataques de día cero. El propósito clave de una solución de control de acceso a red es la habilidad de prevenir en los equipos finales la falta de antivirus, parches, o software de prevención de intrusión de hosts y acceder así a la red poniendo en riesgo a otros equipos de contaminación y expansión de gusanos informáticos.
- Refuerzo de políticas. Las soluciones de control de acceso a red permiten a los operadores de red definir políticas, tales como tipos de ordenadores o roles de usuarios con acceso permitido a ciertas áreas de la red, y forzarlos en switches y routers.
- Administración de acceso e identidad. Donde las redes IP convencionales refuerzan las políticas de acceso con base en direcciones, los dispositivos de control de acceso a red lo realizan basándose en variables más avanzadas tipo autenticación de usuarios y tipos de dispositivo.

2.2.6 Conceptos Importantes del Control de Acceso a Red

2.2.6.a) Pre-admisión y Post-admisión

Existen dos filosofías de diseño predominantes, basadas en políticas de refuerzo antes de ganar acceso a la red o después de hacerlo. En el primer caso denominado control de acceso a red de pre-admisión, las estaciones finales son inspeccionadas antes de permitirles el acceso a la red. Un caso típico de control de acceso a red pre-admisión

sería el prevenir que equipos con antivirus no actualizados pudieran conectarse a servidores sensibles. Alternativamente, el control de acceso a red post-admisión crea decisiones de refuerzo basadas en acciones de usuario después de que a estos usuarios se les haya proporcionado el acceso a la red.

2.2.6.b) Con agente vs sin agente

La idea fundamental de la tecnología de control de acceso a red es permitir a la red tomar decisiones de control de acceso basadas en inteligencia sobre los sistemas finales, por lo que la manera en que la red es informada sobre los sistemas finales es una decisión de diseño clave. Una diferencia clave entre sistemas de control de acceso a red es si requieren agentes software para informar de las características de los equipos finales, o si por el contrario utilizan técnicas de escaneo e inventariado para discernir esas características remotamente.

2.2.6.c) Solución de cuarentena y portal cautivo

Muchas veces cuando los administradores de sistemas y redes despliegan productos de control de acceso a red esperan que a algunos clientes legítimos se les denegara el acceso a la red (si los usuarios no actualizaron su antivirus y otros sistemas). Por ello las soluciones de control de acceso a red requieren de un mecanismo para remediar el problema del usuario final que le ha sido denegado el acceso a la red.

Las dos estrategias comunes para este remedio son redes de cuarentena y portales cautivos.

Una cuarentena de red es una red IP restringida que proporciona a los usuarios acceso sólo a ciertos hosts y aplicaciones. La cuarentena a menudo se implementa mediante la asignación a una VLAN cuando la solución de control de acceso a red determina que un usuario final no cumple las políticas de acceso, entonces su puerto de conmutación es asignado a una VLAN que se dirige sólo a los servidores de parches y actualización mas no al resto de la red. También existen soluciones que utilizan técnicas de gestión de direcciones (por ejemplo, el protocolo de resolución de direcciones ARP) para la cuarentena, evitando la sobrecarga de administración de la VLAN de cuarentena.

Un portal cautivo intercepta el acceso HTTP a páginas web, redirigiendo a los usuarios una aplicación web que proporciona instrucciones y herramientas para la actualización de su equipo. Mientras el equipo pasa la inspección automatizada, no se permite el uso de la red fuera del portal cautivo. Esto es similar a la forma en que trabaja el acceso a una red inalámbrica pública de pago.

CAPITULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 Alternativas de solución

Las alternativas de solución consideradas buscan solucionar los problemas descritos anteriormente y están acorde con lo que la universidad puede ejecutar al corto y mediano plazo. Asimismo la solución elegida se integrará a los procesos establecidos actualmente tanto administrativos como académicos. Las alternativas de solución son las siguientes:

a) Optimizar los recursos que tiene actualmente la universidad y complementar estos recursos con hardware y software avanzado del mismo proveedor.

b) Retirar los equipos que tiene actualmente la universidad y elaborar un diseño de red desde cero basándose en una solución de múltiples proveedores de hardware y software.

A continuación detallaremos cada una de estas alternativas identificadas:

a) Optimizar los recursos que tiene actualmente la universidad y complementar estos recursos con hardware y software avanzado del mismo proveedor.

Ventajas

- Al mantener y optimizar los equipos actuales se protege la inversión realizada con anterioridad de 3 a 4 años.
- El mantener un solo proveedor o marca de hardware y software permite no solo basarse en estándares tecnológicos sino además sacar provecho de las capacidades avanzadas propias del proveedor único que sólo se pueden lograr mediante la integración de sus diversos productos. Por ejemplo lograr que un punto de acceso se autentique en la red de switching antes de entrar en funcionamiento, o que el switch pueda identificar el punto de acceso y configurar de manera automática el puerto por el cual se conecta el punto de acceso.
- Rápida puesta en producción del nuevo hardware y software, ya que se mantiene un único proveedor del cual ya se conocen las herramientas y características de los equipos, es mucho más fácil configurar y operar los equipos sin necesidad de volver a entrenar a los ingenieros del área de TI
- En caso de fallas se tiene un único punto de contacto para solucionar el problema, este único punto de contacto es el proveedor único de la solución. Esto nos ayuda a acortar los tiempos de respuesta ante la presencia de fallas.

- No es necesario cortar el servicio de la red de la universidad, por el contrario se puede hacer una migración gradual de cada componente.

Desventajas

- Es muy probable que el optimizar los equipos actuales signifique un monto a invertir en renovación de hardware o compra de licencias. Por ejemplo actualizar los sistemas operativos o cambios de tarjetas en los switches.
- Un proveedor único de soluciones de TI podría significar un único punto de falla y dependencia a este proveedor.

b) Retirar los equipos que tiene actualmente la universidad y elaborar un diseño de red desde cero basándose en una solución de múltiples proveedores de hardware y software. Con esta alternativa se propone volver a diseñar la red de la universidad de acuerdo a los requerimientos tecnológicos actuales y retirar la red existente que fue pensada en una solución de hace casi 20 años. Criterios básicos de diseño que se tendrían en cuenta serían tener una red convergente por la cual curse todo el tráfico de datos, voz y video y sin importar el medio por el cual se acceda, es decir sea medio cableado o medio inalámbrico.

Ventajas

- Se plantea un diseño de red 100% nuevo y acorde a las nuevas exigencias de la actualidad.
- Se plantea un esquema de distintos proveedores multimarca basado en estándares para asegurar compatibilidad.

Desventajas

- Al retirar el equipamiento actual se estaría desechando la inversión hecha no solo hace 20 años sino también la realizada recientemente hace 1 año lo cual significaría una pérdida de la inversión.
- Al tener una solución de distintos proveedores o multimarca, las soluciones nunca llegan a integrarse al 100% sino se mantienen como islas separadas o si logran integrarse es muy probable que sacrifiquen alguna capacidad avanzada propia de cada fabricante.
- Se necesita personal especializado en cada uno de los productos de distintas marcas y/o invertir en capacitación de los ingenieros de TI.
- En caso de fallas, se tendría que coordinar con el soporte técnico de cada proveedor o marca para encontrar la solución del problema. Esto podría significar tiempos largos de caída de servicios.
- Los tiempos de migración a una nueva solución 100% nueva afectaría los servicios de la universidad e incluso retrasar el funcionamiento de los recursos de información.

3.2 Metodología de evaluación de soluciones

Se seleccionará la alternativa más adecuada, tomando en cuenta ciertos criterios de evaluación. Los criterios se describen en la tabla 3.1.

Tabla Nº 3.1 Criterios de evaluación para la toma de decisiones

N°	CRITERIOS DE EVALUACIÓN
1	Conocimiento actual de la tecnología
2	Tiempo de despliegue de la solución
3	Costo de la solución
4	Uso de protocolos avanzados

Se evalúan los criterios arriba indicados, en base a la técnica de ponderación, para lo cual se definieron los pesos porcentuales en la tabla 3.1.

Tabla Nº 3.2 Pesos porcentuales de los criterios de evaluación

CRITERIO DE EVALUACIÓN	PESO PORCENTUAL
Conocimiento actual de la tecnología	0.25
Tiempo de despliegue de la solución	0.25
Costo de la solución	0.30
Uso de protocolos avanzados	0.20

Para la calificación de cada criterio de evaluación se establece una escala de puntuaciones, la cual se muestra en la tabla 3.3

Tabla Nº 3.3 Descripción de puntuaciones

PUNTUACIÓN	DESCRIPCIÓN
1	Muy Bajo
2	Bajo
3	Intermedio
4	Bueno
5	Muy Bueno

3.3 Descripción de los criterios utilizados en la evaluación

A continuación se detallan los criterios utilizados en la evaluación de la mejor solución.

3.3.1 Conocimiento Actual de la Tecnología

Se refiere al conocimiento que tienen los miembros del departamento de TI de la UPC sobre las tecnologías involucradas en la solución a implementar. Este criterio es importante, por cuanto el departamento de TI de la UPC será el encargado de dar el soporte a todas las tecnologías desplegadas dentro del campus universitario por tanto tener un sólido conocimiento es de vital importancia. Ambas alternativas de solución involucran manejo de software y hardware nuevo por lo que se debe considerar

capacitaciones para el equipo en estas nuevas tecnologías brindadas por externos a la empresa, las mismas que deben ser consideradas como parte del cronograma y costos del proyecto.

3.3.2 Tiempo de Despliegue de la Solución

Se refiere al tiempo que tomaría la puesta en producción de la solución, es importante porque el servicio de conexión para los usuarios de red no se debe cortar en ningún momento. Se podrían aceptar tiempo largos de corte de servicio cuando la universidad está en periodo de vacaciones y no haya alumnos por ejemplo en los meses de diciembre a marzo. Por ello se debe evaluar este criterio en estrecha relación con la disponibilidad del servicio de conectividad para los usuarios de red.

3.3.3 Costo de la Solución

Se refiere al costo que genera para la empresa la elección de una u otra solución. Para la situación descrita, este criterio es importante porque ambas alternativas involucran el uso de una nueva tecnología y para ambas se consideran costos de compra de nuevo equipamiento (hardware y software) y costos de capacitación de personal.

3.3.4 Uso de Protocolos Avanzados

Se refiere a la implementación y uso de protocolos de comunicación avanzados que permitan comunicación a niveles superiores a los que actualmente se tienen. Estos nuevos protocolos significarían el uso de tecnología de punta que asegure la escalabilidad y crecimiento de la red. La importancia de este criterio radica en que la inversión en tecnología que se haga a día de hoy debe ser tal que asegure su vigencia en el mercado tecnológico para al menos los próximos cinco años.

3.4 Toma de decisión

En la tabla 3.4 se detalla el cuadro comparativo entre las dos alternativas propuestas empleando los criterios anteriormente definidos con las ponderaciones que poseen cada uno de estos criterios. Los puntajes fueron establecidos tomando en cuenta el impacto que tiene cada uno de los criterios en la pronta atención a la demanda de conectividad segura y eficiente que requieren los usuarios.

3.5 Análisis de la toma de decisión

El conocimiento actual de la tecnología tiene importancia pues ambas soluciones involucran implementación de nuevas características avanzadas de redes.

La primera alternativa plantea optimizar y mejorar la plataforma con que se cuenta actualmente y de la cual se tiene un amplio conocimiento mientras que la segunda alternativa considera reemplazar el equipo existente lo cual representaría un aprendizaje del 100% de las tecnologías a desplegar, por ello se considera mejor a la primera alternativa dado que requiere menos investigación en despliegue y posterior soporte.

Tabla Nº 3.4 Puntaje ponderado asignado a cada criterio de evaluación – Puntaje final

Nº	CRITERIO	PESO	PUNTAJE ALT A	PUNTAJE ALT B	PUNTAJE POND ALT A	PUNTAJE POND ALT B
1	Conocimiento actual de la Tecnología	25%	4	2	1.00	0.50
2	Tiempo de despliegue de la solución	25%	3	2	0.75	0.50
3	Costo de la Solución	30%	5	3	1.50	0.90
4	Uso de protocolos avanzados	20%	3	3	0.60	0.60
	TOTAL	100%			3.85	2.50

El tiempo de despliegue de la solución para el caso de la primera alternativa es menor, en tal sentido y ante la gran necesidad de conectividad dentro del campus universitario, se elige a la primera alternativa.

Se puede mencionar también que la primera alternativa incluye menos períodos de capacitación dado que el departamento de TI cuenta con el conocimiento y experiencia necesarios para poder desplegar las nuevas soluciones que se vayan a implementar.

El costo de la solución para ambas alternativas es diferente, pues la primera considera optimización de la infraestructura actual y compra de componentes que se integren a lo actual mientras que la segunda opción es una reingeniería total de la red de la universidad. Se elige la primera alternativa, pues requiere menor inversión y menores tiempos de capacitación y despliegue lo que permitirá que el servicio esté disponible más rápidamente asegurando un costo razonable.

Respecto al criterio de uso de protocolos avanzados, se puede mencionar que tanto la primera como la segunda opción se basan en estándares internacionales y por tanto pueden parecer tecnologías parecidas; sin embargo, cada fabricante cuenta con desarrollos propietarios que se deben tomar en cuenta al momento de tomar la decisión pues estas características propietarias deben agregan valor a la solución elegida y simplificar los procesos y mantenimiento de la solución a implementar.

Al análisis antes descrito, se debe adicionar que la primera alternativa considera un cambio por fases y es muy importante el nivel de soporte y conocimiento que manejen los ingenieros que vayan a realizar esta migración por tanto el proveedor deberá hacer el seguimiento correspondiente para poder realizar de forma exitosa esta solución.

En consecuencia, luego de realizado el análisis de la elección, considerando los beneficios que las dos opciones ofrecen, se seleccionó la primera alternativa:

“Optimizar los recursos que tiene actualmente la universidad y complementar estos recursos con hardware y software avanzado del mismo proveedor.”

3.6 Solución del problema

En la sección anterior identificamos como mejor solución “Optimizar los recursos que tiene actualmente la universidad y complementar estos recursos con hardware y software avanzado del mismo proveedor.” Ahora revisaremos los componentes que podemos optimizar dentro de la red de la universidad y terminaremos viendo nuevos componentes que nos permitirán llevar a la red de la universidad a ser una red unificada dentro de una arquitectura concebida en la conectividad y convergencia total; sea esta cableada, inalámbrica, de datos, voz y/o video. Esta arquitectura ofrecerá soluciones y funcionalidades que puedan ir siendo adoptadas por la UPC en el tiempo y así construir una arquitectura integrable que facilite y reduzca los costos operativos.

3.6.1 Optimización de los recursos actuales

Revisaremos las mejoras que podemos realizar sobre los equipos actualmente presentes en la red de la universidad. Se tratará de identificar una solución para cada problema indicado con la optimización de los recursos existentes, lo que no se pueda solucionar con los recursos existentes se planteará con hardware y software nuevo del mismo proveedor.

Ya que actualmente se cuenta en su mayoría con tecnología de la marca Cisco, nos enfocaremos en optimizar los recursos existentes con nuevas funcionalidades de esta marca que solo requieran un cambio de sistema operativo, cambio de configuración, cambio de posición de los equipos o inserción mínima de hardware en los equipos tipo módulos o tarjetas.

3.6.1.a) Optimización de la Red LAN

Para la red LAN que es la plataforma por la que pasaran todas las comunicaciones de los usuarios de la universidad se plantea tener una sola infraestructura de red, es decir dejar de ver la red como dos entes separados en red académica y red administrativa sino que sea una sola plataforma física sobre la cual de manera lógica se dividan los servicios ya sean para fines académicos o fines administrativos.

Para los servidores se debe tener de preferencia un equipo especializado para realizar switching en centros de datos que tenga velocidades de 10Gbps Ehternet y limitar el dominio de broadcast de la LAN mediante la separación de las VLAN y subredes IP.

Como switch core para la LAN se mantendría el switch modular Cisco Catalyst 4507R+E que cubre las necesidades de la universidad (capacidad de switching 848Gbps).

Revisamos los módulos que tiene este switch usando el comando "show module".

```
sw-coreadm#show module
Mod Ports Card Type                                  Model              Serial No.
----+----+--------------------------------------------+------------------+-----------
 1   48  10/100/1000BaseT (RJ45)                     WS-X4648-RJ45-E    JAE14520JAF
 3    4  Sup 7-E 10GE (SFP+), 1000BaseX (SFP)        WS-X45-SUP7-E      CAT1450L0C7
 4    4  Sup 7-E 10GE (SFP+), 1000BaseX (SFP)        WS-X45-SUP7-E      CAT1439L06H
 5   24  1000BaseX (SFP)                             WS-X4624-SFP-E     JAE14500GPT
 6   12  1000BaseX (SFP)                             WS-X4612-SFP-E     JAE1606062F
 7   48  10/100/1000BaseT (RJ45)                     WS-X4648-RJ45-E    JAE16140416
Mod  Redundancy role     Operating mode     Redundancy status
----+--------------------+------------------+-----------------------
 3   Standby Supervisor   SSO                Standby hot
 4   Active Supervisor    SSO                Active
```

Podemos observar que el chasis cuenta con doble modulo supervisor, lo cual asegura la alta disponibilidad activo/standy by del switch. De acuerdo a la hoja de especificaciones de Cisco, el switch Catalyst 4507R+E trabajando con la supervisora Sup7-E entrega una capacidad de 48Gbps a cada slot del chasis.

Todos los módulos de puertos son de la serie 46xx, los cuales solo trabajan a 24Gbps lo cual significa que tenemos una sobresuscripción de 2 a 1. Por tanto se plantea migrar a tarjetas más avanzadas de la serie 47xx para poder utilizar toda la capacidad del chasis de 48Gbps. Para los puertos en cobre usar el módulo WS-X4748-RJ45-E y para los puertos en fibra usar el módulo WS-X4712-SFP+E.

Revisamos la versión de software del switch de core con el comando show versión

sw-coreadm#show version

Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software (cat4500e-UNIVERSALK9-M), Version 03.01.01.SG RELEASE SOFTWARE (fc1)

Según la documentación de Cisco, notamos que esta versión tiene más de 3 años de antigüedad y no es soportada por el fabricante actualmente por lo cual se recomienda pasar a la última versión de software que es la versión 03.04.00.SG

En los switches de distribución también es recomendado realizar un upgrade de software. Actualmente se cuenta con la versión de software 12.2.55.SE3 que tiene una antigüedad de más de dos años y tampoco es soportada por el fabricante por lo que se recomienda actualizar a la versión más actual, 15.0.2.SE4

SWADDIS01_CCMOPLP4#sh ver

Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)

SWADDIS01_CCMOPLP4 uptime is 1 week, 6 days, 12 hours, 14 minutes

System returned to ROM by power-on

System restarted at 21:45:09 PET Thu Dec 6 2012

System image file is "flash:/c3560e-universalk9-mz.122-55.SE3/c3560e-universalk9-mz.122-55.SE3.bin"

En los switches de acceso se sigue de la misma manera, realizando el upgrade de software. Actualmente se cuenta con la versión de software 12.2.55.SE3 que tiene una antigüedad de más de dos años y tampoco es soportada por el fabricante por lo que se recomienda actualizar a la versión más actual, 15.0.2.SE4

SWADACS4_MOCCPLP4#sh ver

Cisco IOS Software, C2960S Software (C2960S-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)

SWADACS4_MOCCPLP4 uptime is 1 week, 6 days, 12 hours, 16 minutes

System returned to ROM by power-on

System restarted at 21:43:36 PET Thu Dec 6 2012

System image file is "flash:/c2960s-universalk9-mz.122-55.SE3/c2960s-universalk9-mz.122-55.SE3.bin"

Para mejorar el rendimiento de la red LAN se pueden aprovechar las características de priorización de tráfico (calidad de servicio) con que cuentan los equipos actuales. En los switches de acceso, el sistema operativo y la licencia LAN Base nos permite configurar QoS de la siguiente manera:

a) Habilitar QoS en el switch

Switch(config)# mls qos

b) Habilitamos QoS en los puertos donde hay tráfico de voz y video.

Switch(config)# interface type mod/num

Switch(config-if)# auto qos trust dscp

En este paso haremos que el switch marque los paquetes de voz que recibe del teléfono conectado con calidad de servicio DSCP 46.

c) Habilitamos QoS en los puertos uplink de los switches.

Switch(config)# interface type mod/num

Switch(config-if)# mls qos trust dscp

Este paso se debe repetir en el switch de distribución donde se conectan los puertos uplink de los switches de acceso para que se mantengan los paquetes marcados con calidad de servicio. Y de la misma manera el marcado de paquetes se debe mantener en los puertos que conectan a los switches de distribución hacia los switches de core. De esta manera toda la red LAN forma lo que se denomina una zona de confianza de QoS donde los paquetes de voz y video se transmitirán con mayor prioridad que los paquetes de datos.

3.6.1.b) Unificación de la Red Académica y la Red Administrativa

Para unificar las dos redes, desde un punto de vista lógico se debe tener especial cuidado con los siguientes criterios:

o Sobrelapamiento de las VLAN. Se tienen VLAN duplicadas en la red académica y en la red administrativa, se debe migrar las VLAN duplicadas en la red académica a la red administrativa. Se recomienda separar los bloques de VLAN de acuerdo al rol que cumplen y diferenciar las VLAN de acuerdo a la numeración que llevan.

Tabla Nº 3.5 Cambio de VLAN sugerido para evitar sobrelapamiento

TIPO DE RED	NÚMERO DE VLAN
Red Académica	200-299
Red Administrativa	300-399

Con este esquema se asegura tener gran cantidad de VLAN para uso actual y futuro, estas VLAN se deben repartir de acuerdo al rol que cumple cada grupo funcional de la universidad, por ejemplo VLAN de marketing, VLAN de docentes, VLAN de estudiantes, etc.

o Sobrelapamiento de redes IP. Afortunadamente no existe sobrelapamiento de redes IP en la red actual de la UPC ya que a este nivel si se trabajó con una adecuada planificación para evitar este tipo de problemas.

o Políticas de Seguridad entre redes IP. Actualmente se tiene un servidor Linux corriendo el servicio de Firewall vía IP tables como equipo de seguridad que controla el acceso de usuarios de la red administrativa a la red académica y viceversa. Como se piensa simplificar todo a una sola red física y hacer la separación de forma lógica, lo que se plantea es mover todas estas políticas de seguridad hacia los switches de distribución y/o de core, solo de ser necesario, mediante el uso de listas de acceso ACL aplicadas a las interfaces VLAN para limitar el acceso entre redes IP y dentro de una misma VLAN si es necesario se podría usar la funcionalidad de VACL para filtrar acceso de usuarios a un recursos dentro de una misma VLAN.

3.6.1.c) Optimización de la Red Inalámbrica

- **El Controlador Inalámbrico**

Hemos revisado en el capítulo anterior que la conexión actual entre el controlador inalámbrico y la red LAN es de 1Gbps lo cual ocasiona un cuello de botella para las comunicaciones, por ello se plantea aumentar el ancho de banda de conexión del controlador hacia la red LAN mediante el uso de las demás de interfaces, al menos 4 interfaces. Para poder balancear la carga de los usuarios entre las cuatro interfaces y tener redundancia se recomienda usar agregación de puertos mediante el protocolo LACP configurado en el switch. De ser posible, sería conveniente usar las 8 interfaces del controlador para tener total balanceo de carga y alta disponibilidad.

Fig. 3.1 WLC Cisco 5508

Para evitar el problema de duplicidad de las direcciones IP en el medio inalámbrico se debe restringir el acceso a la red inalámbrica para que solamente los usuarios que reciban dirección IP vía DHCP de un servidor autorizado puedan navegar por la red. Otros usuarios con direcciones IP estáticas u obtenidas de otro servidor DHCP distinto al definido como confiable serán rechazados por el controlador. Para activar esta funcionalidad, se debe habilitar el "DHCP Addr. Assignment" de manera sencilla completando el check en el recuadro correspondiente.

Fig. 3.2 Habilitamos el requisito de usar DHCP server para navegar

- **Calidad de Servicio en Inalámbrico**

De la misma forma que establecimos la calidad de servicio para la red LAN también estableceremos calidad de servicio para la red inalámbrica. Esta configuración se realiza en el controlador inalámbrico y se pueden diferenciar cuatro niveles de calidad de servicio en el aire según la tabla 3.6.

Tabla Nº 3.6 Tipos de Calidad de Servicio en el aire

TIPO DE QoS	USO TÍPICO	IP DSCP
Platino	Tráfico de voz	46(EF)
Oro	Trafico de video	34(AF41)
Plata	Mejor esfuerzo	0(BE)
Bronce	Background	10(AF11)

Para asignar el nivel de calidad de servicio a un SSID se deben seguir los siguientes pasos:

1. Accediendo a la consola del controlador inalámbrico elegir una WLAN
2. En el tab de QoS elegir el nivel de calidad de servicio que se va implementar. Por defecto debe estar seleccionado Mejor Esfuerzo (Best Effort)

Esta configuración se debe realizar en todos los SSID definidos anteriormente para asegurar que el tráfico sea priorizado adecuadamente. Además en el switch de core donde va conectado el controlador inalámbrico se debe configurar los puertos como trust para la calidad de servicio con el objetivo de asegurar que los paquetes marcados provenientes del medio inalámbrico se mantengan marcados en el medio cableado.

- **Puntos de Acceso Inalámbricos**

Lo primero que se debe mejorar es la señal de radio que captan los usuarios finales, es decir empezar desde la capa física del modelo OSI. Para ello la orientación de los puntos de acceso inalámbricos debe corregirse lo cual implica orientarlos en forma horizontal para que el patrón de radiación llegue con mayor eficiencia a los dispositivos inalámbricos de usuario final. La figura 3.3 muestra la correcta orientación de un punto de acceso.

Otro aspecto importante a mejorar respecto a la radio es habilitar la banda de 5GHz en todos los puntos de acceso posibles para hacer balanceo de carga de clientes entre las bandas de 2.4GHz y 5GHz. Para los puntos de acceso inalámbrico que solo tengan elementos de antena de 2.4GHz se debe completar con elementos de antena que trabajen en 5GHz. La figura 3.4 muestra un punto de acceso con todas sus antenas.

Fig. 3.3 Posición correcta del punto de acceso inalámbrico para aprovechar su patrón de radiación al máximo

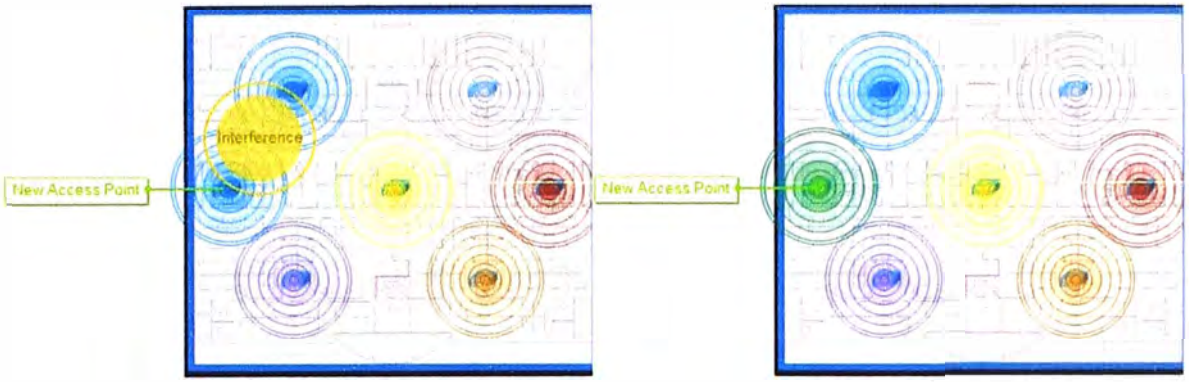
Fig. 3.4 Punto de acceso inalámbrico con los elementos de antena, 2.4 GHz y 5GHz, desplegados

Yendo un paso más adelante, una vez que se tengan los puntos de acceso correctamente instalados con todos los elementos de antena en 2.4 GHz y 5GHz se podría habilitar la funcionalidad avanzada de los equipos Cisco llamado Band Select que consiste en llevar a 5GHz a dispositivos que soporten esta banda ya que normalmente un equipo prefiere conectarse a la banda de 2,4GHz por más que soporte ambas bandas. Con esta funcionalidad la red inalámbrica de manera automática reconocerá los dispositivos de los usuarios y podrá realizar un balanceo de carga de usuarios entre las bandas de 2.4GHz y 5GHz liberando así la banda saturada de 2.4GHz y además sacando provecho de la banda de 5GHz en la que se tienen canales con ancho de banda superior.

La solución desplegada actualmente para la red inalámbrica puede contar con un nivel avanzado de inteligencia mediante la habilitación de la funcionalidad Radio Resource Manager, RRM. Esta funcionalidad consiste en múltiples tareas que realiza el controlador a nivel de gestión de inteligente de la radiofrecuencia y los niveles de potencia de la señal en todos los puntos de acceso a lo largo del campus universitario. Si se instala un nuevo punto de acceso, el controlador identificará el mejor canal de comunicaciones para que trabaje este nuevo punto de acceso y no genere interferencia con otros canales usados por puntos de acceso adyacentes. En la figura 3.5 podemos ver un ejemplo de este ajuste de canales de comunicación en el medio inalámbrico.

En caso que algún punto de acceso se desconecte, pierda la conexión eléctrica o simplemente falle por alguna razón, el controlador tiene la inteligencia para variar los niveles de potencia de los puntos de acceso adyacentes de manera que cubran la zona

que cubría antes el punto de acceso que falló de esta manera se garantiza la comunicación de los dispositivos de usuario final que hayan estado conectados al anterior punto de acceso. En la figura 3.6 podemos ver un ejemplo de este ajuste de niveles de potencia de señal para mejorar la comunicación en el medio inalámbrico.



Nuevo Punto de Acceso generando interferencia en los canales de RF

Nuevo Punto de Acceso en un canal de comunicaciones que no interfiere con el resto de puntos de acceso

Fig. 3.5 Control Inteligente de los canales inalámbricos realizado por el controlador

- **Conectividad entre los Puntos de Acceso y el Controlador**

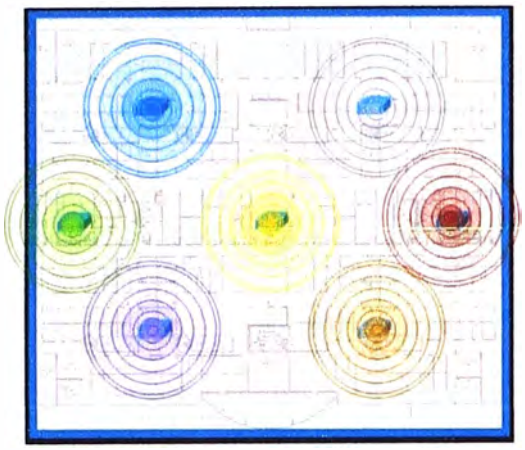
Para mejorar el desempeño de los usuarios cableados como inalámbricos, se debe poner los puntos de acceso en una VLAN diferente a la VLAN que usan los usuarios finales conectados vía cable para generar tráfico de datos, voz y video.

Se debe dejar configurada la VLAN 310 en los puertos de los switches de acceso donde se conectan los puntos de acceso inalámbrico. Esta VLAN llega hasta el controlador inalámbrico a nivel de capa 2 y de esta manera logran la comunicación. Los dispositivos inalámbricos de usuario final estarán en otras VLAN separadas y así podemos aislar el tráfico de control del AP del tráfico de datos de los usuarios finales.

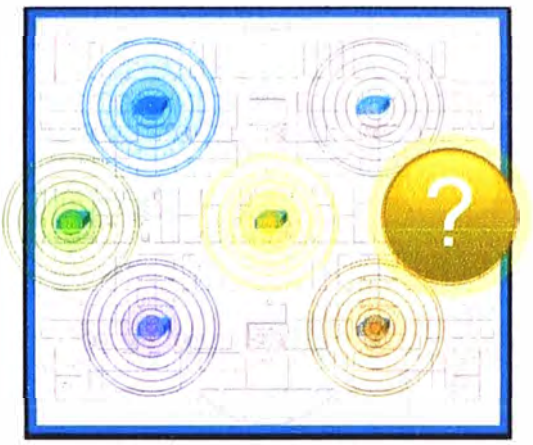
- **Redes Inalámbricas**

Actualmente se tienen distintos SSID en la universidad que fueron creados de acuerdo a la necesidad urgente y sin embargo fueron quedando dentro de la infraestructura de red. Según las mejores prácticas, cada usuario de la universidad se debe conectar a un SSID particular el cual luego se traduce a una VLAN. Para universidades se recomienda tener a lo más 4 SSID según muestra la tabla 3.7.

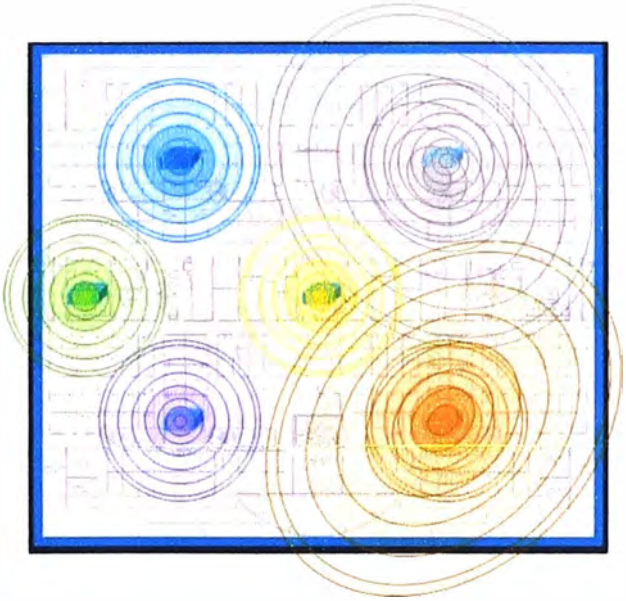
Debemos recordar que la cantidad de SSID debe mantenerse al mínimo para evitar impactar en el rendimiento debido al tráfico de control excesivo. Cada SSID usa un mensaje tipo faro en broadcast que ocupa una porción del ancho de banda disponible y mientras más SSID se tenga, más faros se tendrán, lo cual implica utilizar el ancho de banda disponible para tráfico de control y por tanto dejar menor ancho de banda para el tráfico de usuarios.



El punto de acceso del extremo derecho presenta fallas



El punto de acceso falla y deja una zona sin iluminar



Los demás puntos de acceso cubren la zona dejada por el anterior punto de acceso

Fig. 3.6 Control Inteligente de la potencia de la señal realizado por el controlador

Tabla Nº 3.7 SSID usados en un campus universitario

SSID	USUARIOS
IT	Administradores de red
Facultad	Empleados de la universidad
Estudiantes	Estudiantes de la universidad
Invitados	Solo acceso a internet para Invitados

3.6.2 Complemento con hardware y software

3.6.2.a) Redundancia en el core de la Red LAN

Con el objetivo de tener una red siempre disponible que asegure el acceso a la información las 24 horas del día durante los 365 días del año se debe tener redundancia a todo nivel. Empezando por la capa principal de core, se plantea tener un switch core redundante con las mismas tarjetas supervisoras, sistema operativo y licenciamiento que

el switch actualmente en producción para tener una redundancia coherente. La conexión entre los switches de core debe realizarse a velocidades de al menos 10Gbps. Ambos switches de core deben presentarse al resto de componentes de la red como si fueran un solo switch lógico para evitar interfaces bloqueadas por el protocolo spanning tree, STP, y de esta manera aprovechar al máximo las interfaces 10Gbps presentes en la red. Ya que se ha optado por la tecnología Cisco, en dicha marca, esta funcionalidad es llamada Virtual Switch System, VSS, que viene disponible en los switches Catalyst 4500 desde la versión de software IOS XE 3.4.0SG. En la figura 3.7 podemos ver cómo quedaría el core de la red desde una vista física y una vista lógica. Los switches de distribución o acceso que se conectan al core lógico lo realizarán mediante la configuración de un etherchannel lógico de dos enlaces, por ello ambas interfaces estarán activas y en caso falle una, la otra se hará cargo de reenviar el tráfico total.

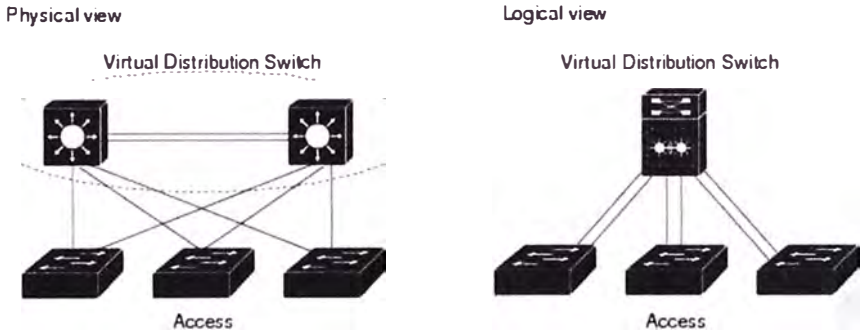


Fig. 3.7 De manera física se tiene dos switches de core en redundancia. De manera lógica se tiene un solo switch de core.

En los switches de distribución se debe configurar el etherchannel hacia el core de la red, VSS, en las interfaces de uplink, ver figura 3.7. Cada pabellón de la universidad cuenta con fibra óptica redundante tendida hacia el core por lo que solo se debería hacer la conexión en los puertos de uplink una vez que se tenga el switch core redundante.

Ya que actualmente la universidad cuenta con telefonía IP y los teléfonos usan la característica Power over Ethernet, PoE, se plantea habilitar la funcionalidad de ahorro de energía automática en los switches llamado Energywise como un valor agregado. Esta funcionalidad permite establecer políticas de ahorro de energía en los switches, de manera que estos equipos puedan apagar y prender de manera automática sus puertos que entregan energía a los dispositivos de usuario final tipo teléfonos IP, puntos de acceso inalámbricos, clientes ligeros, etc. Esta funcionalidad para los switches Cisco no tiene ningún costo de licenciamiento solo debe configurarse via línea de comandos o via consola grafica de administración.

3.6.2.b) Cambio de los puntos de Acceso Inalámbricos

En la sección de optimización revisamos algunas sugerencias para mejorar el rendimiento de los puntos de acceso desplegados actualmente, sin embargo para mejorar aún más

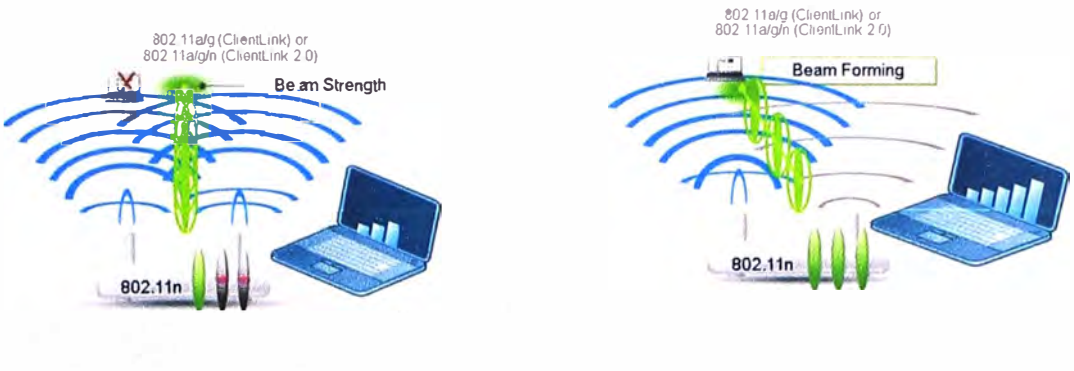
las velocidades de comunicación entre los puntos de acceso inalámbricos y los usuarios, se plantea renovar el parque de puntos de acceso desplegados en la universidad por nuevos puntos de acceso con capacidades avanzadas y que soporten el estándar IEEE 802.11n y estén preparados para soportar a futuro el estándar IEEE 802.11ac que permita llegar a velocidades de 1Gbps en el aire y así proteger la inversión que se haga actualmente. Además estos puntos de acceso deben soportar al menos una densidad de usuarios de 40 por punto de acceso inalámbrico. Dentro de la marca Cisco encontramos el modelo de puntos de acceso Cisco Aironet 3600 que soportan el estándar IEEE 802.11n y además mediante la inserción de un módulo soportan el estándar IEEE 802.11ac. Dicho modulo tiene un costo de la tercera parte de un nuevo punto de acceso que soporte IEEE802.11ac, por lo tanto con el Cisco Aironet 3600 solo tendríamos que agregar el modulo barato en vez de reemplazar todos los puntos de acceso y realizar un nuevo gasto en equipamiento nuevo, es decir no solo se plantea una solución buena técnicamente sino que también se busca proteger la inversión realizada por la universidad.

Fig. 3.8 Punto de Acceso Cisco 3602i con antenas internas

Para evitar la interferencia de señales ajenas a la comunicación wifi se habilitará la funcionalidad Cisco CleanAir, tecnología propietaria de Cisco, esta tecnología nos permitirá optimizar de manera automática e inteligente la comunicación inalámbrica. Los puntos de acceso Cisco Aironet 3600 cuentan con un hardware especializado que va censando el aire e identifica interferencias presentes en los canales de comunicación wifi, si un canal está muy saturado con interferencia el punto de acceso lleva de forma automática a otro canal libre de interferencia la comunicación wifi y al realizar esta funcionalidad en hardware no disminuye el desempeño del punto de acceso, cosa que si sucedería si fuera en software.

Para optimizar la cobertura de los puntos de acceso se habilitará la funcionalidad Cisco Client Link presente en los puntos de acceso Cisco Aironet 3600, dicha funcionalidad consiste en adaptar el patrón de radiación del punto de acceso de acuerdo a la posición del dispositivo de usuario final para obtener como resultado una mayor potencia de la señal donde está el usuario. Esto nos garantiza tener un adecuado canal de

comunicaciones para poder establecer llamadas telefónicas y llamadas de video en alta definición que permitan colaborar en mejor medida y poder aplicarlo a clases a distancia o videoconferencias dentro del campus universitario.



Pobre señal al usuario final dando como resultado una mala experiencia.

Señal dirigida al usuario, da como resultado mejor experiencia y gran desempeño

Fig. 3.9 Señal para el usuario antes y después de Clean Air

3.6.2.c) Redundancia en el Controlador Inalámbrico

De la misma forma que tenemos redundancia en el core de la red LAN, para la red inalámbrica debemos contar con redundancia a nivel de los controladores por ello se plantea adquirir un controlador adicional, WLC 5508 y conectar todas 8 sus interfaces 1Gbps al core VSS de la red. Algo muy importante que resaltar es que la tecnología Cisco permite tener un controlador en activo y otro en stand by con las configuraciones sincronizadas y lo más importante es que las licencias que tiene el controlador activo, que depende del número de puntos de acceso presentes, migrarán al controlador en stand by en caso de falla. De esta manera la universidad no tendrá que invertir en doble licenciamiento de los controladores sino hacer un solo gasto en el controlador. En la figura 3.10 podemos ver un diagrama lógico de lo que sería el esquema de controlador redundante.

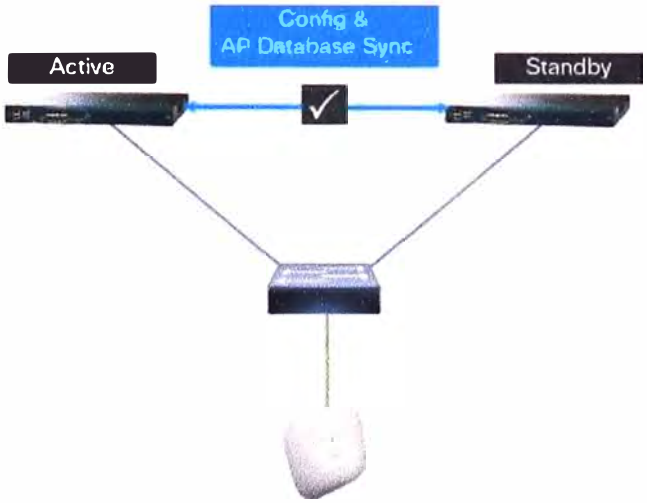


Fig. 3.10 Controladores desplegados en redundancia

3.6.2.d) Control de Acceso a la Red basado en Contexto

Para poder controlar el acceso de usuarios y dispositivos a la red necesitamos contar con un equipo de seguridad al que se consulte los permisos que tienen un usuario y dispositivo que intenta ingresar a la red; dicho equipo de seguridad debe tener configuradas políticas definidas de acuerdo a la realidad de la universidad. Dentro de las tecnologías manejadas por Cisco, la solución propuesta es el Cisco Identity Services Engine, ISE.

El punto de partida para definir el contexto es definir el tipo de usuario y dispositivo que puede acceder a la red. En tal sentido el usuario puede ser corporativo o no corporativo. En caso sea un usuario corporativo se refiere a un estudiante, docente o personal administrativo de la universidad; en caso sea un usuario no corporativo se refiere a algún proveedor externo o persona que está de visita en la universidad. Siguiendo la misma lógica, los dispositivos pueden ser corporativos o no corporativos. En caso sea un dispositivo corporativo se refiere a una PC o laptop instalada en alguna sala de estudio o sala de profesores de la universidad, también dentro de la universidad se está dando el servicio de préstamo de iPads para que los estudiantes accedan al material bibliográfico digital de la universidad desde cualquier locación dentro de la universidad a través este dispositivo móvil; en caso sea un dispositivo no corporativo se refiere a cualquier otro dispositivo, en su mayoría dispositivos móviles tipo teléfonos inteligentes, tablets o laptops, que los usuarios sean corporativos o no portan consigo e intentan acceder a la red de la universidad usando estos dispositivos. En la figura 3.11 podemos ver a manera de resumen los tipos de usuario y dispositivo divididos en cuatro cuadrantes. El punto central que es el cerebro que se encarga de otorgar permiso y ejecutar las políticas de seguridad es el Identity Services Engine, ISE.

Fig. 3.11 Tipos de usuarios y dispositivos que pueden acceder a la red

Todos los usuarios corporativos, que están conformados por los estudiantes, docentes y personal administrativo de la universidad están registrados en el directorio activo de la

universidad, los usuarios que no estén registrados en el directorio activo y por tanto no tienen un nombre de usuario predefinido, serán usuarios no corporativos. Todas las PC y laptop de la universidad registrados como dispositivos corporativos están también en el directorio activo y las iPad serán reconocidas por un certificado que se instalara desde el Identity Services Engine, ISE. Los demás dispositivos que no estén registrados serán reconocidos como dispositivos no corporativos.

Para terminar de definir el contexto, falta definir el dónde, cuándo y cómo. Para acceder a los recursos de la universidad se debe acceder desde el campus universitario de Monterrico de la universidad. En esta primera etapa no se tomará en cuenta las oficinas remotas ubicadas en otros distritos de Lima y provincias con el objetivo de acotar el alcance y revisar que todo marche correctamente en la sede central. Además de la sede central de Monterrico también se permitirá el acceso vía VPN de los docentes cuando quieran acceder vía una VPN de tipo acceso remoto; como una segunda etapa se integrará a esta solución las oficinas remotas de la universidad.

Se permitirá acceder a los recursos de información de la universidad en cualquier momento en esta primera etapa de despliegue de la solución.

Las formas de conectarse a la red de la universidad pueden ser a través de un cable de cobre, a través de la red inalámbrica corporativa y a través de una conexión VPN de tipo acceso remoto (solo para docentes).

Ahora que ya tenemos definido el contexto de acceso a la red, el siguiente paso es establecer la política de acceso a la red y para ello utilizaremos un diagrama de flujo donde se tiene como punto de partida un usuario que intenta ingresar a la red, siguiendo el diagrama de flujo se determinará el contexto de acceso del usuario y dependiendo de este contexto se le otorgará acceso a determinada información.

Dentro de los servicios adicionales que se pueden entregar a la red usando el Identity Services Engine, podemos citar:

- **Autoaprovisionamiento de Dispositivos Personales**

Este servicio permite al departamento de IT no preocuparse por registrar cada nuevo dispositivo no corporativo que ingresa a la red ya que quien se encarga de enrolar el dispositivo a la red es el mismo usuario final, sea corporativo o no corporativo.

Cuando un dispositivo no corporativo intenta conectarse a la red se le redirige a un portal donde se debe ingresar los datos del dispositivo y asociarlos al usuario que intenta ingresar a la red. El departamento de TI de la universidad puede limitar la cantidad dispositivos permitidos por usuario. Se plantea limitar a 3 la cantidad de dispositivos que pueden ser registrados por cada usuario, al cuarto dispositivo que se intente registrar no se le dará acceso.

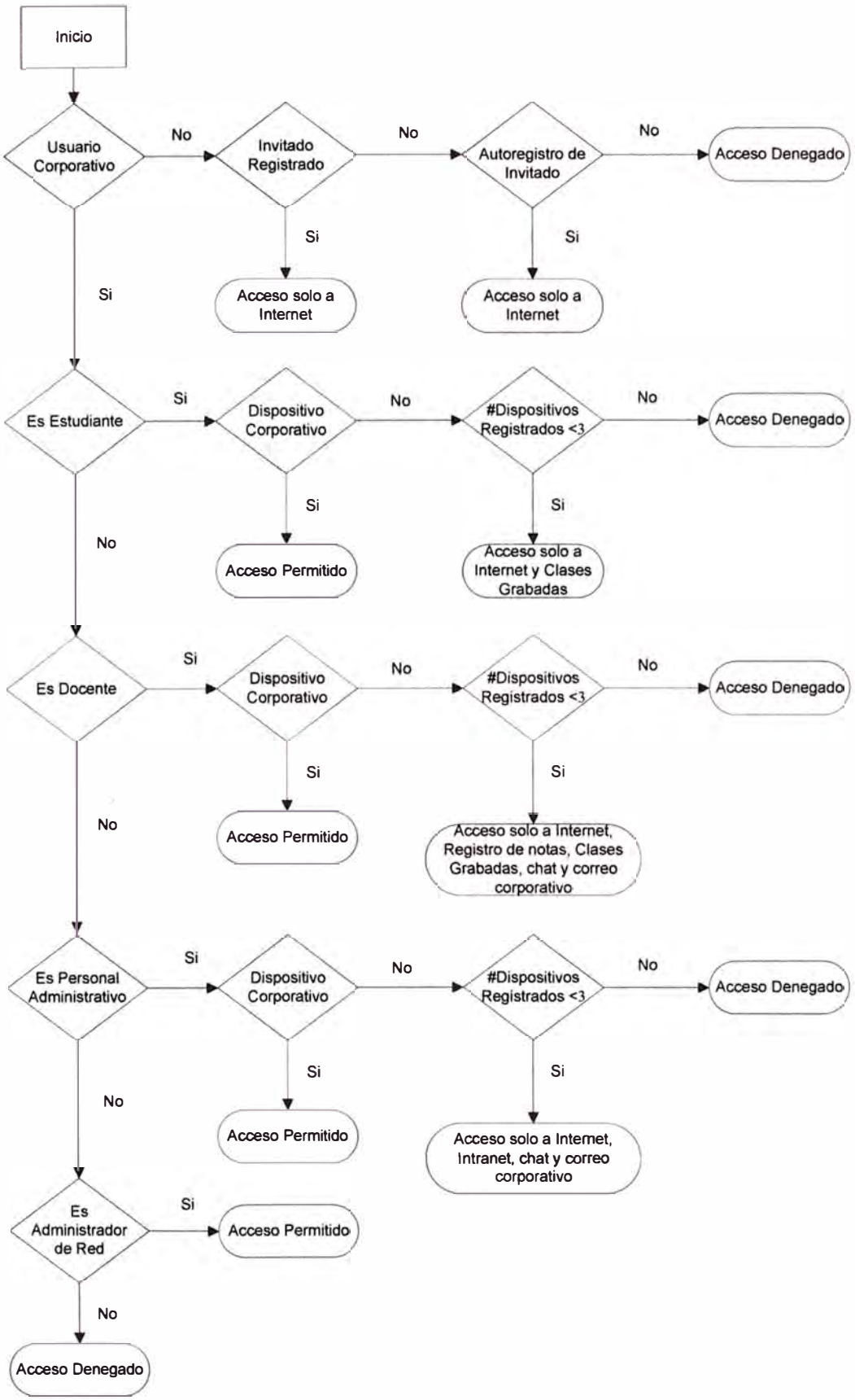


Fig. 3.12 Política de acceso dependiente del contexto

En caso que un usuario haya perdido su dispositivo personal o haya sido robado, el usuario podrá acceder al portal donde registro sus dispositivos para suspender el

dispositivo extraviado hasta que sea encontrado o eliminarlo en caso lo de por perdido. De esta manera si otros usuarios intentan ingresar a la red mediante este dispositivo, el ISE bloqueara su acceso.

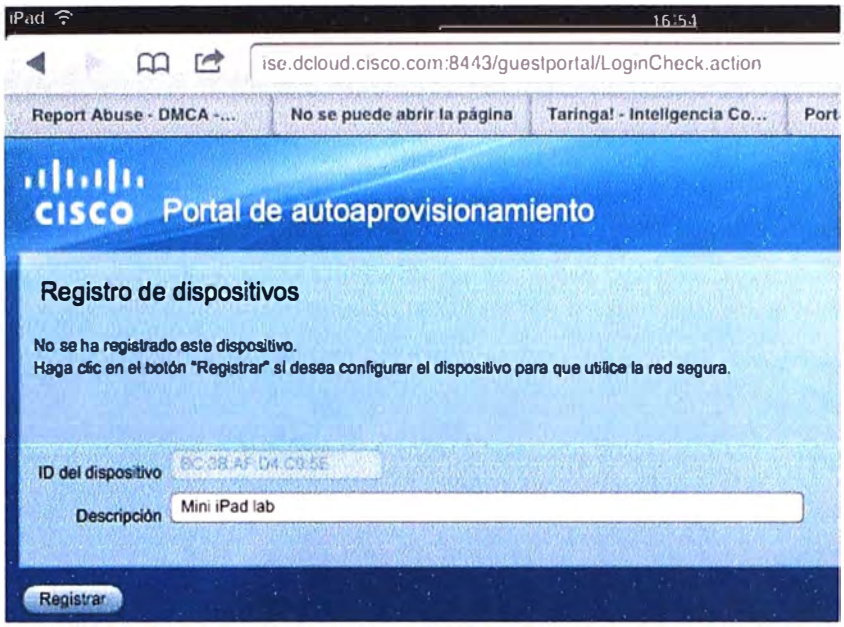


Fig. 3.13 Interface del portal de autoaprovisionamiento

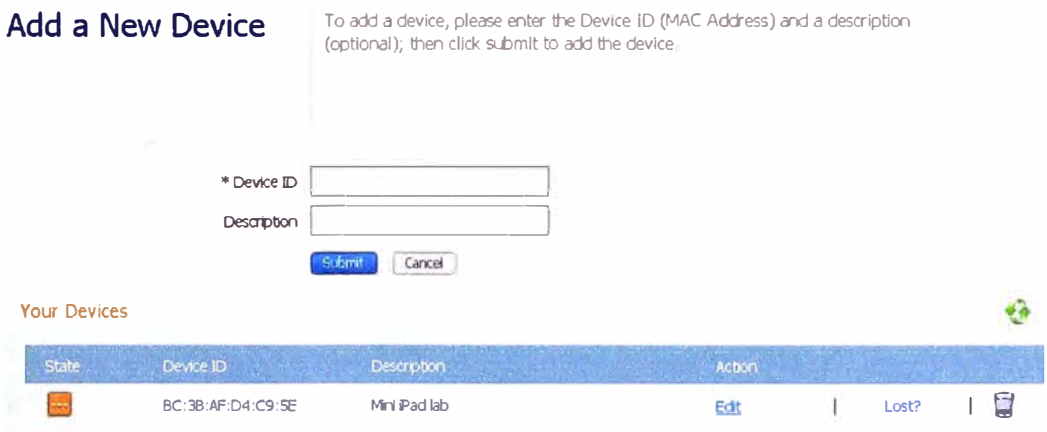


Fig. 3.14 Interface de dispositivos registrados

- **Perfilamiento de Dispositivos**

El perfilamiento es una capacidad del Identity Services Engine, ISE, para clasificar dinámicamente cada dispositivo que se conecta a la red. De esta manera logramos tener visibilidad de todos los dispositivos que están conectados a la red independiente de la identidad del usuario, es mas también se incluyen los dispositivos que no tienen usuarios tipo impresoras u otros.

La primera fase del perfilamiento sucede en los switches y en los puntos de acceso que son a donde se conectan los dispositivos de usuario final, estos switches y puntos de acceso recolectan información del dispositivo conectado y envían toda esa información al ISE. La segunda fase es que el ISE reconozca el dispositivo conectado y lo clasifique de

acuerdo a las categorías que tiene pre configuradas de fábrica. Y como último punto el ISE aplica la política definida para ese dispositivo como por ejemplo ponerlo en una VLAN para que pueda comunicarse. En la figura 3.15 se grafican los pasos que siguen el ISE para realizar el perfilamiento.

Fig. 3.15 Pasos para el perfilamiento de dispositivos

- **Control de Acceso a Invitados**

El servicio de acceso a la red para invitados, es decir, usuarios no corporativos usando dispositivos no corporativos, sirve para restringir el acceso de estas personas solo a internet y que no puedan acceder a los recursos internos y/o confidenciales de la universidad. Existen dos formas de brindar acceso a los invitados:

1. Un usuario corporativo genera un usuario y password invitado mediante un portal de sponsor. Luego, estas credenciales son entregadas al invitado vía mensaje de texto, vía escrito o vía un correo compartido con anterioridad para que al momento de que el usuario invitado intenta entrar a la red use estas credenciales. En la figura 3.16 se muestra un ejemplo de este portal de sponsor.
2. El mismo usuario invitado genera sus credenciales mediante el acceso a un portal de autoprovisionamiento de acceso a la red. Esta funcionalidad debe ser habilitada por el administrador del Identity Services Engine, ISE. En la figura 3.17 se muestra un ejemplo de este portal de autoprovisionamiento.

Para cualquiera de los casos, el administrador del ISE puede definir las siguientes políticas de acceso de invitado:

1. Tiempo de vigencia del usuario y password generado ya sea autoprovisionado o mediante un sponsor.

2. Los formatos (mayúsculas, signos, números, etc.) que deben tener el usuario y password que usaran los usuarios invitados.

3. Acuerdo de términos de uso que deberá ser aceptado por el usuario invitado cuando ingrese a la red para que cumpla los términos de uso definidos dentro de la universidad.

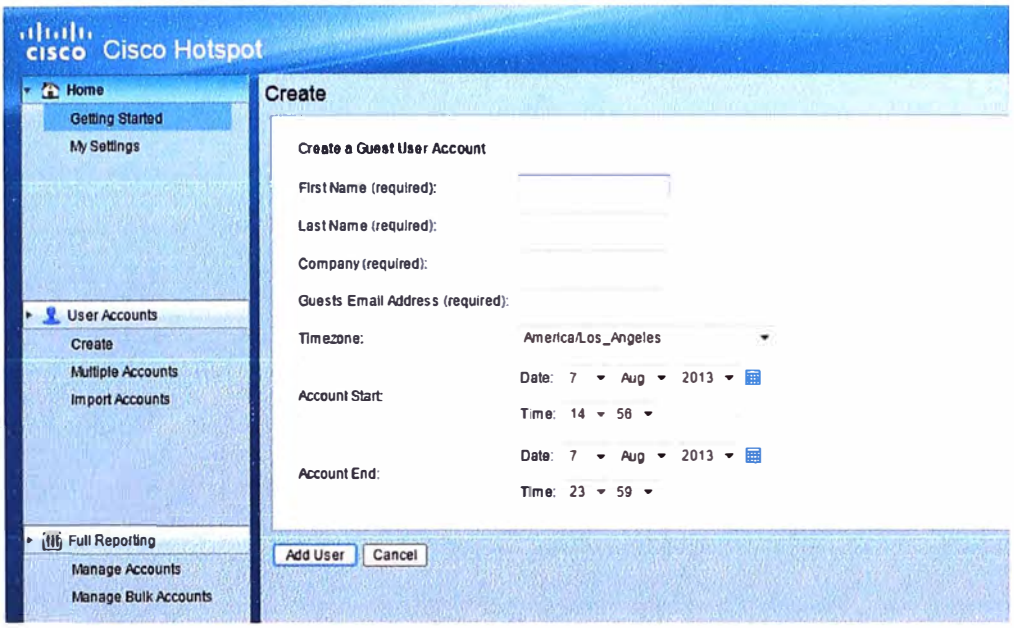
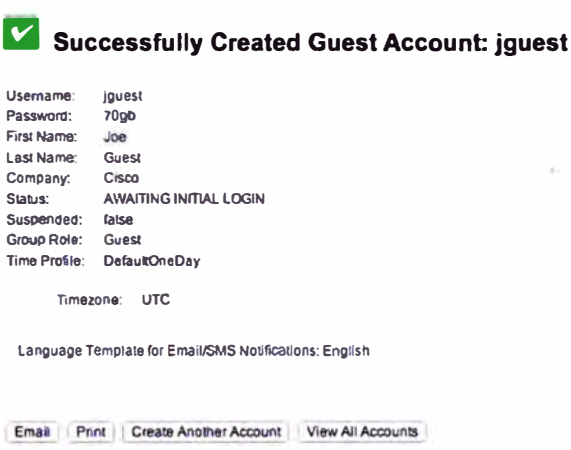


Fig. 3.16 Portal de sponsor

Creación de usuario invitado



Cuenta creada

Fig. 3.17 Portal de autoaprovisionamiento de invitado

3.6.2.e) Gestión Unificada de Red

Hasta este punto tenemos la red cableada en redundancia, la red inalámbrica cubriendo todo el campus y con redundancia en el controlador, hemos implementado la seguridad mediante el control de acceso de usuarios y dispositivos a la red. Con todo esto la red ha crecido con nuevos servicios y nuevos dispositivos que se unirán de manera segura, ahora para simplificar la tarea del departamento de TI es necesario contar con una herramienta de software que nos permita gestionar tanto la red cableada como la red

inalámbrica desde un solo punto de gestión y los servicios que entrega toda esta infraestructura de red hacia los usuarios finales. En la marca Cisco, el software único de gestión de red para entornos de LAN es el Cisco Prime Infrastructure. Es importante resaltar que este software de gestión tiene dos modos de instalación, el primero es con un hardware dedicado a correr este software de gestión y el otro modo es mediante una máquina virtual; para la UPC se recomienda usar la versión virtual ya que se cuenta con servidores compatibles con este software y con la capacidad de hardware suficiente para soportar hasta 500 dispositivos administrados.

Las características de este software de gestión se pueden dividir en tres grandes bloques:

- **Administración de Red**

Dentro de los principales beneficios que presenta este software de gestión de red, podemos citar:

1. Gestión convergente para facilitar la supervisión, la resolución de problemas y la generación de informes. Los dispositivos de red se gestionan usando el protocolo SNMP, soportado en sus versiones 1, 2c y 3, tanto para dispositivos de red cableada como inalámbrica. El uso del protocolo SNMP permite administrar dispositivos que no sean de la marca Cisco como pueden ser los switches 3com que tiene la universidad.
2. Monitoreo continuo de los dispositivos de red con la capacidad de generar alarmas para que los administradores de red estén alerta frente a cualquier cambio que exista en la red. Se pueden definir niveles de severidad en las alarmas y configurar acciones a tomar automáticamente.
3. Mejores capacidades de gestión de la configuración de los dispositivos mediante una consola gráfica, modificaciones de grupos de configuraciones en dispositivos con características idénticas, menor probabilidad de error al realizar las configuraciones en grupo y mediante la verificación automática de la configuración.
4. Reportes detallados y topología completa de toda la infraestructura de red. Nos permite tener un inventario y en caso de que se tengan versiones de software más actuales poder realizar las actualizaciones en línea desde la consola grafica de la herramienta de gestión.
5. En caso de que un dispositivo presente fallas de hardware, el software de gestión tiene la inteligencia para abrir un caso de soporte en la web de Cisco y debido a que toda la infraestructura de red es Cisco logramos conseguir tiempos de respuesta cortos ante el evento de una falla de hardware.
6. Mediante este software de gestión podemos configurar fácilmente los protocolos avanzados que Cisco incluye en sus dispositivos de red. Sin esta herramienta de gestión, dichos protocolos avanzados podrían significar muchas horas hombre invertidas,

entrenamiento y hasta posibilidad de cometer errores por ello es muy importante resaltar este valor diferencial de la solución.

7. Específicamente para los equipos inalámbricos podemos tener un mapa de calor donde se muestra la cobertura y el nivel de señal que entrega cada punto de acceso y de esta forma poder tomar medidas correctivas o de mejora donde no se tenga una buena cobertura.

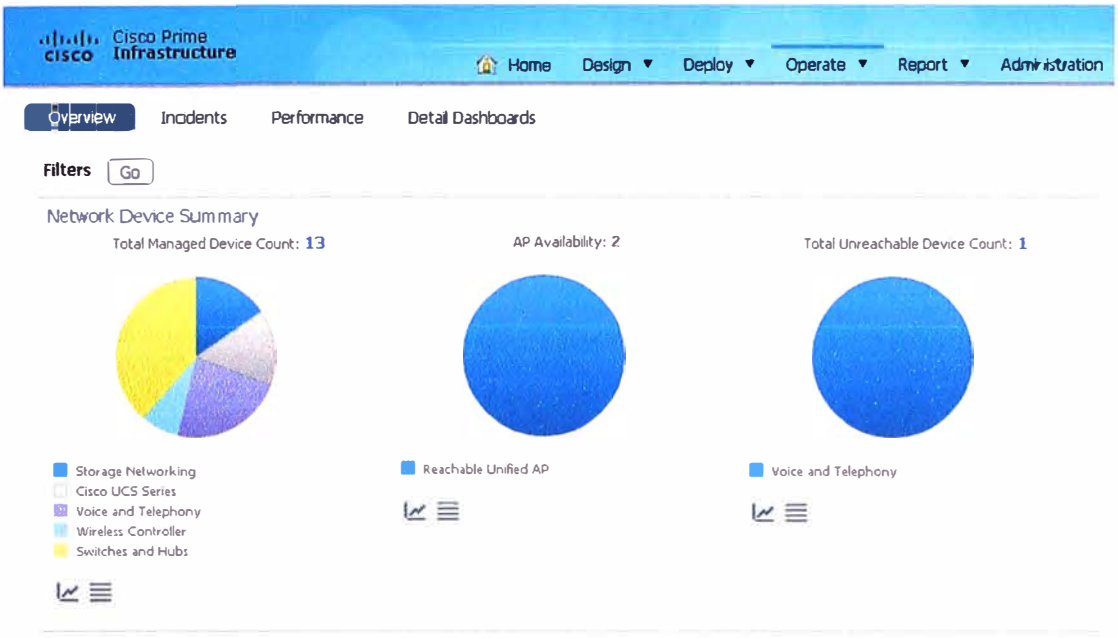


Fig. 3.18 Consola gráfica del Cisco Prime Infrastructure

- **Monitoreo de la Experiencia del Usuario**

El Prime Infrastructure es una herramienta de gestión avanzada que no solo se encarga de la gestión de los dispositivos de red como tradicionalmente se hace en forma de cajas separadas sino que se centra en el servicio que se entrega al usuario final. En tal sentido se tienen las siguientes características.

1. Maneja una interface gráfica donde se presentan los dispositivos asociados a cada usuario y se pueden separar de acuerdo a la locación del usuario. También se encuentran estadísticas del tráfico que cursa por cada dispositivo y se pueden filtrar intervalos de tiempo donde se necesite analizar el comportamiento de las aplicaciones por ejemplo debido a alguna caída en el servicio o saturación. A esta capacidad Cisco le llama visión 360 de la experiencia de usuario final.

2. Permite monitorear el tráfico que cursa por las interfaces de los dispositivos de red tales como switches y routers con el objetivo de tener visibilidad del uso del ancho de banda y los retardos que se manejan dentro de la red LAN y así poder tomar acciones correctivas antes que surjan problemas de saturación de red.

3. Permite monitorear tráfico de voz y video en tiempo real tanto a nivel de oficina remota como a nivel de cada usuario final.

4. Debido a que cuenta con un resumen de los servicios a los que accede un usuario desde cada uno de sus dispositivos, se logra integrar con el Identity Services Engine para entregar una sola experiencia de acceso al usuario, no sólo de reconocimiento y aplicación de políticas sino de control y monitoreo de los servicios a los accede.

Fig. 3.19 Visión 360 de la experiencia del usuario final

- **Cumplimiento de las Normas**

El software de gestión tiene un módulo que permite hacer una auditoría a la red mediante procesos predefinidos que se aplican sobre los dispositivos y servicios reconocidos previamente. Si los dispositivos no pasan la auditoría en forma satisfactoria, el software tiene la capacidad de sugerir los cambios necesarios para hacer cumplir al dispositivo con la norma, dependerá del administrador de red que acepte o deniegue los cambios.

1. El cumplir con estándares de seguridad ayuda a las organizaciones a lograr un menor coste total de oportunidad, ya que si no cumplieran el estándar es más probable caer ante un ataque informático y por tanto no dar servicio a los usuarios de red. En el caso que se tenga un ataque al momento de las matrículas de los estudiantes podría significar una perdida

2. Los estándares soportados son PCI, HIPAA, CIS, DHS, DISA, NSA, SANS, SOX, ISO17799 y Cisco SAFE, que permiten contar con una red confiable.

3. Se cuenta con plantillas de configuración recomendadas por el fabricante. Dicha información responde a la experiencia que tiene el fabricante a lo largo de los más de 25 años en el mercado.

3.7 Recursos humanos y equipamiento

Dentro de los criterios de evaluación se tuvo en cuenta el conocimiento de las tecnologías presentes en la solución y se optó por la solución propuesta debido a que el personal con

el que cuenta actualmente la universidad tiene amplia experiencia en productos de la marca Cisco, por tanto será la misma universidad a través del departamento de sistemas, el encargado de desplegar y monitorear estas mejoras.

Dentro del departamento de sistemas de la universidad, el equipo de trabajo responsable de desplegar esta solución es el área de redes constituido por el jefe del área, un coordinador y dos analistas, esta conformación se muestra en la figura 3.20.

Fig. 3.20 Organigrama del Área de Redes de la UPC

A continuación se detallan brevemente las funciones de cada miembro del área de redes:

o Jefe de Infraestructura y Plataforma de TI, es la persona responsable del área y encargado de recomendar las soluciones para mejorar el desempeño de la red. Se encarga de planificar los cambios tecnológicos concernientes a la conectividad de red.

o Coordinadora de Redes y Comunicaciones, es la persona con mayor rango de certificaciones en tecnología y responsable del área de redes cuando el jefe está de viaje. Además se encarga de coordinar tareas que involucren trabajo conjunto con otras áreas del departamento de TI como servidores y plataforma web. Apoya al jefe en la planificación del área y a los analistas en la ejecución, cuando la situación es muy compleja y lo amerita.

o Analista de Redes y Comunicaciones, son las personas encargadas de implementar las nuevas soluciones y monitorear el correcto funcionamiento de los servicios de red. En caso que se presenten problemas de conectividad son ellos los encargados de dar solución inmediata.

Un beneficio adicional de la marca Cisco es que cuenta con gran información de sus productos y soluciones publicada en su página web www.cisco.com por lo que el primer nivel de escalación en caso de presentarse alguna dificultad en el despliegue es visitar la página web del fabricante. Dentro de la solución propuesta se tendrá en cuenta el costo de los servicios de soporte del fabricante para cada dispositivo, esto le permitirá a la universidad tener soporte directo de la marca vía la apertura de tickets de atención a través del Centro de Asistencia Técnica, Cisco TAC, y poder tener asistencia remota de un ingeniero certificado Cisco; otro beneficio importante de contratar este soporte es que se podrá tener acceso a las actualizaciones de software que surjan durante la duración del contrato de servicios.

Respecto al equipamiento necesario para el despliegue de la solución, vamos a tomar en cuenta las cantidades, el licenciamiento de cada equipo y el soporte a contratar. En la tabla 3.8 vemos este dimensionamiento.

Para el controlador 5508 estamos considerando el licenciamiento modo redundante debido a que la universidad ya cuenta con un controlador idéntico, este controlador se encargara de dar redundancia.

En el control de acceso el servidor donde reside ISE tiene capacidad para soportar hasta 20000 dispositivos concurrentes, como primera fase se licenciara los dispositivos inalámbricos, actualmente se tienen registro de 5000 dispositivos inalámbricos que se conectan, se asegurara un crecimiento del 20% debido a que con las mejoras en la red inalámbrica se tendrán más usuarios que atender, corporativos y no corporativos, por lo tanto la cantidad de licencias que necesitamos es de 6000 dispositivos inalámbricos concurrentes. A futuro, para poder controlar el acceso de dispositivos cableados se tendría que agregar una licencia de actualización.

El software de gestión está pensado para cubrir la cantidad total de puntos de acceso y switches de la red.

Tabla Nº 3.8 Equipamiento necesario para el despliegue de la solución

EQUIPO	CANTIDAD	LICENCIAMIENTO	SOPORTE
Switch Catalyst 4500 incluye Modulo supervisor y de Puertos	1	No necesita	Por 3 años 24x7x4
Controlador Inalámbrico 5508	1	Modo Redundante	Por 3 años 24x7x4
Punto de Acceso 3600	100	No necesita	Por 3 años 24x7x4
Seguridad para el Acceso Secure Network Server 3495	1	6000 dispositivos inalámbricos concurrentes	Por 3 años 24x7x4
Gestión Unificada de Red Prime Infrastructure 1.3	1	200 dispositivos de red	Por 3 años 24x7x4

CAPITULO IV
PRESENTACIÓN DE LA PROPUESTA

4.1 Presupuesto y tiempo de ejecución

En esta sección revisaremos los costos de adquirir los equipos presentados en la solución, se tomara un descuento del 30% sobre el precio de lista para obtener los precios que le costaría la solución a la universidad, este nivel de descuento es aproximado y debe tomarse una variación de ±3%, el valor exacto se definiría mediante una orden de compra en coordinación con un representante comercial de la marca Cisco. Los costos de implementación están cubiertos totalmente por el trabajo que realizarían los ingenieros del área de redes de la UPC, además tomaremos en cuenta el costo de un curso oficial de Cisco para capacitar al personal de la universidad en la configuración del Identity Services Engine, que es el componente principal de la solución, se tomará en cuenta 3 vacantes para este curso. En la tabla 4.1 se muestran los costos de cada componente descrito en este informe y vemos que el precio total de adquirir esta solución es de 379,463.18 dólares americanos.

Esta solución al ser totalmente modular le da la flexibilidad a la universidad de poder hacer la inversión por fases hasta llegar a completar todos los componentes de acuerdo al presupuesto que maneje la universidad. Los componentes que son la base de esta solución son la plataforma de switching y wireless, estos componentes deben ser los primeros en ser adquiridos y optimizados, sobre esta base sólida entra el Cisco Identity Services Engine a dar la solución de control de acceso basado en contexto para los usuarios finales. Y finalmente para cubrir todo el despliegue como si fuera un paraguas que cubre toda la red entra el Cisco Prime Infrastructure para la gestión unificada de la red.

Respecto a los tiempos de ejecución, tomaremos en cuenta la duración cada tarea en días para establecer el cuadro de trabajo, entiéndase un día como 8 horas de trabajo. Queda en total potestad de la universidad el definir las horas de trabajo diarias que le dedique a este proyecto. Se puede observar, en la tabla 4.2, que el despliegue de esta solución nos tomaría aproximadamente dos meses ser implementada en su totalidad, lo cual es un tiempo aceptable para la universidad y va acorde con los objetivos que buscan en el corto plazo.

Tabla Nº 4.1 Propuesta económica de la solución planteada

NÚMEROS DE PARTE	DESCRIPCIÓN	CANTIDAD	PRECIO DE LISTA	PRECIO TOTAL	DSCTO	PRECIO DE VENTA
WS-C4507R+E	Switch Catalyst 4500 incluye modulo supervisor y de puertos	1	126,738.26	126,738.26	0.30	88,716.78
AIR-CT5508-HA-K9	Controlador Inalámbrico 5508	1	38,646.75	38,646.75	0.30	27,052.73
AIR-CAP3602I-A-K9	Punto de Acceso 3600	100	1,891.00	189,100.00	0.30	132,370.00
SNS-3495-M-ISE-K9	Seguridad para el Acceso Secure Network Server 3495	1	149,178.39	149,178.39	0.30	104,424.87
R-PI12-K9	Gestion Unificada de Red Prime Infrastructure 1.3	1	28,784.00	28,784.00	0.30	20,148.80
ISE Presencial (CI-ISE)	Implementing Cisco Identity Service Engine Secure	3	3,000.00	9,000.00	0.25	6,750.00
					TOTAL	379,463.18

Tabla Nº 4.2 Tiempos de Implementación de la solución propuesta

TAREA	DURACIÓN (DÍAS)
Optimización de la Red LAN	10
Unificación de la Red Académica y la Red Administrativa	4
Optimización de la Red Inalámbrica	12
Mejoras en la Red LAN	6
Mejoras en la Red Inalámbrica	16
Despliegue de Control de Acceso basado en Contexto	13
Despliegue del Software de Gestión de Red Unificado	5
	66

CONCLUSIONES Y RECOMENDACIONES

1. Tal como se indica a lo largo del desarrollo de este informe, las tecnologías de información permiten encontrar nuevas formas para el proceso de aprendizaje mediante el acceso a nuevas formas de estudio y a información académica cada vez más abundante. Este proceso de aprendizaje al ser potenciado también es controlado con la seguridad descrita basada en contexto y de esta manera se asegura que la entrega de información se realiza a la persona correcta y de una forma segura sin temor a fugas de información y sin comprometer la experiencia de los estudiantes, docentes y trabajadores de la universidad.
2. Al tomar como referencia el contexto de acceso, y no solo la autenticación de usuario, para asignar privilegios de acceso a los recursos de información se asegura que la información llegara a la persona correcta y no se tendrán ataques ni robo de información.
3. La integración avanzada entre el sistema de control de acceso basado en contexto y la herramienta de gestión única para toda la red, forman la base para una única visión de red donde la seguridad va de la mano con la gestión dando como resultado un entorno más confiable y fácil de adaptarse a los cambios.
4. Con la optimización de la red se logra que los usuarios consigan una mejor experiencia para el aprendizaje con anchos de banda mayores que aseguren el uso de video en alta definición sobre una red inalámbrica y con la alta disponibilidad que se necesita para acceder a información en todo momento.
5. La utilización de la plataforma Cisco permite para los administradores de red desplegar la solución en menor tiempo debido al conocimiento previo de esta plataforma, con menor probabilidad de error y eliminar labores tediosas y repetitivas como tener que dar soporte a cada persona que intenta acceder a la red de la universidad. Para los estudiantes, docentes y trabajadores les permite interactuar con interfaces de usuario sencillas e intuitivas para gestionar sus dispositivos personales y poder dar acceso a invitados.
6. En caso se vea la necesidad de realizar algún cambio en algún componente de la solución e incluso cambiar un componente completo, se debe considerar tiempos de holgura en cada una de las etapas que permitan manejar estos eventuales cambios que

se presenten, asimismo las capacitaciones oportunas al personal en caso de no contar con el conocimiento.

7. El fabricante Cisco System cuenta con un amplio portafolio de productos de tecnología basada en IP que logran integrarse para dar una solución y/o servicio superior. Esto permite agregar valor a las redes y hacer que las organizaciones sean cada vez más eficientes. Debido a esto es recomendable revisar las innovaciones que presenta esta marca para poder a futuro integrar nuevas soluciones sobre la base establecida en este informe y así lograr beneficios superiores y nuevos servicios para la mejora de la enseñanza. Servicios como telepresencia y/o videoconferencias en alta definición para clases a distancia podrían ser servicios a implementar en el corto plazo sobre la red optimizada y segura que se tiene en la actualidad.

8. La solución descrita en este informe cuenta con interfaces de gestión graficas simples e intuitivas, esto facilita un manejo visual mejor para el administrador de red. Sin embargo conforme salgan las nuevas versiones de software estas interfaces pueden cambiar parcialmente agregando nuevas funcionalidades dentro de los equipos, por ello se recomienda familiarizarse al máximo para mejorar los procesos que se realicen empleando esta solución de modo que se reduzcan los tiempos de respuesta en caso que se presente algún cambio.

9. Antes de la implementación de la solución se debe realizar un back up de las configuraciones de todos los equipos, switches y controlador inalámbrico, para poder hacer rollback de la configuración en caso de que suceda algún hecho inesperado, por ejemplo que se corte la electricidad antes de terminar la configuración de los equipos. Adicionalmente se debe realizar un test de la red a nivel de tiempos de respuesta y ancho de banda de los usuarios antes de la implementación de la solución para luego poder contrastar los resultados y ver los beneficios obtenidos.

10. Todas las configuraciones que se realicen deben ser documentadas para que facilite el entendimiento de cualquier persona que necesite conocer de esta solución e incluso para nuevo personal que se contrate a futuro.

11. Es muy importante tener los diagramas físicos y lógicos debidamente actualizados donde se muestren al menos los segmentos IP usados, las interfaces por las que se conectan los dispositivos, los SSID de las redes inalámbricas y las VLAN. Esto servirá para poder entender como está organizada la red y poder realizar cambios con rapidez y facilidad. Todo cambio futuro debe ser también documentado.

12. Documentar las configuraciones de los switches con los comandos, “show running-config” para guardar la configuración del equipo, “show versión” para guardar la versión

de software usado, "show module" en caso de equipos modulares para guardar la información sobre los módulos supervisor y de puertos.

13. Además de las configuraciones es muy importante guardar las imágenes de los sistemas operativos y software que usemos para en caso de falla de hardware se reemplace y se use la el mismo software.

14. Si bien la solución económica plantea desplegar el ISE solo para los dispositivos inalámbricos, se debe tener en cuenta que la solución también puede controlar el acceso para dispositivos cableados, solo bastaría agregar la licencia wireless upgrade.

ANEXO A

Criterios de Diseño de una Red Inalámbrica Wifi en un Entorno Educativo

1. Establecer y validar los requisitos de ancho de banda por cada conexión

En la tabla A.1 se muestran se muestran los requerimientos promedio de ancho de banda para aplicaciones bastante conocidas dentro de un entorno convencional y dentro de un entorno educativo.

Tabla Nº A.1 Requerimientos de ancho de banda por aplicación

APLICACIÓN POR CASO DE USO	VELOCIDAD DE TRANSMISIÓN PROMEDIO
Web – Convencional	500 Kbps
Web – Educativo	1 Mbps
Audio – Convencional	100 Kbps
Audio – Educativo	1 Mbps
On-demand or Streaming Video - Convencional	1 Mbps
On-demand or Streaming Video – Educativo	2-4 Mbps
Printing	1 Mbps
File Sharing – Convencional	1 Mbps
File Sharing – Educativo	2-8 Mbps
Device Backups	10-50 Mbps

Los valores numéricos presentados son referenciales, para estar seguros al 100% es mejor realizar un test de velocidad con las aplicaciones que necesitemos usar en el medio inalámbrico. Adicionalmente tener en cuenta que las velocidades de transmisión dependen también del dispositivo que se conecta a la red, por ejemplo una aplicación web que requiere 100Kbps al acceder usando una laptop vía Internet Explorer puede requerir más ancho de banda al acceder desde un teléfono inteligente o una Tablet.

Una vez conocido el ancho de banda requerido por aplicación se puede determinar el ancho de banda agregado requerido en la cobertura del área de la red inalámbrica.

2. Cálculo del Ancho de Banda Agregado para cubrir un área

Para el cálculo del ancho de banda agregado debemos tomar en cuenta que en los entornos educativos los usuarios portan consigo en promedio 3 dispositivos inalámbricos y cada uno de estos dispositivos establecerá una conexión, el número total de conexiones que se establezcan en el medio inalámbrico nos ayudará a determinar el ancho de banda agregado.

Lo que le preocupa al usuario es el ancho de banda que requieren sus aplicaciones para lograr una buena experiencia. Del lado de la red debemos cuidar que la velocidad con que se transporta la información en el aire pueda cubrir la expectativa que tiene el usuario en su aplicación. Las distintas versiones de los protocolos definidos en 802.11 establecen

diferentes velocidades de transmisión en el medio inalámbrico, estas velocidades de transmisión toman en cuenta el total de información que se envía, cabecera (bits de control) más carga útil, lo que le interesa al usuario final es la velocidad de transmisión de la carga útil en el medio inalámbrico ya que es ahí donde se transmite la información de su aplicación. En la tabla A.2 vemos la velocidad total que entrega cada protocolo 802.11 en la columna "Data Rate", la velocidad que entrega el protocolo para la carga útil se muestra en la columna "Aggregate Throughput". Tomando una cantidad de usuarios de muestra podemos calcular la velocidad que entrega la red a cada usuario, estos valores se muestran en la columna "Throughput Promedio por Usuario".

Tabla Nº A.2 Velocidades dentro de los estándares 802.11

PROTOCOLO	DATA RATE (MBPS)	AGGREGATE THROUGHPUT (MBPS)	CANTIDAD DE USUARIOS	THROUGHPUT PROMEDIO POR USUARIO
802.11b	11	7.2	10	720 Kbps
802.11b	11	7.2	20	360 Kbps
802.11b	11	7.2	30	240 Kbps
802.11b/g	54	13	10	1.3 Mbps
802.11b/g	54	13	20	650 Kbps
802.11b/g	54	13	30	430 Kbps
802.11a	54	25	10	2.5 Mbps
802.11a	54	25	20	1.25 Mbps
802.11a	54	25	30	833 Kbps
802.11n MCS7	72	35	10	3.5 Mbps
802.11n MCS7	72	35	20	1.75 Mbps
802.11n MCS7	72	35	30	1.16 Mbps

BIBLIOGRAFÍA

[1] Zeb Hallock, John Johnston, Fernando Macias, Roland Saville, Srinivas Tenneti, Mike Jessup, Suyog Deshpande, Tim Szigeti "Cisco Bring Your Own Device (BYOD) CVD Release 2.5", Cisco Systems – Estados Unidos, 2013

[2] Mark Ciampa, "CWNA Guiteto Wireless LANs, Third Edition", Course Technology CENGAGE Learning – Estados Unidos, 2013

[3] Jim Florwick, Jim Whiteaker, Alan Cuellar Amrod, Jake Woodhams, "Wireless LAN Design Guide in Higher Education", Cisco Systems – Estados Unidos, 2012

[4] Cisco Smart Business Architecture, "LAN Design Overview", Cisco Systems – Estados Unidos, 2012

[5] Kevin Roebuck, "Network Access Control", Estados Unidos, 2011

[6] David Hucaby, "CCNP SWITCH Official Certification Guide", Cisco Systems – Estados Unidos, 2010

[7] Kevin Wallace, "CCNP TSHOOT Official Certification Guide", Cisco Systems – Estados Unidos, 2010

[8] Información pública de los productos en la página web de 3COM

3COM Switch 5500 10/100 Family Data Sheet

[9] Información pública de los productos en la página web de Cisco Systems

Cisco Identity Services Engine www.cisco.com/go/ise

Cisco Prime Infrastructure www.cisco.com/go/primeinfrastructure

Cisco Wireless Architecture www.cisco.com/go/wireless