ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

ANÁLISIS Y DISEÑO DE REDES MÓVILES AD-HOC

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ARTURO MAURICIO GARCÉS RUIZ
JUAN PABLO ZALDUMBIDE PROAÑO

DIRECTOR: PhD. ENRIQUE MAFLA

Quito, Septiembre 2007

DECLARACIÓN

Nosotros, Arturo Mauricio Garcés Ruiz y Juan Pablo Zaldumbide Proaño, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Arturo Mauricio Garcés Ruiz	**Juan Pablo Zaldumbide Proaño**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Arturo Mauricio Garcés Ruiz y Juan Pablo Zaldumbide Proaño, bajo mi supervisión.

PhD. Enrique Mafla
DIRECTOR DE PROYECTO

DEDICATORIA

A mi mami, padre, hermanos, primos, familiares y amigos.

Juan Pablo

A mis padres, Arturo y Anita, quienes con su apoyo incondicional, confianza, ejemplo y amor han sido los mentores de todos mis logros y éxitos.

A mis hermanos Cristian y María Isabel por su confianza y ayuda.

Mauricio

AGRADECIMIENTOS

Agradezco a mi mami que con su cariño, paciencia y amor me ha apoyado en las buenas y malas a lo largo de mi carrera.
A mi padre que con sus consejos y cariño me ha enseñado que no hay que rendirse en el camino y culminar lo que has empezado.
A mi ñaño Javi que con su cariño y protección me ha mostrado que las carreras no son de velocidad sino de resistencia.
A mi ñaño Mateo que con su alegría me ha impulsado a seguir adelante cada día.
A mi primo por su apoyo y amistad cada día.
A mis abuelitas por brindarme amor y a toda mi familia por darme su apoyo.

Juan Pablo

Agradezco a Dios por haberme bendecido con una familia maravillosa.
A mis padres, por creer en mí, en cada desafío y momento de mi vida, por su ejemplo de persistencia y lucha, por guiarme y comprenderme.
A mis hermanos por su amistad y apoyo incondicional.
Al Dr. Enrique Mafla por su acertada dirección y guía en el desarrollo de este proyecto.

Mauricio

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La realización de congresos, conferencias y seminarios en el Centro de Exposiciones Quito (CEQ) necesitan de la implementación de una red inalámbrica. La red inalámbrica tiene como particularidad que su funcionamiento es temporal y el mismo tendrá un tiempo de duración equivalente al tiempo de duración del evento. La solución para este tipo de red está basada en las Redes Móviles Ad-hoc que a diferencia de las redes cableadas y redes inalámbricas convencionales están diseñadas para un funcionamiento temporal.

La contribución de nuestra tesis, permitirá el despliegue de redes móviles para la realización de los eventos antes mencionados, sin depender de la existencia de una infraestructura de red previamente existente o si existe, que sea independiente de esta.

El desarrollo de este proyecto comienza con la selección de metodología y herramientas. Las herramientas elegidas son utilizadas en las diferentes etapas de la metodología seleccionada para la elaboración del proyecto. Luego se procede a la realización de un análisis de requerimientos a partir del cual se elaboran varias alternativas de diseño, las mismas que son aplicadas al Centro de Exposiciones Quito como un caso de estudio. Finalmente se plantean las conclusiones y recomendaciones obtenidas de la realización del proyecto.

INTRODUCCIÓN

Este proyecto consiste en el Análisis y Diseño de Redes Móviles Ad-hoc, para eventos tales como conferencias, congresos y seminarios. El diseño se realiza a partir de un análisis de requerimientos en base al cual se obtiene como resultado un diseño parametrizable que será aplicado como caso de estudio al Centro de Exposiciones Quito (CEQ).

Este documento está dividido en cuatro capítulos. En el primer capítulo relacionado a las Definiciones se realiza la definición del proyecto, la descripción del problema y la solución planteada al mismo, adicionalmente se realiza la respectiva Selección de Metodología y Herramientas que nos permitirán el desarrollo de este proyecto.

En el segundo capítulo relacionado al Análisis de Redes, se realiza un análisis de requerimientos de rendimiento, disponibilidad, seguridad, despliegue y finalmente se realiza un análisis enfocado en la conectividad interna y externa.

En el tercer capítulo correspondiente al Diseño de Redes, se realiza el diseño de la red de infraestructura, la distribución de los puntos de acceso y el diseño de seguridades basándonos en los requerimientos establecidos en el segundo capítulo. Finalmente se aplica las diferentes alternativas de diseño propuestas para el CEQ.

En el último capítulo se desarrollan las respectivas conclusiones derivadas del desarrollo del proyecto, en conjunto con la elaboración de recomendaciones.

CAPÍTULO I

DEFINICIONES

En el presente capítulo se realiza la definición del problema, se propone la solución al mismo y finalmente se selecciona y justifica la metodología y herramientas a ser utilizadas en el desarrollo de este proyecto.

Primero definiremos el problema de una forma global tomando en cuenta las necesidades de comunicación, despliegue y parámetros de confiabilidad de los usuarios. Después se propondrá la solución más adecuada que satisfaga los problemas planteados.

En la selección de metodología se detallan las diferentes etapas a seguir para la elaboración del proyecto. En la selección de herramientas, se elegirá aquellas que nos permitan desarrollar el diseño mencionado, justificando su uso.

1.1 DEFINICIÓN DEL PROYECTO

El Centro de Exposiciones Quito no posee una infraestructura de acceso inalámbrico para la realización de congresos, conferencias y seminarios. La red móvil a ser diseñada no necesita de una infraestructura previamente establecida, su funcionamiento es temporal y los requerimientos varían de acuerdo a las necesidades específicas del evento a realizarse.

La solución propuesta a los problemas antes mencionados es el diseño de una Red móvil Ad-hoc. La Red Ad-hoc es fácil de desplegar, fácil de implementarse, su funcionamiento es temporal y no necesita de una infraestructura previamente establecida, a diferencia de las redes inalámbricas y redes cableadas convencionales. Adicionalmente el diseño de la red debe brindar un alto

rendimiento, disponibilidad y seguridad considerando la concentración y distribución de usuarios y las necesidades de comunicación de los mismos.

1.2 SELECCIÓN DE METODOLOGÍA Y HERRAMIENTAS

1.2.1 SELECCIÓN DE METODOLOGÍA

Para la realización de este proyecto utilizaremos una metodología sistemática. El uso de una metodología sistemática nos permite definir los pasos a seguir para la elaboración de cada etapa, el conjunto de etapas definidas relacionadas entre sí ordenadamente contribuyen a que la realización de este proyecto funcione como un sistema.

La metodología sistemática estará enfocada al análisis y diseño de la red móvil considerando su despliegue, conectividad y sus requerimientos de confiabilidad. La metodología estará compuesta de las siguientes etapas:

1. Análisis de Requerimientos
2. Diseño
3. Aplicación en un caso de estudio.

1.2.1.1 Análisis de Requerimientos

En esta etapa se elabora un análisis de los requisitos variables de: Rendimiento que se refiere al ancho de banda de la conexión, Disponibilidad que se relaciona al porcentaje activo del servicio, el porcentaje de conexión a la red física y la conectividad IP a un punto de Internet o a otra red externa, la Concentración y Distribución de usuarios y finalmente se considerará la Seguridad relacionada a la Confidencialidad e Integridad.

Luego se realizará un análisis de requerimientos de despliegue en función del lugar en donde se implantará la infraestructura de la red móvil, de tal forma que los usuarios puedan trasladarse de un lugar a otro sin que estos pierdan su conexión.

Finalmente se elaborará un análisis de la Conectividad Interna de cada usuario la misma que se refiere a la forma como se comunicarán entre ellos. De igual forma se hará un análisis de la conexión externa, es decir la conexión a un punto de Internet o a otra red externa, en estas se considerará el o los protocolos de conexión, la seguridad y el tipo de conexión a ser usados de tal forma que se asegure la confiabilidad deseada.

1.2.1.2 Diseño

En esta fase, se utilizarán los requerimientos definidos en la etapa de análisis que se refieren a la Confiabilidad, Despliegue y Conectividad de la red. Como referencia de diseño utilizaremos la propuesta por Cisco para redes inalámbricas, la arquitectura modular SAFE[1] y su respectiva extensión para redes inalámbrica SAFE PARA WIRELESS[2].

1.2.1.3 Aplicación en un caso de estudio

Finalmente una vez que se ha determinado el diseño parametrizable en base a un previo análisis de requerimientos, este será aplicado como caso de estudio en el Centro de Exposiciones Quito.

---

[1] SAFE: A Security Blueprint for Enterprise Networks
[2] Cisco SAFE: Wireless LAN Security in Depth

1.2.2 SELECCIÓN DE HERRAMIENTAS

1.2.2.1 Modelo OSI

La utilización del Modelo OSI[3], basándonos en sus tres macro capas, nos permitirá realizar el diseño de la red de una manera modular. Las macro capas que componen el Modelo OSI son: Red Física (capa Física y de Enlace), Red de Datos (Capa de red y de Transporte) y Aplicaciones (capa de Sesión, Presentación y Aplicación).

La macro capa de Red Física comprende las características físicas de los componentes de la red, los mismos que son descritos en forma modular. La macro capa de Red de Datos considera el direccionamiento, enrutamiento y configuración del protocolo a usarse. La macro capa de Aplicaciones se relaciona a los servicios y aplicaciones que operan en la red. Los detalles de cada capa del Modelo OSI se detallan en el Anexo 1.

1.2.2.2 SLA[4] (Acuerdo de Nivel de Servicio)

El análisis de requerimientos para el diseño de una red Ad-hoc no puede ser realizado de la misma forma que se lo hace para redes convencionales. El número de usuarios y las aplicaciones que operarán en la red no son variables definidas y son específicas del evento, por lo que es necesario definir los requerimientos para cada evento y lo realizaremos mediante SLA's.

La elaboración de SLA's serán utilizados para la determinación del número de usuarios, las aplicaciones que operarán en la red, los requerimientos de rendimiento, seguridad, disponibilidad, conectividad y el área de cobertura que se proporcionará en el Centro de Exposiciones Quito.

---

[3] Open Systems Interconnection
[4] Service Level Agreement

Un Acuerdo de Nivel de Servicio (SLA), es el mantenimiento de la disponibilidad de un determinado servicio basado en un compromiso, medible y demostrable, del nivel de cumplimiento en su ejecución.

Un SLA es un acuerdo formal negociado entre dos partes. Es un contrato que existe entre clientes y su proveedor de servicio, o entre proveedores de servicio. Este transcribe un entendimiento común acerca de los servicios, prioridades, responsabilidades, garantías, etc. Con el principal propósito de coincidir en el nivel de servicio. Por ejemplo, este debe especificar los niveles de disponibilidad, habilidad del servicio, desempeño, operación u otros atributos del servicio como facturación y hasta penalidades en caso de violación del SLA.

SLA es esa parte en un contrato de servicio en el que cierto nivel del servicio es acordado. Un SLA por lo tanto no es un tipo de contrato de servicio, pero si una parte de un servicio contratado. Un contrato de servicio puede tener cero, uno o más SLA's.

Un SLA está generalmente orientado a los negocios y no profundiza mucho en detalles técnicos. Sus especificaciones técnicas son comúnmente descritas a través de SLS[5] (Especificación de Nivel de Servicio) o SLO[6] (Objetivo del Nivel de Servicio).

SLS es una interpretación técnica de SLA. Es por lo tanto dirigido como una guía operacional para la implementación del servicio.

SLO es un subconjunto de SLS, el cual contiene algunos parámetros de los servicios y los objetivos a ser logrados por el SLS.

[5] Service Level Specification, guía operacional para la implementación del servicio.
[6] Service Level Object, subconjunto de SLS que contiene parámetros de los servicios y los objetivos a ser logrados por el SLS

1.2.2.3 ITIL[7]

El uso del modelo de Gestión de Servicios de ITIL nos permitirá suministrar un soporte adecuado a los servicios proporcionados por la red. El manejo de los servicios proporcionados por una red Ad-hoc utilizando ITIL no puede ser realizado en la misma forma que se lo hace para redes convencionales, siendo necesario solamente para la realización de este proyecto enfocarnos en los bloques de ITIL referentes a la *"Prestación de Servicios*" y "*Soporte a los Servicios"* debido al funcionamiento temporal de la red.

ITIL se inicio como una guía para el gobierno de UK a finales de 1980. La estructura de ITIL ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software.
ITIL es conocido y utilizado mundialmente gracias a que es de libre uso.

Figura 1-1: Elementos de ITIL

[7] Information Technology Infrastructure Library

El Soporte a los servicios Se enfoca a establecer el soporte de servicios como un conjunto de procesos integrados. Tiene como misión definir los procesos necesarios para lograr los objetivos, la continuidad y la calidad de los servicios de tecnologías de información, consiguiendo con ello, la satisfacción del cliente, además de contribuir a la obtención de los objetivos organizacionales.

La Prestacion de servicios Cubre aspectos indispensables que deben considerarse para la implementación de servicios de las TI[8]. Los componentes incluidos son: administración de los niveles de servicio, administración financiera de servicios de las TI, administración de la continuidad de los servicios de las TI y administración de la disponibilidad.

Las Perspectivas del negocio como objetivo principal proporcionar a la alta dirección el diseño, la arquitectura y los componentes fundamentales para definir la Infraestructura de Tecnologías de Información y Comunicaciones (TIC) indispensable para impulsar los procesos estratégicos del negocio, con base en los estándares y mejores prácticas definidos para la administración del servicio.

Finalmente la Gestión de la infraestructura Cubre todos los aspectos de administración de la infraestructura de las TIC, desde la identificación de los requerimientos tecnológicos del negocio, por medio del análisis y definición de alternativas de solución, hasta la prueba, instalación, liberación, soporte en operación, y mantenimiento de los componentes de las TIC y servicios de las TI.

En el Anexo 3 se detallan los procesos de cada uno de los bloques mencionados anteriormente.

[8] Tecnologías de Información

1.2.2.4 Arquitectura SAFE

El uso de la arquitectura SAFE y su respectiva extensión para redes inalámbricas, SAFE PARA WIRELESS, nos proporcionará una guía para la elaboración del diseño de la red en una forma modular, considerando varios niveles de seguridad.

SAFE es una arquitectura de seguridad que evita que la mayor parte de los ataques afecten a los recursos de red más valiosos. La arquitectura SAFE no es una forma revolucionaria de diseñar redes, sino meramente un modelo para asegurarlas. SAFE sirve de guía a los diseñadores de red que están planteándose los requisitos de seguridad de su red. SAFE adopta un enfoque de defensa en profundidad para el diseño de la seguridad de las redes.

SAFE utiliza un enfoque modular. El enfoque modular tiene dos ventajas principales. En primer lugar, permite a la arquitectura afrontar la relación de seguridad entre los distintos bloques funcionales de la red. Y, en segundo lugar, permite a los diseñadores evaluar e implementar la seguridad módulo a módulo, en lugar de intentar completar la arquitectura en una sola fase.

SAFE también es resistente y ampliable. La resistencia de las redes incluye redundancia física que las protege de los fallos de los dispositivos debidos a una configuración errónea, a un fallo físico o a un ataque a la red.

Esta arquitectura se compone de tres macro módulos: Campus Empresarial, Perímetro de la Empresa y Perímetro del ISP[9]. La Siguiente figura muestra la primera capa de modularidad de SAFE.

[9] Internet Service Provider

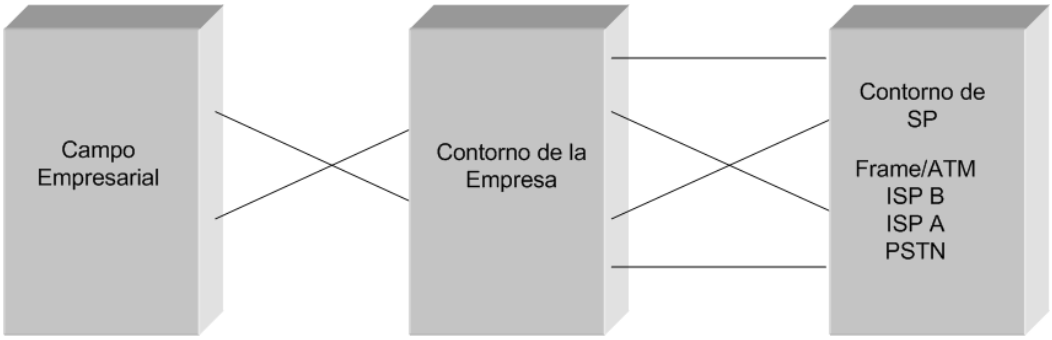

Figura 1-2: Primera capa de modularidad de SAFE

La segunda capa de modularidad, que se muestra en la siguiente ilustración, representa una vista de los módulos de cada área funcional, adaptado a las necesidades para el diseño de la red móvil motivo de este trabajo:

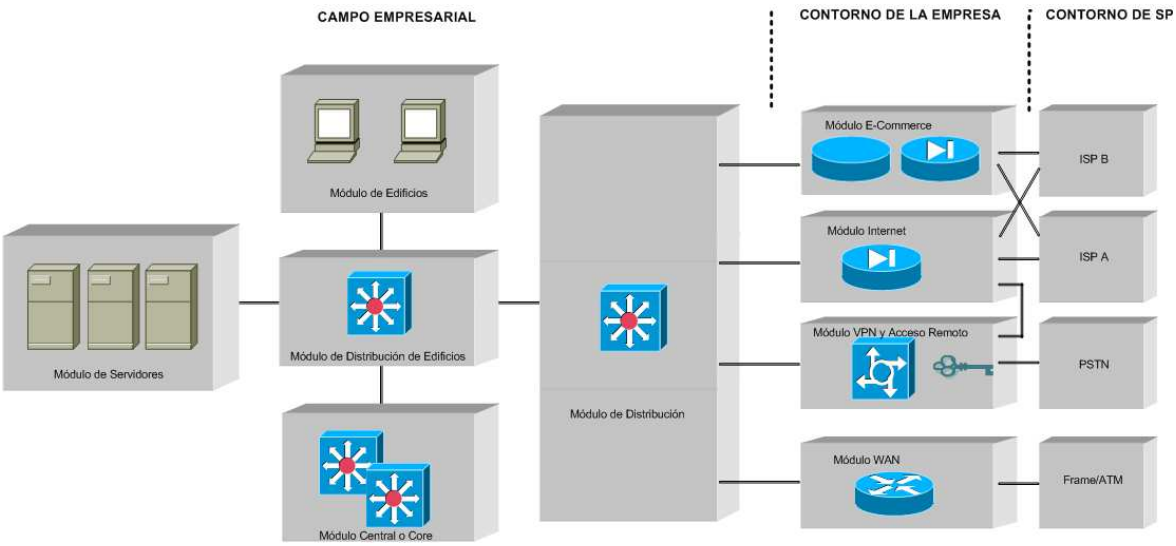

Figura 1-3: Segunda capa de modularidad de SAFE

CAMPUS EMPRESARIAL

Módulo de edificios

SAFE define el módulo del edificio como la parte amplia de la red que contiene las estaciones de trabajo de los usuarios finales, los teléfonos y sus puntos de acceso de Capa 2 asociados. Su objetivo principal es ofrecer servicios a los usuarios finales.

Módulo de distribuicion de edificios

El objetivo de este módulo es proporcionar servicios de la capa de distribución a los switches del edificio, entre los que se incluyen el enrutamiento, la calidad de servicio (QoS) y el control de accesos. Las solicitudes de datos entran en estos switches y en el núcleo, mientras que las respuestas siguen el camino inverso.

Módulo central

El módulo central de la arquitectura SAFE es casi idéntico al de cualquier otra arquitectura de red. Solamente enruta y conmuta el tráfico lo más rápidamente posible de una red a otra.

Módulo de servidores

El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones a los usuarios finales y a los dispositivos. Los flujos de tráfico del módulo de servidores los inspecciona la detección de intrusos a bordo en los switches de Capa 3.

Módulo de distribución

El objetivo de este módulo es agregar la conectividad de los distintos elementos al contorno. El tráfico se filtra y se enruta desde los módulos de contorno al núcleo.

CONTORNO DE LA EMPRESA.

Módulo de ecommerce

Este modulo esta orientado a hacer transacciones de comercio electrónico.

Módulo de internet corporativo

El módulo de Internet de la empresa proporciona a los usuarios internos conexión a los servicios de Internet y acceso a los usuarios de Internet a la información de los servidores públicos. El tráfico también fluye de este módulo de VPN[10] y de acceso remoto en que tiene lugar la terminación de la VPN.

[10] Virtual Private Network

Módulo de vpn y acceso remoto

Como su nombre implica, el objetivo principal de este módulo se divide en tres: terminar el tráfico VPN de los usuarios remotos, proporcionar un hub[11] para terminar el tráfico VPN de los sitios remotos y terminar los usuarios de acceso telefónico tradicionales. Todo el tráfico que se envía a la distribución del contorno es de los usuarios remotos de la empresa que están autenticados de alguna forma antes de que puedan pasar por el firewall.

Módulo wan

En lugar de incluir todos los diseños potenciales de WAN[12], este módulo muestra la resistencia y la seguridad de la terminación de WAN. Utilizando la encapsulación de Frame Relay, el tráfico se enruta entre los sitios remotos y el sitio central.

En el Anexo 4 se realiza una visión general de la arquitectura SAFE enfocado en su extensión para redes inalámbricas SAFE PARA WIRELESS.

[11] Dispositivo de red para conmutación de información
[12] Wide-Area Network

CAPÍTULO II

ANÁLISIS DE REDES

En el presente capítulo se realiza el análisis de los requerimientos de Rendimiento, Disponibilidad, Seguridad, Despliegue y Conectividad.

Primero analizaremos los requerimientos de rendimiento, disponibilidad y seguridad en base al tipo de aplicaciones a ser utilizadas y al número de usuarios. Luego analizaremos los requerimientos de despliegue, en esta etapa se tomará en cuenta las necesidades de movilidad de los usuarios determinada por el área de cobertura, esto nos permitirá determinar la posterior ubicación de los Access Points. Finalmente realizaremos un análisis de la conectividad interna y externa a fin de determinar los tipos de conexiones y protocolos a ser utilizados, los mismos que satisfagan las necesidades de conexión tanto interna como externa de los usuarios.

2.1 REQUERIMIENTOS DE RENDIMIENTO, DISPONIBILIDAD Y SEGURIDAD

Los requerimientos de rendimiento, disponibilidad y seguridad se respaldan con la aprobación del usuario sobre el servicio que recibe y se fundamenta de una manera formal en un Acuerdo de Nivel de Servicio (SLA). El SLA estará conformado por tres módulos, el primer módulo es de alto nivel, en este se selecciona los servicios a ser proporcionados y se define el número de usuarios. El segundo módulo está designado para la selección de la cobertura del servicio a través de un mapa del sitio. El tercer módulo es de nivel técnico y se describe cada uno de los servicios proporcionados. En el Anexo 2 se detallan los tres módulos del SLA para cada uno de los servicios.

Los requerimientos antes mencionados los definiremos basándonos en las aplicaciones que operarán en la red, en el número de usuarios y en el uso de dichas aplicaciones por parte de los mismos, parámetros definidos en los SLA's.

El diseño y gestión en que los SLA's serán realizados lo haremos apoyados en el modelo de Gestión de Servicios de ITIL enfocándonos solamente en los bloques de *"Prestación de Servicios*" y "*Soporte a los Servicios"*

Las aplicaciones fundamentales que operarán en la red son las siguientes: e-mail, navegación Web, y FTP[13]. Estas son clasificadas según el tipo de aplicación que las mismas representan como se muestra a continuación:

Aplicaciones	***Tipo de Aplicación***
Navegación Web	Interactiva
E-mail	Batch
FTP	Semi-interactiva

Tabla 2-1: Aplicaciones y su tipo

La naturaleza y particularidad de las redes Ad-hoc hace necesario que el nivel de servicio sea un sistema altamente redundante en cuanto a disponibilidad y rendimiento por lo tanto dicho sistema debe estar acompañado de un sistema formal de gestión como COBIT[14] en el cual nos enfocaremos solamente en los dominios de "*Despliegue y Soporte"* y "*Monitoreo y Control"* con el fin de cumplir con los requisitos establecidos en el SLA.

[13] File Transfer Protocol

[14] Modelo de referencia que contiene políticas claras y buenas prácticas para establecer controles y seguridad sobre los sistemas de tecnología de información.

2.1.1 RENDIMIENTO

Primeramente estableceremos las variables independientes y las variables dependientes. Las variables independientes no están previamente definidas y son especificadas para cada evento mediante el uso de SLA's, estas son: el número de usuarios y las aplicaciones que operarán en la red. Las variables dependientes son aquellas relacionadas al rendimiento: tiempo de respuesta, throughput y ancho de banda y están definidas a partir de las variables independientes mencionadas anteriormente.

El número de usuarios y las aplicaciones soportadas, definidas en los SLA's determinan el tiempo de respuesta, el throughput y el uso de ancho de banda de la red y de cada aplicación. Además se considera el uso simultáneo de los usuarios en la red y el rendimiento deseado de las aplicaciones por parte de los usuarios.

Los parámetros que determinan el rendimiento que el usuario requiere de las aplicaciones son los siguientes:

- Aplicaciones.
- Número de Usuarios.
- Forma de uso
    - Número de Solicitudes.
    - Complejidad de respuesta a las solicitudes.
    - Distribución de los intervalos de tiempo entre solicitudes.

Una vez definidos los parámetros anteriores, se determina el Tiempo de Respuesta, Throughput y Uso de ancho de banda, basándonos en los valores cualitativos requeridos por estos parámetros para cada una de las aplicaciones.

2.1.1.1 Tiempo de respuesta

El tiempo de respuesta se refiere al tiempo que espera el usuario desde el instante que realiza un requerimiento hasta el momento que la información es recibida. El tiempo de respuesta especifica la rapidez de la red al momento de proveer la información requerida por el usuario.

En la siguiente tabla se muestra el Tiempo de Respuesta requerido por cada una de las aplicaciones.

Aplicaciones	***Tiempo de Respuesta***
Navegación Web	Alto
E-mail	Bajo
FTP	Medio

Tabla 2-2: Aplicaciones y su tiempo de respuesta

2.1.1.2 Throughput

El throughput es la velocidad de transmisión de un lugar a otro en una unidad de tiempo. El throughput por usuario es el throughput total dividido para el número de usuarios, este throughput por usuario determina el máximo throughput teórico que una aplicación o usuario puede utilizar.

El throughput que cada aplicación agregará al tráfico de red y los Kilobits por conexión de las mismas, se muestran en la siguiente tabla:

Aplicaciones	***Throughput***	***Kbits por conexión***
Navegación Web	Alto	100 a 500
E-mail	Bajo	100
FTP	Medio	500

Tabla 2-3: Aplicaciones y throughput

2.1.1.3 Ancho de Banda

El ancho de banda indica la cantidad de información que puede fluir a través de una conexión de red en un período dado. El ancho de banda ilustra la velocidad o la tasa de transmisión de datos disponibles para una aplicación determinada.

En base al tipo de aplicación, a continuación se muestra el monto de ancho de banda requerido por cada una de estas.

Aplicaciones	*Uso de Ancho de Banda*
Navegación Web	Alto
E-mail	Bajo
FTP	Medio

Tabla 2-4: Aplicaciones y su uso de ancho de banda

2.1.2 DISPONIBILIDAD

Si las aplicaciones que se encuentran en la red no están disponibles para los usuarios de la misma, entonces esta no está cumpliendo con su objetivo. Los porcentajes de disponibilidad que se pondrán a consideración del usuario en los SLA's, para que este determine la disponibilidad que necesita se muestran en la siguiente tabla:

Disponibilidad %	*Downtime por año*	*Downtime por mes*	*Downtime por semana*
98%	7.30 días	14.4 horas	3.36 horas
99%	3.65 días	7.20 horas	1.68 horas
99.5%	1.83 días	3.60 horas	50.4 min.
99.9%	8.76 horas	43.2 min.	10.1 min.

Tabla 2-5: Porcentajes de disponibilidad

La disponibilidad de las aplicaciones que se encuentran operando en la red será asegurada mediante la implementación de medidas de tolerancia a errores como:

redundancia de servicios con la utilización de puntos de acceso redundante en frecuencias separadas y un diseño apropiado de las áreas de cobertura.

2.1.3 SEGURIDAD

La seguridad es un parámetro importante en redes Ad-hoc, debido a que son mucho más vulnerables y susceptibles de ataques que una red inalámbrica convencional.

Este requerimiento está subdividido en:

Confidencialidad: La confidencialidad nos asegura que los datos trasferidos solo pueden ser leídos por el destinatario final.

Integridad: La integridad nos permite que los datos enviados deban llegar al destinatario completo y sin modificaciones.

Para definir el nivel de seguridad que el usuario necesita, este deberá determinar el nivel de Confidencialidad e Integridad que requiere, dichos niveles se muestran en la siguiente tabla.

Parámetros de Seguridad	***Nivel***		
Confidencialidad	Alta	Media	Baja
Integridad	Alta	Media	Baja

Tabla 2-6: Parámetros y niveles de seguridad

2.2 REQUERIMIENTOS DE DESPLIEGUE

Los requerimientos de despliegue también se respaldarán, con la aprobación del usuario, de una manera formal en un Acuerdo de Nivel de Servicio (SLA).

En el SLA se proporcionará al usuario un mapa del Centro de Exposiciones Quito, de manera que este pueda elegir y determinar en que lugares del mismo desea tener cobertura para los usuarios finales.

El área de cobertura determinada debe proporcionar a los usuarios lo que necesitan, donde lo necesitan. Esto se relaciona con las distintas estrategias de despliegue, como la Planeación de Cobertura que se refiere a la evaluación del sitio donde se desea tener el servicio.

En la Planeación de Cobertura se tomará en cuenta el diseño de las localidades y los materiales con que estos fueron construidos, las capacidades de rango y cobertura de los puntos de acceso que se deberán usar y la flexibilidad de esas capacidades, las tecnologías y la capacidad de salida resultante para los canales disponibles para estas tecnologías.

De esta forma se asegurará la movilidad de los usuarios permitiéndoles a estos que se puedan trasladar de un área de cobertura de un punto de acceso a un área de cobertura del siguiente punto de acceso sin una degradación de los servicios prestados.

2.3 CONECTIVIDAD INTERNA Y EXTERNA

2.3.1 CONECTIVIDAD INTERNA

Una vez determinado el número de usuarios, el área de cobertura y las aplicaciones que operarán en la red, estableceremos en base a los parámetros anteriores el número, tipo y lugar en donde se colocarán los Access Points de una manera dinámica, considerando las posibles variaciones del número de usuarios por área de cobertura y la movilidad de estos, asegurando de esta forma que los usuarios estén siempre conectados, sin importar en que lugar se encuentren dentro del rango de cobertura. Además se determinará la configuración de los

Access Points mediante los cuales se establecerá la conexión con la red de infraestructura.

2.3.2 CONECTIVIDAD EXTERNA

La forma de conexión a redes externas y la velocidad de conexión a Internet, serán establecidas en el SLA.

En el SLA constará el tipo de la red externa a la que se desea conectar, el medio de conexión, la velocidad de conexión, los protocolos que se utilizan, además de las seguridades existentes. Una vez establecidos los parámetros anteriores, se determinará el tipo y la configuración del módulo mediante el cual se conectará a dichas redes, ya que mediante este se establecerá la comunicación entre los dispositivos de la red externa y los dispositivos de la red a ser diseñada.

CAPÍTULO III

DISEÑO DE REDES

El presente capítulo comprende el diseño de la red móvil Ad-hoc basándonos en el análisis de requerimientos realizado en el Capítulo II. Además consideramos que el diseño de una red Ad-hoc no requiere de una infraestructura previamente implementada y que su funcionamiento es temporal a diferencia de las redes convencionales.

Primero se realizará el diseño de la Red de Infraestructura la cual estará fundamentada en el Modelo OSI, en la arquitectura modular SAFE para WIRELESS y en la referencia de diseño de redes WLAN, ambas propuestas por Cisco. Luego procederemos al Diseño de la distribución de los Puntos de Acceso considerando los requerimientos de Despliegue establecidos en el Capítulo II y tomando en cuenta que dicha distribución es un proceso dinámico resultado de un constante monitoreo. A continuación se realizará el Diseño de Seguridades, el mismo que se basará tomando en cuenta los niveles de seguridad definidos en el SLA y las consideraciones establecidas en la arquitectura SAFE para WIRELESS y en la referencia de diseño de redes WLAN, propuestas por Cisco.

Finalmente se aplicará el diseño para el Centro de Exposiciones Quito (CEQ) considerado al mismo como un módulo móvil. Este módulo móvil podrá ser incorporado de acuerdo a la arquitectura SAFE, al Módulo de Contorno de la Empresa de la red del CEQ que representa el caso de estudio de nuestro trabajo. El diseño de la red móvil Ad-hoc elaborado en este capítulo y el cual es objeto de nuestro estudio es realizado de una manera independiente de la red existente del CEQ.

3.1 RED DE INFRAESTRUCTURA

El diseño de la Red de Infraestructura se basará en el Modelo OSI enfocándonos en sus tres macro capas. Adoptaremos como referencia de diseño la arquitectura SAFE para WIRELESS propuesta por Cisco y la propuesta de diseño de redes WLAN propuesta también por Cisco, lo cual nos permitirá tener un diseño de arquitectura modular.

El diseño de la red se realizará de acuerdo al análisis de requerimientos y los respectivos SLA's efectuados en el segundo capítulo, permitiéndonos de esta forma justificar cada decisión tomada durante el proceso de diseño.

El objetivo primordial del diseño es brindar una solución dentro de la cual se consideren conceptos de rendimiento, disponibilidad, seguridad y niveles de acceso a los servicios. De esta forma el diseño cumplirá con los requerimientos de los servicios brindados a los usuarios finales, previamente acordados en los respectivos SLA's.

3.1.1 DISEÑO DE LA RED DE INFRAESTRUCTURA

El diseño de la Red de infraestructura es realizado basado en las tres macro capas del Modelo OSI, lo cual determina que la red esté estructurada en tres módulos. En el primer módulo se realiza el diseño de la Red Física en la cual se consideran los conceptos de la capa física y capa de enlace, además utilizaremos como referencia de diseño la arquitectura SAFE para WIRELESS y la referencia de diseño de redes WLAN, ambas propuestas por Cisco. En el segundo módulo que se refiere a la Red de Datos, se realiza el enrutamiento, direccionamiento y configuración considerando los conceptos de la capa de red. En el último módulo relacionado a la macro capa de Aplicación, se realiza el diseño de los servicios basándonos en la capa de sesión, presentación y aplicación

3.1.1.1 Selección de Tecnología

Una vez que las aplicaciones, el número de usuarios y las áreas de cobertura han sido definidos en los SLA's, se determinará que estándar es el que mejor se ajusta a los requerimientos de los parámetros antes mencionados.

La selección del estándar 802.11 de la IEEE[15] se realiza mediante una comparación entre las diferentes tecnologías del estándar antes mencionado. La comparación es realizada de acuerdo al Throughput, Velocidad de Transmisión y Área de Cobertura de tal manera que el estándar seleccionado satisfaga los requerimientos establecidos en los SLA's.

Dentro del estándar 802.11 encontramos al estándar 802.11b el cual opera en la frecuencia 2.4 Ghz y soporta velocidades de transmisión de 1, 2, 5.5 y 11 Mbps. El estándar 802.11g opera en la misma frecuencia que 802.11b y es compatible con este último, adicionalmente soporta velocidades de transmisión de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps. Un tercer estándar, el 802.11a opera en la frecuencia de 5 Ghz y provee velocidades de transmisión de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps a diferencia del 802.11g el 802.11a no tiene compatibilidad con el 802.11b.

Throughput

Se considera el throughput que se proveerá a cada usuario, el throughput de cada aplicación y el throughput de la red.

El throughput por usuario está definido por el throughput total en un canal determinado, dividido para el número de usuarios en dicho canal. Este throughput consiste en el throughput teórico máximo que una aplicación o usuario podría utilizar.

[15] Institute for Electrical and Electronics Engineers

Velocidad de Transmisión

La velocidad de transmisión está relacionada a estándares, el medio ambiente y la distancia. Bajas velocidades de transmisión implica una mayor área de cobertura del Access Point mientras que altas velocidades de transmisión implica menor área de cobertura del Access Point. Esto influye en el área de cobertura y el número de Access Point a ser utilizados.

La velocidad de transmisión depende del tipo de aplicación a ser soportada, es decir son los requerimientos de las aplicaciones los que determinan la velocidad de transmisión.

A continuación se muestra una tabla comparativa de las distintas tecnologías de acuerdo a la Velocidad de Transmisión y al Throughput asociado a cada una de ellas.

Tecnología	Velocidad de Transmisión (Mbps)	Throughput Agregado (Mbps)	Número de Usuarios de ejemplo	Promedio de Throughput por Usuario
802.11b	11	6	10	600Kbps
802.11b	11	6	20	300Kbps
802.11b	11	6	30	200Kbps
820.11g	54	22	10	2.1Mbps
820.11g	54	22	20	1.1Mbps
820.11g	54	22	30	760Kbps
820.11a	54	25	10	2.5Mbps
820.11a	54	25	20	1.25Mbps
820.11a	54	25	30	833Kbps

Tabla 3-1: Comparación de Tecnologías de acuerdo a la Velocidad de Transmisión

Área de Cobertura

El área de cobertura depende del ambiente en donde se desea implementar la red inalámbrica. Mientras más obstrucciones estén presentes la cobertura se verá afectada.

A continuación se muestra una tabla comparativa del rango de cobertura de los diferentes estándares de acuerdo a su respectiva velocidad de transmisión.

	Interiores		**Exteriores**	
	802.11a	**802.11g**	**802.11a**	**802.11g**
Velocidades de Transmisión y Rangos de Cobertura	24 m @ 54Mbps 45 m @ 48Mbps 60 m @ 36Mbps 69 m @ 24Mbps 76 m @ 18Mbps 84 m @ 12Mbps 91 m @ 9Mbps 100 m @ 6Mbps	30 m @ 54Mbps 53 m @ 48Mbps 76 m @ 36Mbps 84 m @ 24Mbps 100 m @ 18Mbps 107 m @ 12Mbps 110 m @ 11Mbps 114 m @ 9Mbps 122 m @ 6Mbps 128 m @ 5.5Mbps 134 m @ 2Mbps 137 m @ 1Mbps	30 m @ 54Mbps 91 m @ 48Mbps 130 m @ 36Mbps 152 m @ 24Mbps 168 m @ 18Mbps 183 m @ 12Mbps 190 m @ 9Mbps 198 m @ 6Mbps	37 m @ 54Mbps 107 m @ 48Mbps 168 m @ 36Mbps 198 m @ 24Mbps 229 m @ 18Mbps 224 m @ 12Mbps 250 m @ 11Mbps 267 m @ 9Mbps 274 m @ 6Mbps 277 m @ 5.5Mbps 287 m @ 2Mbps 290 m @ 1Mbps

Tabla 3-2: Comparación de Tecnologías de acuerdo al Área de Cobertura

La interoperabilidad que existe entre el estándar 802.11g y 802.11b permite que dispositivos que soporten estas tecnologías puedan comunicarse entre sí a diferencia de aquellos que solamente soportan el estándar 802.11a. El estándar 802.11b añade menor throughput a la red pero soporta menores velocidades de transmisión a diferencia de los estándares 802.11g y 802.11a. El estándar 802.11g soporta mayor número de velocidades que el estándar 802.11a lo que se traduce en abarcar un mayor rango de cobertura.

3.1.1.2 Red Física

El diseño de la red física es realizado basándonos en el rendimiento de las aplicaciones, en los niveles de seguridad y en los porcentajes de disponibilidad definidos en los SLA's. La red física estará compuesta de dos partes fundamentales, una parte fija y una parte variable la cual se refiere a la ubicación dinámica y configuración de los Access Points.

Obtendremos como resultado varias alternativas de diseño en función de los distintos niveles de seguridad y de disponibilidad contemplados en los SLA's, a diferencia de las redes convencionales en las cuales los parámetros anteriores se encuentran definidos previamente.

Como referencia de diseño utilizaremos la arquitectura SAFE para WIRELESS, la cual está compuesta por tres macro módulos: Módulo de la Empresa, Módulo de Contorno de la Empresa y Módulo de Periferia. El módulo de Periferia o Módulo del proveedor de servicios no es desarrollado en la arquitectura, ya que este no lo implementa la empresa. Cada macro módulo de la arquitectura SAFE, está compuesto por una segunda capa de módulos, estos módulos realizan funciones específicas en la red y tienen requisitos de seguridad específicos.

El diseño de cada módulo y de su segunda capa de módulos se lo realiza en base a los niveles de Seguridad y a los porcentajes de Disponibilidad establecidos en el SLA.

3.1.1.2.1 Módulo de la Empresa

3.1.1.2.1.1 Módulo Central o Core

El objetivo del Módulo Central es solamente enrutar y conmutar el tráfico lo más rápidamente posible de una red a otra. El dispositivo a ser utilizado es un Switch de capa 3 que nos permita integrar tanto equipos de comunicación como equipos

que cumplen con la función de servidores. El switch se encarga de realizar actividades de filtrado, decisiones de retransmisión y seguridad.

3.1.1.2.1.2 Módulo de Distribución

Basándonos en las alternativas de diseño que SAFE propone para este módulo unificamos el módulo Central y el módulo de Distribución. La unificación de ambos módulos se justifica debido a que las actividades que se realizan en el módulo de distribución como: enrutamiento, conectividad, calidad de servicio (QoS) y control de accesos de los servicios de la capa de distribución al switch del Módulo de Edificio, pueden ser implementadas sin ningún problema en el Módulo Central.

La realización del diseño del Módulo Central y el Módulo de Distribución unificados (Módulo Central-Distribución), se lo efectúa en base a los diferentes niveles de Seguridad y Disponibilidad establecidos en los respectivos SLA's, como ya se mencionó anteriormente.

El diseño del Módulo Central-Distribución referente a la Seguridad se lo realiza basándonos en los niveles de la misma relacionados a la confidencialidad e integridad, como se muestran en la siguiente tabla:

Parámetros de Seguridad	***Nivel***		
Confidencialidad	Alta	Media	Baja
Integridad	Alta	Media	Baja

Tabla 3-3: Parámetros y niveles de seguridad

Para los niveles de seguridad Alta y Media, se utiliza un Switch de Capa 3. La configuración del switch de Capa 3 se basa en las siguientes consideraciones de seguridad:

- Los puertos que no necesiten enlaces troncales, son desactivados, en lugar de dejar la configuración en auto. Esto evita que un host se convierta en un

puerto troncal y que reciba todo el tráfico que normalmente llegaría a dicho puerto.

- Los puertos troncales usan un número de VLAN[16] que no se emplea en ninguna otra parte del switch. Esto evita que los paquetes marcados con la misma VLAN que el puerto troncal lleguen a otra VLAN sin cruzar el Switch de Capa 3.
- Los puertos no utilizados son desactivados. Esto evita que los hackers se conecten a los puertos no utilizados y se comuniquen con el resto de la red.
- Se desactivan los servicios no necesarios.
- Se realiza registro a los niveles apropiados.

Las consideraciones de seguridad antes mencionadas son aplicadas a todos los switches indicados en los diferentes módulos citados en el desarrollo de este capítulo, sean estos Switches de Capa 2 o Switches de Capa 3.

La función primordial del Switch del Módulo Central-Distribución es proporcionar: direccionamiento y conmutación del tráfico de producción, servicios de la capa de distribución (ruteo, calidad de servicio [QoS], y control de acceso) para los switches del módulo de edificio, conectividad para los servidores, y servicios avanzados como filtrado de tráfico entre subredes. El Switch de Capa 3 fue seleccionado para proporcionar el manejo de VLAN's separadas para el segmento de servidores, grupos de usuarios y conectividad al módulo WAN y al módulo de Internet. La configuración de las VLAN's se especifica más adelante en este capítulo en el diseño de la Red de Datos.

El switch de capa 3 proporciona una línea de defensa y prevención contra ataques generados internamente. Mitiga la oportunidad de que un grupo de usuarios pueda acceder a la información confidencial de otro a través del uso de acceso de control. El control de acceso previene ataques de falsificación de direcciones locales a través del uso de filtrado RFC 2827. Adicionalmente se implementa el uso de ACL's[17] las cuales limitarán la conectividad hacia y desde

[16] LAN Virtual
[17] Access Control Level

los servidores, solamente a esos dispositivos (vía direcciones IP) bajo su control y solamente a esos protocolos/servicios (vía número de puertos) que son requeridos. Esto también incluye control de acceso para la administración de tráfico destinado para los dispositivos de sitios remotos. El acceso a los dispositivos es controlado permitiendo solamente establecer conexiones de regreso a través de ACL's.

El uso de VLAN's no es el único método adicional empleado para asegurar el acceso entre subredes. Las VLAN's son combinadas con consideraciones y métodos de seguridad adicionales, los mismos que serán explicados a lo largo del desarrollo de este capítulo.

A continuación se muestra el diseño de Módulo Central-Distribución para los niveles de seguridad antes mencionados:

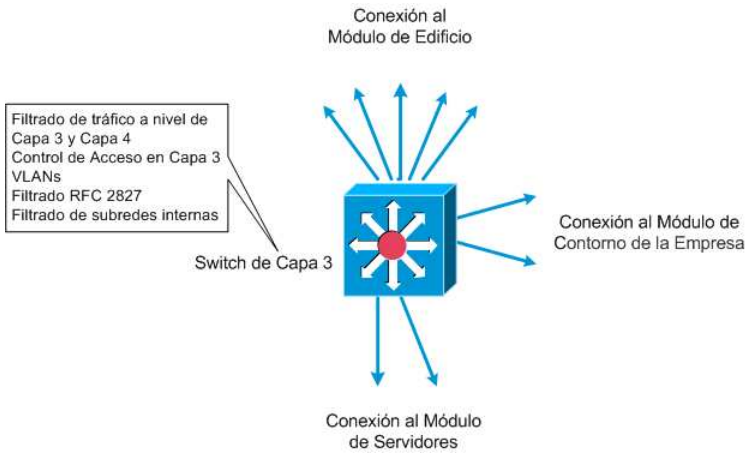

Figura 3-1: Módulo Central-Distribución para Seguridad Alta y Media

Descripción de los dispositivos del diseño:

- ***Switch de Capa 3.-*** enruta y conmuta datos de la red de producción de un módulo a otro.

Amenazas que combate el diseño:

- ***Rastreadores de paquetes (Packet Sniffers).-*** una infraestructura conmutada limita la efectividad del rastreo.

- ***Acceso no autorizado.-*** los ataques contra los recursos del módulo del servidor se limitan mediante el filtrado en la Capa 3 de determinadas subredes.

- ***Ataques de falsificación (spoofing) de IP.-*** los filtros de RFC 2827 detienen la mayoría de los intentos de falsificación.

El diseño para seguridad Baja en lugar de utilizar un switch de capa 3, se utiliza un switch de capa 2. Las consideraciones de su configuración son las mismas especificadas anteriormente en el Switch de capa 3.

La utilización de un Switch de capa 2 ocasiona que ya no existan restricciones de acceso al tráfico de la red desde los clientes mediante el access point, no se usa VLAN's para el manejo de servidores, usuarios y conectividad al módulo WAN y de Internet, y no existe la utilización de ACL's. Esto no significa que la seguridad de este nivel sea totalmente nula ya que se utilizan diseños de seguridad implementados en el Módulo de Edificio.

A continuación se muestra el diseño del Módulo Central-Distribución para el nivel de seguridad Baja:

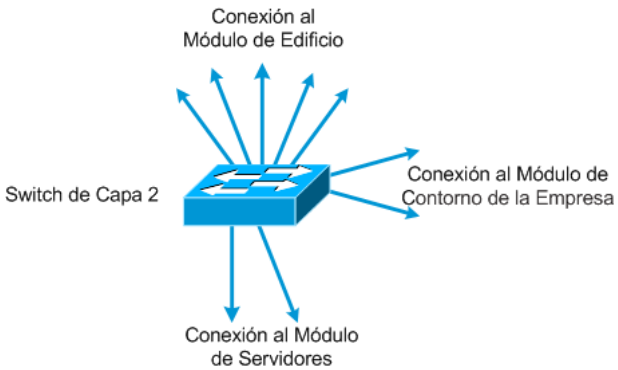

Figura 3-2: Módulo Central-Distribución para Seguridad Baja

Descripción de los dispositivos del diseño:

- ***Switch de Capa 2.-*** enruta y conmuta datos de la red de producción de un módulo a otro.

Amenazas que combate

- ***Rastreadores de paquetes (Packet Sniffers).-*** una infraestructura conmutada limita la efectividad del rastreo.

El diseño del Módulo Central-Distribución referente a la Disponibilidad se lo efectúa basándonos en los diferentes porcentajes de la misma como se muestran en la siguiente tabla:

Disponibilidad %
98%
99%
99.5%
99.9%

Tabla 3-4: Porcentajes de disponibilidad

Para los porcentajes de disponibilidad de 98% y 99% se utilizan los mismos diseños establecidos anteriormente de acuerdo a la Seguridad requerida, ya que los mismos satisfacen los porcentajes de disponibilidad mencionados.

Con respecto a los porcentajes de disponibilidad de 99.5% y 99.9% se incluye en los diseños anteriores la implementación de un Switch de capa 3 adicional en el diseño de los niveles de Seguridad Alta y Media; y un Switch de capa 2 para el diseño del nivel de seguridad Baja. La función de estos switches es actuar en modo Stand By, en caso de falla de los primeros switches los switches adicionales entrarán a reemplazar a los mismos.

Los diseños para los porcentajes de disponibilidad de 99.5% y 99% son los siguientes:

Diseño de disponibilidad para Seguridad Alta y Media:

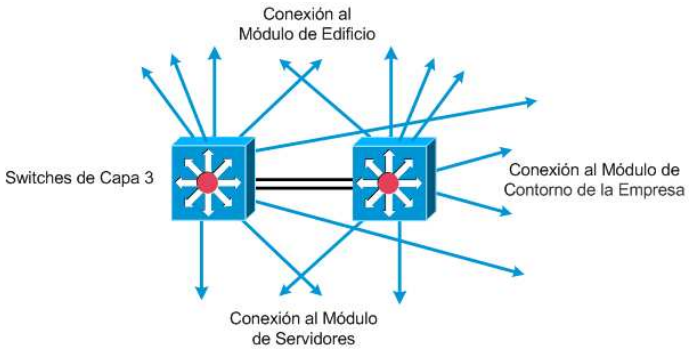

Figura 3-3: Módulo Central-Distribución para Seguridad Alta y Media con Disponibilidad de 99.5% y 99%

Diseño de disponibilidad para Seguridad Baja:

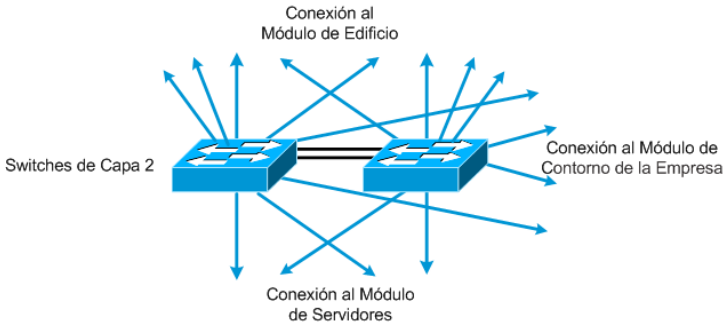

Figura 3-4: Módulo Central-Distribución para Seguridad Baja con Disponibilidad de 99.5% y 99%

3.1.1.2.1.3 Módulo de Edificio

Constituye la parte amplia de la red, contiene las estaciones de trabajo de los usuarios finales permitiéndoles a estos conectarse con los servidores de la red. El dispositivo a ser utilizado es un Switch de capa 2 con la capacidad de implementar VACL[18]. Este switch se comunica con el Módulo Central-Distribución, además se conectará con los Access Points que sean requeridos. El diseño de

[18] Tecnología llamada VLAN ACL

este módulo está determinado por los requerimientos de seguridad y disponibilidad establecidos en los SLA's.

De igual forma como se definió en el diseño del Módulo Central-Distribución, los niveles de seguridad a considerarse son los mismos.

El diseño del nivel de Seguridad Alta se basa en una solución que utiliza IPsec VPN. Los clientes se asocian con los access points los mismos que están configurados con filtrado de puertos y protocolos de tal forma que solamente estén habilitados los protocolos requeridos para establecer un túnel seguro hacia el VPN gateway. El access point mantiene una conexión a través de una VLAN dedicada con el Switch de Capa 2 el cual transmite el tráfico de los clientes de la WLAN hacia el concentrador VPN. Los clientes establecen una conexión IPsec automática con el VPN gateway una vez que la correcta dirección IP ha sido recibida del servidor DHCP, mientras dura este proceso el VPN gateway provee la autenticación de dispositivos utilizando certificados digitales, adicionalmente utiliza servicios RADIUS[19], que se contactan con el servidor OTP[20] para la autentificación de los usuarios. EL VPN gateway usa DHCP para la información de direccionamiento IP para que los clientes de la WLAN se comuniquen a través del túnel VPN. La conexión del VPN gateway con los servidores RADIUS, DHCP y OTP se establece mediante el Switch de Capa 3 del módulo Central-Distribución el cual está configurado con ACL's que se encargan de permitir solamente los protocolos necesarios para la conectividad y administración para VPN, garantizando que solamente el tráfico IPsec destinado hacia el concentrador VPN cruce el switch. Adicionalmente cada cliente debe estar configurado con firewalls personales para proteger a los mismos mientras estos están conectados a la red inalámbrica no segura sin la protección de IPsec, es decir antes que se establezca el túnel IPsec, además cada usuario es equipado con un cliente IPsec mediante el cual se establecerá el túnel IPsec.

[19] Remote Access Dial-In User Service
[20] One-Time Password

El diseño incluye un dispositivo NIDS[21]. El puerto del switch que está conectado con el dispositivo NIDS está configurado de una forma que el tráfico de todas las VLAN's que requieren monitoreo es copiado al puerto de monitoreo del dispositivo, en donde se detectan ataques en los puertos y protocolos que el switch está configurado para permitir. El sistema NIDS tiene límites en la cantidad de tráfico que puede analizar, solamente se le envía el tráfico sensible a ataques como SMTP, FTP y WWW. Muy pocos ataques deben ser detectados aquí porque el dispositivo NIDS proporciona análisis contra los ataques que pueden originarse dentro del mismo módulo. Los servidores tienen instalado HIDS[22], cuya función primordial es monitorear cualquier actividad maliciosa que ocurre al nivel de Sistema Operativo tanto como en aplicaciones comunes en los servidores (HTTP, FTP, SMTP, etc.). La detección de intrusos basada en host funciona interceptando las llamadas al sistema operativo y a las aplicaciones de un host individual. A causa de la especificidad de su función, los sistemas IDS[23] basados en host (HIDS) suelen ser mejores para evitar ciertos ataques que los IDS de red (NIDS), que normalmente sólo emiten una alerta al descubrir un ataque. Para lograr un sistema de detección de intrusos completo, Cisco recomienda una combinación de ambos sistemas (HIDS en los servidores y NIDS supervisando toda la red). La especificación de los servidores citados anteriormente se especifica en este capítulo en la parte del Módulo de Servidores.

La inclusión del dispositivo WLSE[24] tiene el propósito de administrar todos los access points de la red, la función detallada de sus funciones de describen en el segmento Distribución de Puntos de Acceso desarrollado más adelante en este capítulo. Este dispositivo se encuentra presente en todos los diseños relacionados al Módulo de Edificio.

A continuación se muestra el diseño del Módulo de Edificio para el nivel de seguridad Alta basado en IPsec VPN:

---

[21] Network Intrusion Detection Systems
[22] Host-Based Intrusion Detection Systems
[23] Intrusion Detection Systems
[24] Wireless LAN Solution Engine

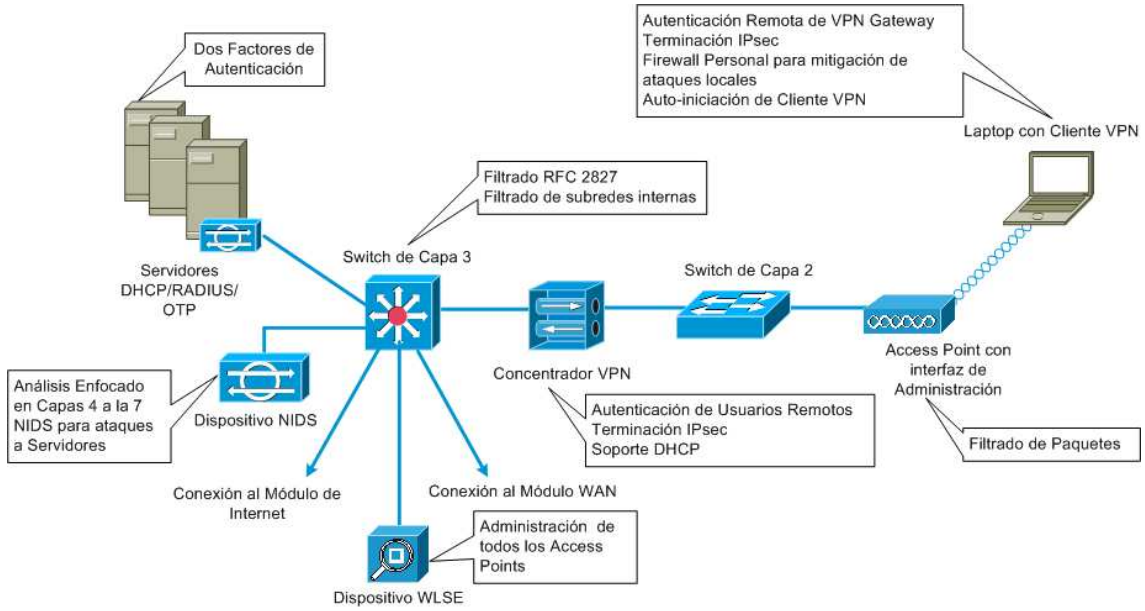

Figura 3-5: Módulo de Edificio para Seguridad Alta

Descripción de los dispositivos del diseño IPsec VPN:

- ***Software para Acceso Remoto de Cliente VPN y firewall personal***.- software en el cliente que provee túneles encriptados de fin a fin entre las PCs individuales y los VPN gateways inalámbricos corporativos; software de firewall personal que provee un nivel de protección a nivel de dispositivos para las PCs individuales.

- ***Access point***.- provee el control inicial de filtrado IP entre la red inalámbrica y la red corporativa.

- ***Switch de Capa 2***.- Provee conectividad Ethernet entre los access points y la red corporativa

- ***Switch de Capa 3***.- enruta y conmuta los datos de la red de un módulo a otro, provee adicionalmente la ejecución de políticas vía filtrado a nivel de protocolo para el tráfico inalámbrico mediante el uso de VLAN ACL (VACL), lo cual provee una capa adicional de filtrado IPsec.

- ***Servidor RADIUS***.- Autentica a los usuarios inalámbricos que llegan al VPN gateway; opcionalmente se comunica con el servidor OTP.

- ***Servidor OTP***.- Autoriza la información OTP transmitida desde el servidor RADIUS.

- ***Servidor DHCP***.- Entrega la información de la configuración IP para los clientes inalámbricos VPN antes y después de establecer VPN.

- ***VPN gateway***.- Autentica individualmente a los usuarios remotos y termina los túneles IPsec y puede también proveer la funcionalidad de transmitir DHCP para los clientes inalámbricos.

- ***Dispositivo de NIDS.-*** proporciona supervisión de la Capa 4 a la Capa 7 de los elementos de red clave del módulo.

- ***Dispositivo WLSE.***- Administra todos los access points de la red

Ataques mitigados con este diseño:

- ***Rastreadores de paquetes inalámbricos.-*** estas amenazas son mitigadas mediante encriptación IPsec del tráfico inalámbrico del cliente. También, nuevas características en el software VPN en el cliente permiten especificar que el túnel VPN sea automáticamente iniciado cuando la correcta dirección IP es asignada al cliente. Esto elimina la interacción del usuario para crear el túnel IPsec y también protege la PC del cliente del tráfico de transmisión en el medio inalámbrico que podría ser usado para ataques basados en interferencia.

- ***MITM[25].-*** estas amenazas son mitigadas mediante encriptación IPsec y la autenticación del tráfico inalámbrico del cliente.

- ***Acceso no autorizado.-*** Solamente los protocolos conocidos para la configuración inicial IP (DHCP) y acceso VPN (DNS, Internet Key Exchange [IKE] y Encapsulating Security Payload [ESP]) son permitidos desde la red inalámbrica a la red corporativa a través de filtrado en el access point y control de acceso en el switch. Políticas de autorización son implementadas en el VPN gateway para grupos de usuarios individuales.

- ***Ataques de falsificación de IP.-*** hackers pueden falsificar el tráfico en la red inalámbrica, pero solamente aquellos paquetes IPsec que han sido autenticados legítimamente alcanzarán la red cableada.

- ***Ataques de falsificación de ARP[26].-*** ataques de falsificación ARP pueden ser lanzados; sin embargo, los datos son encriptados al VPN gateway así los hackers no serán capaces de leer los datos.

- ***Ataques de Password.-*** estas amenazas son mitigadas mediante el uso de políticas de buenos passwords, además del uso de OTP.

- ***Descubrimiento de la topología de red.-*** Solamente IKE, ESP, DNS, y DHCP están permitidos el ingreso a este segmento de la red corporativa. Internet Control Message Protocol (ICMP) es solamente permitido en la interfaz exterior del concentrador VPN para propósitos de reparación técnica.

- ***Ataques de falsificación de MAC[27] o IP de usuarios autenticados.-*** Los ataques de falsificación ARP e IP son todavía efectivos en la subred inalámbrica hasta que el cliente inalámbrico use IPsec para asegurar la

[25] Man In The Middle attack
[26] Address Resolution Protocol
[27] Media Access Control

conexión. Esta amenaza es mitigada mediante el uso de firewalls personales en las PCs de los clientes.

- ***Protección contra Virus y Troyanos*.-** Esta amenaza es mitigada a través del escaneo de virus en los clientes mediante el uso de antivirus.

- ***Ataques a la Capa de Aplicación*.-** Mitigado a través de NIDS.

El diseño del Módulo de Edificio para el nivel de seguridad Media contempla la utilización de EAP[28] con TKIP[29]. El protocolo EAP a ser utilizado y la manera de autenticación es mediante la propuesta por Cisco, Cisco LEAP.

Los access points se encuentran conectados al Switch de capa 2, los clientes inalámbricos y los access points usan EAP para la autenticación de usuarios en el servidor RADIUS. Los dispositivos de los clientes son configurados para usar protocolos DHCP, luego de una exitosa configuración DHCP los usuarios inalámbricos tienen acceso a la red corporativa. Se implementa el uso de VLAN's inalámbricas únicas en los access points permitiendo la implementación de diferenciación de usuarios. La asignación dinámica de VLAN es implementada para los usuarios EAP usando el servidor RADIUS y configuraciones de usuarios y grupos, esto proporciona la ventaja de la segregación de usuarios en comunidades de usuarios y el cumplimiento de políticas para estos grupos en la capa de distribución. Las VLAN's son configuradas en los access points en los cuales el tráfico de administración es aislado del tráfico de los usuarios mediante la implementación de la *VLAN de administración* en los access points, adicionalmente se implementa una *VLAN invitado* para usuarios invitados con el fin de permitir a estos el acceso a ciertos servicios y recursos limitados de la red corporativa. De igual forma el Switch de Capa 3 del módulo Central-Distribución es configurado con ACL's que se encargan de permitir solamente los protocolos y tráfico necesarios para la conectividad.

[28] Extensible Authentication Protocol
[29] Temporal Key Integrity Protocol

La autenticación mediante LEAP[30] reside en la mutua autenticación entre los clientes asociados con un access point y el servidor RADIUS. Una vez que se ha desarrollado el logeo en la red, los clientes y el servidor RADIUS intercambian mensajes EAP para desarrollar la mutua autenticación, en donde los clientes verifican las credenciales del servidor RADIUS y viceversa. En los clientes es usado un *EAP supplicant* mediante el cual se obtiene las credenciales de usuario (user ID y password). Luego de una exitosa autenticación mutua, el cliente y el servidor RADIUS derivan una clave WEP[31] específica del cliente a ser usada por este para la sesión de logeo actual. El password del usuario y las claves de sesión nunca son transmitidas sin protección en el ambiente inalámbrico.

Adicionalmente para EAP con TKIP se utiliza el tiempo recomendado por CISCO de 4 horas y 40 minutos para volver a generar las claves WEP, además luego de un corto número de intentos de logeos incorrectos, la cuenta es bloqueada para prevenir ataques de fuerza-bruta que puede ocurrir en la cuenta del usuario. El número de intentos especificado en el servidor RADIUS es de 3 combinados con el uso de políticas de contraseñas fuertes. Además los servidores tienen instalado HIDS, cuya función primordial es monitorear cualquier actividad maliciosa que ocurre al nivel de Sistema Operativo tanto como en aplicaciones comunes en los servidores (HTTP, FTP, SMTP, etc.).

A continuación se muestra el diseño del Módulo de Edificio para el nivel de seguridad Media basado en EAP con TKIP:

[30] Lightweight EAP
[31] Wired Equivalent Privacy

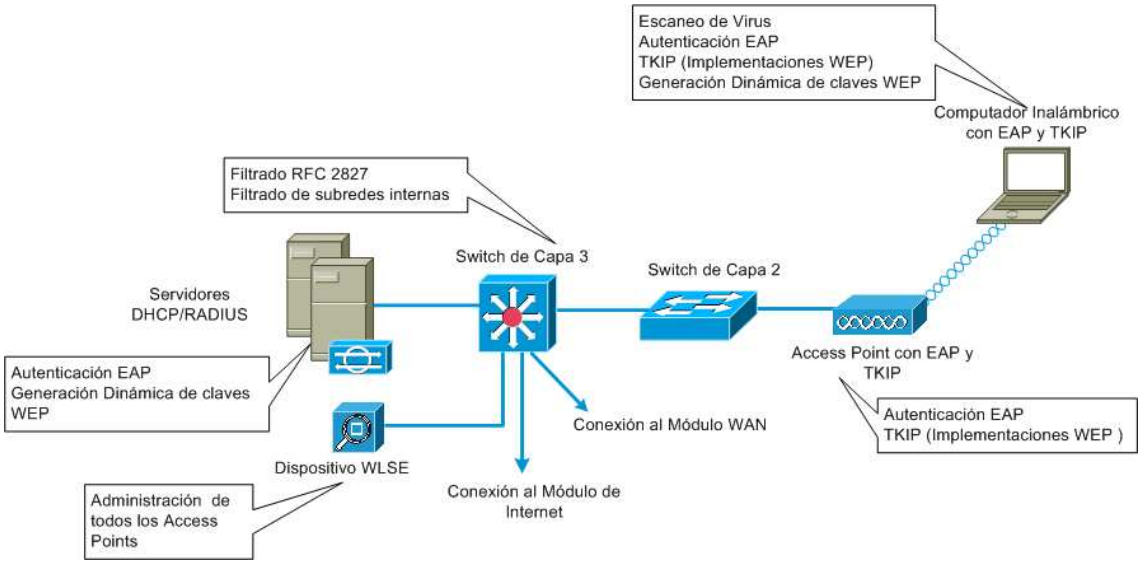

Figura 3-6: Módulo de Edificio para Seguridad Media

Descripción de los dispositivos del diseño EAP:

- ***Adaptador de cliente inalámbrico y software.-*** una solución de software que provee el hardware y software necesario para las comunicaciones inalámbricas con el access point, provee mutua autenticación con el access point a través de EAP; un EAP supplicant es requerido en la máquina del cliente para soportar el apropiado tipo de autenticación EAP.

- ***Access Point.-*** autentica mutuamente los clientes inalámbricos vía EAP y puede soportar múltiples VLAN's de capa 2 para la diferenciación de usuarios.

- ***Switch de Capa 2***.- Provee conectividad Ethernet entre los access points y la red corporativa

- ***Switch de Capa 3***.- enruta y conmuta los datos de la red de un módulo a otro, provee adicionalmente la ejecución de políticas vía filtrado a nivel de protocolo para el tráfico inalámbrico mediante el uso de VLAN ACL (VACL), lo cual provee una capa adicional de filtrado entre la red inalámbrica y la red corporativa.

- ***Servidor RADIUS***.- Entrega autenticaciones basadas en usuarios para los clientes inalámbricos y autenticación de los access points con los clientes inalámbricos; adicionalmente es usado para especificar parámetros de accesos de control de VLAN para usuarios y grupos de usuarios.

- ***Servidor DHCP***.- Entrega la información de la configuración IP para los clientes inalámbricos LEAP.

- ***Dispositivo WLSE.***- Administra todos los access points de la red

Amenazas mitigadas con este diseño:

- ***Rastreadores de paquetes inalámbricos.-*** los rastreadores de paquetes inalámbricos pueden tomar ventaja de cualquiera de los ataques WEP conocidos que derivan en la encriptación de la clave. Estas amenazas son mitigadas a través de las mejoras en WEP (específicamente con per-packet keying PPK como parte de TKIP) y la rotación de claves usando EAP.

- ***Acceso no autenticado.-*** solamente usuarios autenticados son capaces de acceder a la red inalámbrica. El control de acceso en el Switch de capa 3 limita el acceso a la red cableada.

- ***MITM.-*** La naturaleza de autenticación mutua de los diferentes tipos de autenticación EAP combinada con MIC puede prevenir que los hackers interfieran en el camino de las comunicaciones inalámbricas.

- ***Ataques de falsificación de IP.-*** Hackers no pueden desarrollar ataques de falsificación de IP sin haberse autenticado primero en la red inalámbrica, luego de haberse autenticado el filtrado opcional RFC 2827 en el switch de capa 3 restringe cualquier ataque de falsificación a la extensión de subred local.

- ***Ataques de falsificación de ARP.-*** hackers no pueden desarrollar falsificación ARP sin antes haberse autentificado en la red inalámbrica; luego

de haberse autenticado, la falsificación ARP puede ser lanzada in la misma forma como se la hace en un ambiente cableado para interceptar los datos de otros usuarios.

- ***Descubrimiento de la topología de la red.-*** hackers no pueden desarrollar el descubrimiento de la red si estos no son capaces de autenticarse. El atacante puede notar que existe la red inalámbrica mirando el SSID[32] del access point, pero no puede acceder a la red. Cuando se ha autenticado vía EAP, el descubrimiento de la topología estándar puede ocurrir en la misma forma que es posible en una red cableada.

- ***Ataques de Password.***- mitigado mediante el uso de una política de contraseña fuerte es recomendado para mitigar los ataques en contra de LEAP. El administrador de IT además tiene que limitar el número de los intentos de registro de entrada antes de bloquear la cuenta.

- ***Protección contra Virus y Troyanos*.-** Esta amenaza es mitigada a través del escaneo de virus en los clientes mediante el uso de antivirus.

Finalmente el diseño de Módulo de Edificio para el nivel de Seguridad Baja está basado en la utilización de EAP con TKIP. A diferencia del nivel de seguridad media en este diseño se suprime el uso de un Switch de capa 3. Se unifican los módulos Central-Distribución con el módulo de Edificio para lo cual se usa un Switch de capa 2 el cual se encargará de enrutar y conmutar todo el tráfico de la red. Se suprime el uso de VLAN's para los grupos de usuarios, solamente se implementa VLAN's para los servidores y la VLAN para administración de los access points. La administración del tráfico de red desde los clientes hacia los access points no es restringido debido a la ausencia del Switch de capa 3. Los access points están conectados al Switch de capa 2, los usuarios inalámbricos EAP utilizan los servicios DHCP y RADIUS para acceder a la red, ambos servidores se encuentran conectados al Switch de Capa 2. La autenticación de los usuarios es la misma especificada en el diseño para el nivel de seguridad media.

[32] Service Set ID

La utilización de EAP con TKIP garantiza que la seguridad establecida para este nivel no sea nula. Este diseño tiene mitigados los ataques más peligrosos conocidos sobre las redes inalámbricas. Además los servidores también tienen instalado HIDS, cuya función primordial es monitorear cualquier actividad maliciosa que ocurre al nivel de Sistema Operativo tanto como en aplicaciones comunes en los servidores (HTTP, FTP, SMTP, etc.).

A continuación se muestra el diseño del Módulo de Edificio para el nivel de seguridad Baja basado en EAP con TKIP:

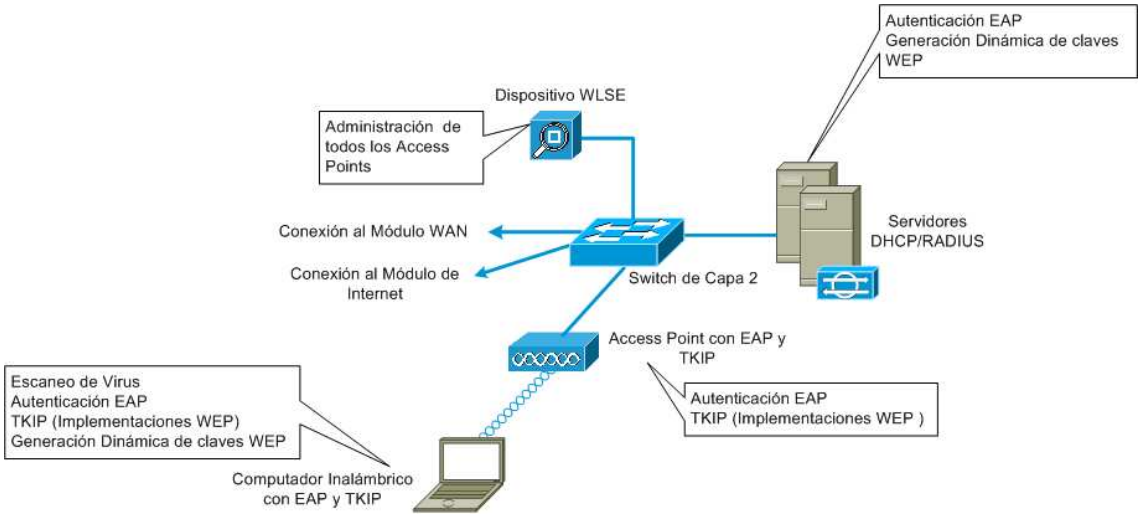

Figura 3-7: Módulo de Edificio para Seguridad Baja

Descripción de los dispositivos del diseño EAP:

- ***Adaptador de cliente inalámbrico y software.-*** una solución de software que provee el hardware y software necesario para las comunicaciones inalámbricas con el access point, provee mutua autenticación con el access point a través de EAP; un EAP supplicant es requerido en la máquina del cliente para soportar el apropiado tipo de autenticación EAP.

- ***Access Point.-*** autentica mutuamente los clientes inalámbricos vía EAP y puede soportar múltiples VLAN's de capa 2 para la diferenciación de usuarios.

- ***Switch de Capa 2 (con soporte para VLAN privada).***- Provee conectividad Ethernet entre los access points y la red corporativa y el módulo de Servidores

- ***Servidor RADIUS***.- Entrega autenticaciones basadas en usuarios para los clientes inalámbricos y autenticación de los access points con los clientes inalámbricos.

- ***Servidor DHCP***.- Entrega la información de la configuración IP para los clientes inalámbricos LEAP.

- ***Dispositivo WLSE.***- Administra todos los access points de la red

Amenazas mitigadas con este diseño:

- ***Rastreadores de paquetes inalámbricos.-*** los rastreadores de paquetes inalámbricos pueden tomar ventaja de cualquiera de los ataques WEP conocidos que derivan en la encriptación de la clave. Estas amenazas son mitigadas a través de las mejoras en WEP (específicamente con per-packet keying PPK como parte de TKIP) y la rotación de claves usando EAP.

- ***Acceso no autenticado.-*** solamente usuarios autenticados son capaces de acceder a la red inalámbrica. El control de acceso en el Switch de capa 3 limita el acceso a la red cableada.

- ***MITM.-*** La naturaleza de autenticación mutua de los diferentes tipos de autenticación EAP combinada con MIC[33] puede prevenir que los hackers interfieran en el camino de las comunicaciones inalámbricas.

- ***Ataques de falsificación de ARP.-*** hackers no pueden desarrollar falsificación ARP sin antes haberse autentificado en la red inalámbrica; luego de haberse autenticado, la falsificación ARP puede ser lanzada en la misma

[33] Message Integrity Check

forma como se la hace en un ambiente cableado para interceptar los datos de otros usuarios.

- ***Descubrimiento de la topología de la red.-*** hackers no pueden desarrollar el descubrimiento de la red si estos no son capaces de autenticarse. El atacante puede notar que existe la red inalámbrica mirando el SSID del access point, pero no puede acceder a la red. Cuando se ha autenticado vía EAP, el descubrimiento de la topología estándar puede ocurrir en la misma forma que es posible en una red cableada.

- ***Ataques de Password.***- mitigado mediante el uso de una política de contraseña fuerte es recomendado para mitigar los ataques en contra de LEAP. El administrador de TI además tiene que limitar el número de los intentos de registro de entrada antes de bloquear la cuenta.

- ***Protección contra Virus y Troyanos*.-** Esta amenaza es mitigada a través del escaneo de virus en los clientes mediante el uso de antivirus.

De igual forma a la realizada en el diseño del módulo Central-Distribución se especificarán diseños para los diferentes porcentajes de disponibilidad establecidos en el SLA, basados en los ya establecidos para los niveles de seguridad determinados anteriormente.

Para los porcentajes de disponibilidad de 98% y 99% se utilizan los mismos diseños establecidos anteriormente de acuerdo a la Seguridad requerida. Estos diseños satisfacen los porcentajes de disponibilidad mencionados.

Los porcentajes de disponibilidad de 99.5% y 99.9% requieren que se incluya en los diseños anteriores la implementación de dispositivos adicionales para conseguir los porcentajes mencionados como se estableció en el diseño del módulo Central-Distribución. Los servidores son desplegados en una forma

redundante sobre subredes diferentes, adicionalmente se implementa balanceo de carga para dichos servidores.

A continuación se muestran los diseños que satisfacen los porcentajes de 99.5% y 99.9% de disponibilidad basados en los diseños ya desarrollados anteriormente.

Diseño de disponibilidad de 99.5% y 99.9% para Seguridad Alta:

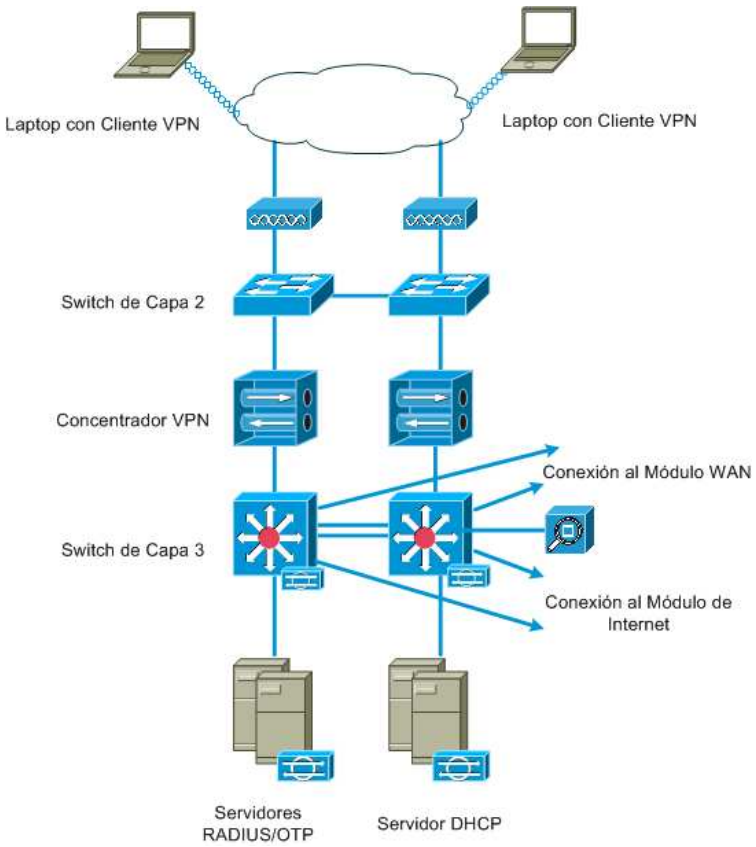

Figura 3-8: Módulo de Edificio para Seguridad Alta y Disponibilidad de 99.5% y 99%

Diseño de disponibilidad de 99.5% y 99.9% para Seguridad Media:

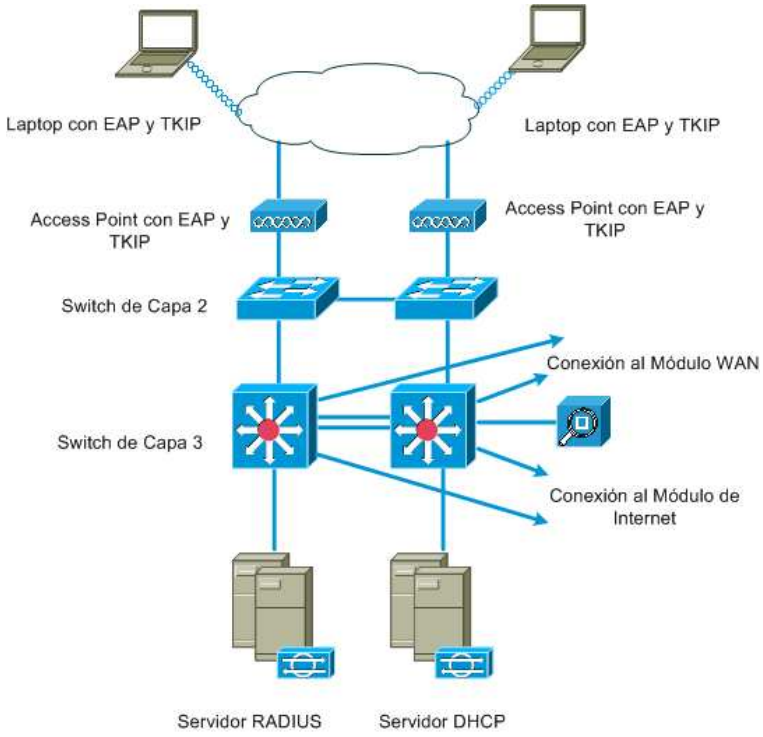

Figura 3-9: Módulo de Edificio para Seguridad Media y Disponibilidad de 99.5% y 99%

Diseño de disponibilidad de 99.5% y 99.9% para Seguridad Baja:

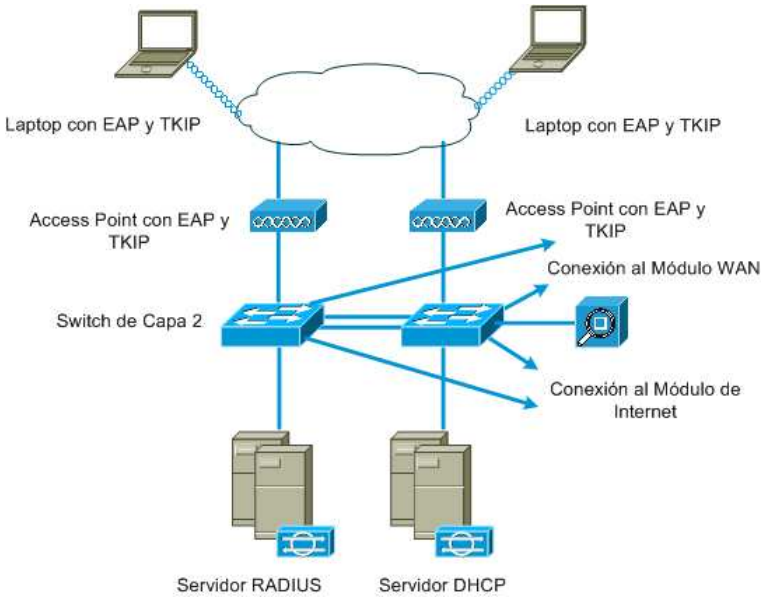

Figura 3-10: Módulo de Edificio para Seguridad Baja y Disponibilidad de 99.5% y 99%

3.1.1.2.1.4 Módulo de Servidores

El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones a los usuarios finales y a los dispositivos. Los flujos de tráfico del módulo de servidores los inspecciona el switch del Módulo Central-Distribución sea este de Capa 2 o Capa 3 según sea el caso.

Los servidores pueden ser el objetivo principal de los ataques originados internamente. El simple uso de contraseñas eficaces no es suficiente para una estrategia global de combate de ataques. Se usa IDS basado en host y en red según sea el caso, VLAN privadas, control de accesos y buenas prácticas de administración de sistemas (como mantener los sistemas actualizados con los últimos parches) lo cual proporciona una respuesta mucho más exhaustiva a los ataques.

Cada servidor especificado en este diseño tiene instalado HIDS, cuya función primordial es monitorear cualquier actividad maliciosa que ocurre al nivel de Sistema Operativo tanto como en aplicaciones comunes en los servidores (HTTP, FTP, SMTP, etc.). La detección de intrusos basada en host funciona interceptando las llamadas al sistema operativo y a las aplicaciones de un host individual.

Los servidores que se incluirán en el diseño de este módulo de acuerdo a la seguridad requerida se muestran en las siguientes tablas:

Seguridad Alta:

Servidores
Servidor FTP/http
Servidor de Correo Electrónico
Servidor DHCP
Servidor RADIUS
Servidor OTP

Tabla 3-5: Servidores para Red con Seguridad Alta

Seguridad Media y Baja:

Servidores
Servidor FTP/HTTP
Servidor de Correo Electrónico
Servidor DHCP
Servidor RADIUS

Tabla 3-6: Servidores para Red con Seguridad Media y Baja

La inclusión del Servidor FTP/HTTP y Servidor de Correo Electrónico depende de las aplicaciones que operarán en la red, definidas en el SLA. El Servidor DHCP/RADIUS y los servidores antes mencionados están incluidos en todos los diseños especificados, de acuerdo al nivel de seguridad, en el diseño del Módulo de Edificio. Adicionalmente para el diseño de Módulo de Edificio, para seguridad alta, se incluye un Servidor OTP el mismo que es implementado en conjunto con el Servidor RADIUS, el Servidor DHCP es implementado independientemente de los dos anteriores. El dimensionamiento de cada servidor es realizado de acuerdo al número de clientes especificados en el SLA y a las aplicaciones a ser implementadas, considerando proporcionar un alto rendimiento y disponibilidad.

En lo referente al rendimiento, el dimensionamiento de cada servidor se basará en los requerimientos establecidos, relacionados a este parámetro, en el Capítulo II que comprende: el número de usuarios establecido en el SLA, las aplicaciones también establecidas en el SLA y en la forma de uso de dichas aplicaciones. Los parámetros antes mencionados los aplicaremos al uso de SPEC[34] considerando el tipo de servidor que se desea evaluar. SPEC proporciona benchmark para servidores Web SPEC WEB2005, Correo Electrónico SPEC MAIL2001, SPEC CPU2006, etc.

Además para mejorar el rendimiento de las aplicaciones se utiliza las herramientas de QoS disponibles en los Access Points. Las aplicaciones

[34] Standard Performance Evaluation Corporation

identificadas como sensitivas para el throughput y retardo de la red pueden ser clasificadas y organizadas como se requiera.

Servidor FTP/HTTP.- Este servidor es diseñado considerando el número de usuarios a ser atendidos, el número aproximado de transacciones que generarán dichos usuarios considerando las aplicaciones FTP y navegación Web y en los requerimientos de rendimiento establecidos en el Capítulo II. Estos parámetros serán aplicados al benchmark para SPEC WEB2005, para determinar que características debe tener el servidor para soportar el rendimiento deseado.

Servidor de Correo Electrónico.- Este servidor es diseñado considerando el número de clientes a ser atendidos y por los requerimientos de rendimiento establecidos en el capítulo II para la aplicación de correo electrónico. Ambos parámetros serán aplicados al benchmark para SPEC MAIL2001, con el fin de establecer que características debe tener el servidor para soportar el rendimiento deseado.

Servidor DHCP y RADIUS/OTP.- Este servidor es diseñado considerando el número de clientes a ser atendidos y las transacciones simultáneas hechas a este servidor. Estos parámetros serán aplicados al benchmark para SPEC CPU2006, para determinar que características debe tener el servidor para soportar el rendimiento deseado.

En lo referente a la disponibilidad, como ya se trató en el desarrollo del Módulo de Edificio se estableció dos grupos de porcentajes. El primer grupo en el cual se encuentran los porcentajes de 98% y 99% no se tomarán más consideraciones para el diseño de este módulo solamente se considerará aquellas referentes al rendimiento las cuales fueron citadas anteriormente. El segundo grupo en el cual se encuentran los porcentajes de 99.5% y 99.9% se tomarán consideraciones adicionales a las anteriormente mencionadas relacionadas al rendimiento como:

- Los servidores son desplegados en una forma redundante sobre subredes diferentes.

- Se implementa balanceo de carga para dichos servidores.

- La ubicación de los servidores se establece dentro del sitio donde se realiza el evento en un lugar determinado para los mismos con las seguridades pertinentes, esto con el fin de evitar cualquier tipo de pérdida de conexión con los servidores, si es que estos se encontrasen ubicados en las oficinas centrales.

A continuación se muestra el diseño lógico del Módulo de servidores para el nivel de Seguridad Alta:

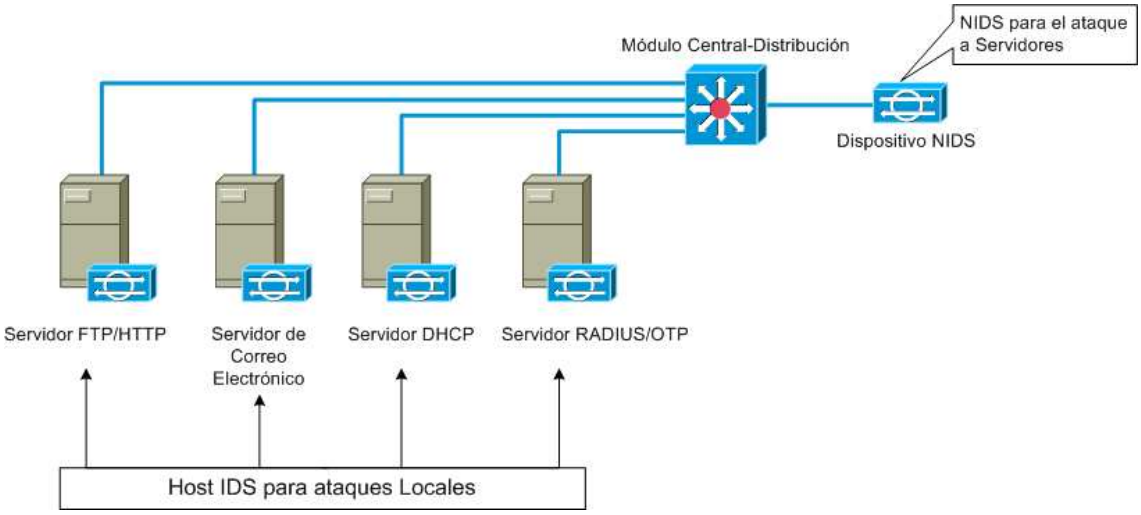

Figura 3-10: Módulo de Servidores para Seguridad Alta

A continuación se muestra el diseño lógico del Módulo de servidores para el nivel de Seguridad Media:

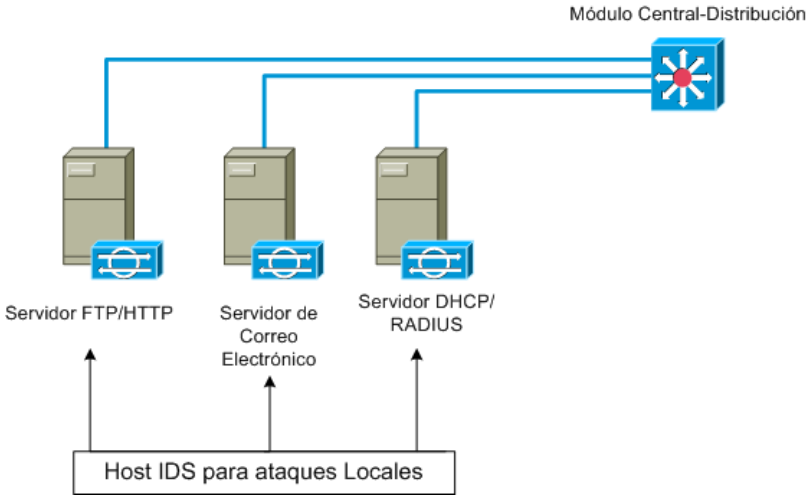

Figura 3-11: Módulo de Servidores para Seguridad Media

A continuación se muestra el diseño lógico del Módulo de servidores para el nivel de Seguridad Baja:

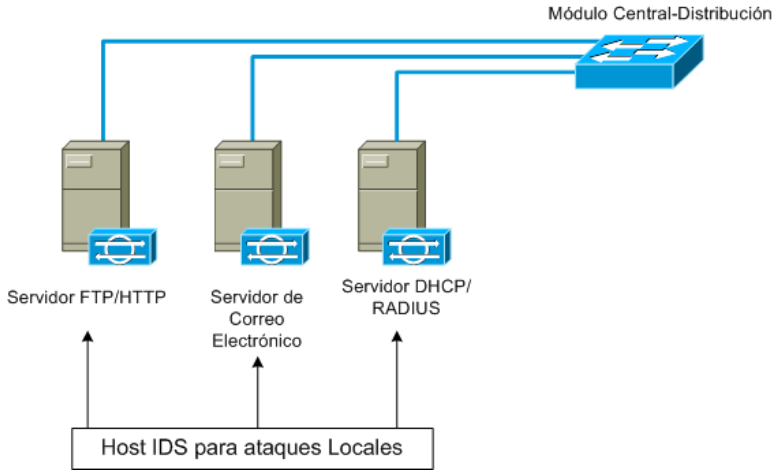

Figura 3-12: Módulo de Servidores para Seguridad Baja

Descripción de los dispositivos del diseño:

- ***Servidor FTP/HTTP.-*** proporciona a los usuarios conexión a los servicios de Internet

- ***Servidor de correo electrónico.-*** proporciona servicios SMTP y POP3 a los usuarios internos.

- ***Servidor RADIUS.-*** Entrega autenticaciones basadas en usuarios para los clientes inalámbricos y autenticación de los access points con los clientes inalámbricos.

- ***Servidor OTP***.- Autoriza la información OTP transmitida desde el servidor RADIUS.

- ***Servidor DHCP***.- Entrega la información de la configuración IP para los clientes inalámbricos.

Amenazas que combate este diseño:

- ***Acceso no autorizado.-*** combatido mediante el uso de detección de intrusos basada en hosts.

- ***Ataques a la capa de aplicaciones.-*** los sistemas operativos, los dispositivos y las aplicaciones se mantienen actualizados con las actualizaciones más recientes de seguridad y protegidos mediante IDS basado en host.

- ***Ataques de falsificación (spoofing) de IP.-*** los filtros de RFC 2827 evitan la falsificación de direcciones de origen.

- ***Rastreadores de paquetes (Packet Sniffers).-*** una infraestructura conmutada limita la efectividad del rastreo.

- ***Abuso de confianza.-*** las organizaciones de confianza son muy explícitas, las VLAN privadas evitan que los hosts de la misma subred se comuniquen a menos que sea necesario.

- ***Redireccionamiento de puertos.-*** el IDS basado en host evita que se instalen agentes de redireccionamiento de puertos.

Los diseños referentes a los distintos porcentajes de disponibilidad son los mismos establecidos para los distintos niveles de seguridad, con las respectivas consideraciones citadas anteriormente en lo que concierne a dichos porcentajes de disponibilidad.

3.1.1.2.2 Módulo de Distribución del Contorno

El módulo de distribución del contorno es unificado con el módulo central. Entre las funciones que realiza el módulo de distribución del contorno están: control de acceso para filtrar tráfico y conmutación de Capa 3 para lograr un alto rendimiento. El módulo de distribución del contorno proporciona la última línea de defensa para todo el tráfico destinado al módulo central desde el módulo del contorno. Esto incluye la defensa contra los paquetes falsificados, actualizaciones erróneas de enrutamientos y provisiones para el control de acceso a las capas de la red.

Debido al tipo de red diseñada y considerando que las funciones antes mencionadas ya se encuentran implementadas en el Módulo Central-Distribución y por facilidad de diseño, el Módulo de Distribución del Contorno se implementará en el Módulo Central-Distribución basándonos en las alternativas de diseño propuestas por SAFE para el diseño de este módulo.

3.1.1.2.3 Módulo de Contorno de la Empresa

3.1.1.2.3.1 Módulo de Internet

El diseño de este módulo se basa en los requerimientos de conectividad externa referente a la conexión a Internet establecida en los SLA’s siendo el parámetro primordial la velocidad de conexión con el proveedor del servicio (ISP). El proveedor de servicio de Internet (ISP) puede ser proporcionado por la conexión a Internet del CEQ, si el mismo dispone de dicha conexión y si satisface la

velocidad de conexión requerida por los usuarios finales, caso contrario el servicio de Internet se lo contratará de otros proveedores.

La disponibilidad, rendimiento y seguridad de la conexión a Internet será establecida con el proveedor del mismo, ISP, en un SLA en el cual se establezcan los detalles de los parámetros antes mencionados, relacionado al servicio proporcionado. Adicionalmente se realiza el diseño de este módulo considerando medidas de seguridad adicionales a las proporcionadas por el ISP las cuales son detalladas a continuación:

El Módulo de Internet proporciona a los usuarios conexión a los servicios de Internet y acceso a los usuarios de Internet a la información de los servidores públicos. Este módulo también soporta tráfico VPN y de acceso remoto en que tiene lugar la terminación de la VPN. Este módulo no está diseñado para servir aplicaciones de comercio electrónico.

El módulo de Internet representa la última escala en el diseño de seguridad de la red, donde todas las seguridades y servicios VPN están comprimidos en una sola caja.

La funcionalidad de este módulo es diseñada mediante el uso de un router con firewall y funcionalidad VPN. Esta configuración produce una alta flexibilidad para el diseño de la red ya que el router soporta todos los servicios avanzados (QoS, ruteo, soporte para múltiples protocolos, etc.) necesarios para las redes. Se usa inspección en todos los estados para examinar el tráfico en todas las direcciones, asegurando que solamente el tráfico legítimo llegue y cruce el firewall. Antes que el tráfico llegue al firewall, algunos filtros de seguridad ya han ocurrido en el ISP. Además de la resistencia de la Capa 2 y de la Capa 3 integrada en el módulo y la capacidad de recuperación con estado del firewall, las restantes consideraciones del diseño se centran en la seguridad y la defensa contra ataques.

Comenzando en el router del ISP, la velocidad de salida del ISP limita el tráfico no esencial que supera los umbrales previamente especificados para combatir los

ataques de DoS. Además, en la salida del router del ISP, los filtros de RFC 1918 y RFC 2827 combaten la falsificación de las redes locales y de los rangos de redes privadas.

En la entrada del firewall, primeramente se proporcionan los filtros RFC 1918 y RFC 2827 como una verificación del filtrado realizado en el ISP. Adicionalmente debido a la enorme amenaza que crean contra la seguridad, el firewall está configurado para eliminar la mayoría de los paquetes fragmentados que normalmente no deberían verse de los tipos de tráfico estándar de Internet. Toda pérdida de tráfico legítimo perdido a causa de estos filtros se considera aceptable al compararla con el riesgo de permitir dicho tráfico. El tráfico destinado hacia el mismo firewall desde afuera está limitado al tráfico IPsec y a cualquier protocolo necesario para el ruteo.

El firewall proporciona cumplimiento del estado de las conexiones y filtros detallados para las sesiones iniciadas a través del firewall. Los servidores con direcciones públicas tienen cierta protección contra desbordamientos SYN de TCP a través del uso de límites de conexiones medio abiertas en el firewall. Desde el punto de vista de los filtros, además de limitar el tráfico en el segmento de servidores públicos a las direcciones y puertos pertinentes, también tiene lugar el filtro en la dirección opuesta. Si algún ataque pone en peligro a uno de los servidores públicos (sorteando el firewall y el IDS basado en host) dicho servidor no podría atacar la red. Para combatir este tipo de ataque, el filtrado específico evita que los servidores públicos generen peticiones no autorizadas en otra ubicación. Esto ayuda a evitar que los hackers descarguen más utilidades en el equipo en peligro tras el ataque inicial. También ayuda a impedir que el hacker inicie sesiones no deseadas durante el ataque primario. Además, se configuran VLAN’s privadas en el Switch de capa 2 de la zona militarizada DMZ para evitar que los servidores públicos que estén en peligro ataquen a otros servidores del mismo segmento. Este tráfico no lo detecta ni el firewall, que es el motivo por el que las VLAN privadas son vitales en el diseño.

Desde la perspectiva de servidores, cada uno de los servidores en el segmento de servicios públicos tiene implementado HIDS (Host Intrusion Detection Software). HIDS permite monitorear cualquier actividad maliciosa a nivel del sistema operativo, como también en aplicaciones de servidores comunes (HTTP, FTP, SMTP). El host de DNS debe bloquearse para que responda solamente a los comandos deseados y elimine todas las respuestas innecesarias que puedan ayudar a los hackers en el reconocimiento de la red. Aquí se impide que realice transferencias de zona desde cualquier parte que no sean los servidores DNS internos. El servidor SMTP incluye servicios de inspección de los contenidos del correo que combaten los ataques de virus y troyanos generados contra la red interna y que suelen introducirse a través del sistema de correo. El propio firewall filtra los mensajes de SMTP en la Capa 7 para permitir solamente los comandos necesarios en el servidor de correo. El dimensionamiento de estos servidores se realiza basándonos en el diseño de los servidores del Módulo de Servidores.

El tráfico del segmento de inspección de contenidos se limita a las solicitudes de filtro de direcciones URL en el router con firewall.

El Router con Firewall generalmente tienen capacidad NIDS limitada dentro de sus funciones de seguridad. Esta capacidad afectará el desempeño de este dispositivo, pero proveerá cierta visibilidad adicional de ataques en el caso que la red se encontrara bajo los mismos.

La conectividad VPN es provista mediante el router con firewall. Los sitios remotos son autenticados entre ellos mediante claves pre-compartidas y los usuarios remotos son autenticados a través del servidor de control de acceso en el módulo Central-Distribución.

Para la configuración de la seguridad del router-firewall se toman en cuenta las siguientes consideraciones, con el fin de reducir la posibilidad de que se pongan directamente en peligro.

- Bloqueo del acceso por telnet a un router.

- Bloqueo del acceso por el protocolo Simple Network Management Protocol (SNMP) a un router.

- Control del acceso a un router a través del uso de RADIUS.

- Desactivación de los servicios no necesarios.

- Registro a los niveles apropiados.

- Autenticación de las actualizaciones del enrutamiento.

Las consideraciones de seguridad antes citadas son aplicadas a cada router mencionado en el desarrollo de este capítulo.

A continuación se muestra el diseño lógico del Módulo de Internet:

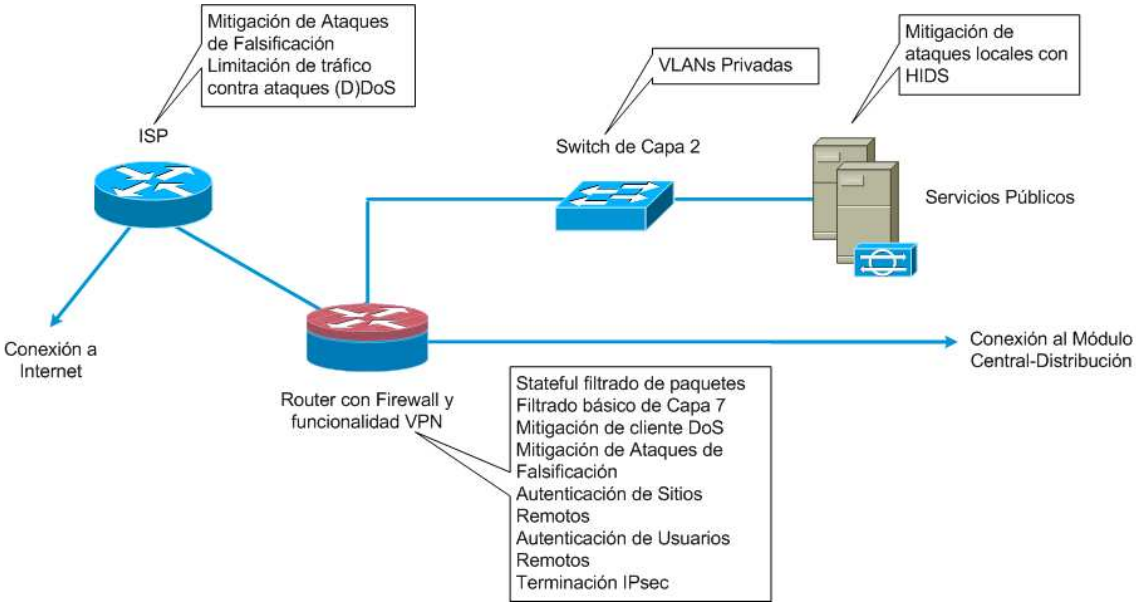

Figura 3-13: Módulo de Internet

Descripción de los dispositivos del diseño:

- ***Servidor SMTP.-*** actúa como relevo entre Internet y los servidores de correo de Internet (inspecciona los contenidos).

- ***Servidor DNS.-*** sirve como servidor DNS externo autorizado de la empresa, transmite las solicitudes internas a Internet.

- ***Servidor FTP/HTTP.-*** proporciona información pública acerca de la organización.

- ***Router con Firewall.-*** proporciona protección a nivel de red de los recursos y filtro con estado del tráfico y terminación VPN para sitios y usuarios remotos.

- ***Switch de Capa 2 (con soporte para VLAN privada).-*** asegura que la información desde los dispositivos de administración solamente puedan atravesar directamente al firewall.

Amenazas que combate este diseño:

- ***Acceso no autorizado.-*** combatido a través de los filtros del ISP y del firewall

- ***Ataques a la capa de aplicaciones.-*** combatidos a través de HIDS en los servidores públicos.

- ***Virus y troyanos.-*** combatidos a través del filtro de los contenidos de los correos electrónicos y de IDS de los hosts.

- ***Ataques a contraseñas.-*** servicios limitados disponibles para ataques por fuerza bruta, el sistema operativo e IDS pueden detectar la amenaza.

- ***Denegación de servicio.-*** CAR[35] en el contorno del ISP y los controles de configuración de TCP en el firewall limitan la exposición.

- ***Ataques de falsificación (spoofing) de IP.-*** los filtros de RFC 2827 y 1918 en el contorno de ISP y del firewall

- ***Rastreadores de paquetes (Packet Sniffers).-*** una infraestructura conmutada e IDS de hosts limita la exposición.

- ***Reconocimiento de la red.-*** HIDS detecta el reconocimiento, se filtran los protocolos para limitar la eficacia.

- ***Abuso de confianza.-*** un modelo de confianza restrictivo y VLAN privadas limitan los ataques basados en la confianza.

- ***Redireccionamiento de puertos.-*** los filtros restrictivos y el IDS de hosts limitan el ataque

3.1.1.2.3.2 Módulo WAN

De igual forma que en el Módulo de Internet, el diseño del Módulo WAN está basado en los requerimientos de conectividad externa referente a la conexión a otras redes establecido en el SLA. Los parámetros primordiales son la seguridad y la calidad de servicio de la conexión entre ambas redes, la red móvil y la red externa. Dependiendo de la seguridad y la calidad de servicio (QoS) que se desee en la conexión se proponen dos diseños uno basado en un link WAN privado y otro en IPsec VPN como se mencionó anteriormente.

La disponibilidad, rendimiento y seguridad de la conexión WAN será establecida con el administrador de la red externa a conectarse en un SLA. En el SLA se

[35] Committed Access Rate

establecen los detalles de los parámetros antes mencionados, relacionado al servicio proporcionado.

El Módulo WAN es utilizado cuando se requiere conexión a locaciones remotas sobre una red privada. Este módulo muestra la resistencia y la seguridad de la terminación de WAN. Utilizando la encapsulación de Frame Relay o si es viable IPsec VPN, el tráfico se enruta entre los sitios remotos y el sitio central.

El nivel de seguridad del Módulo WAN basado en un link WAN privado depende del nivel de confianza para los sitios remotos a los cuales se está conectando. La resistencia la proporciona la conexión dual desde el proveedor de servicios, a través de los routers, configurados con control de acceso de capa 3, al módulo Central-Distribución. La seguridad se proporciona utilizando las características de seguridad de IOS. Las listas de acceso entrantes aplicadas a la interfaz serial son usadas para bloquear todo el tráfico no deseado de la red móvil. Listas de acceso entrantes a la interfaz Ethernet son usadas para luego limitar que tráfico pasa desde la red móvil hacia los sitios remotos. Adicionalmente el tráfico puede ser cifrado a través del link WAN.

A continuación se muestra el diseño basado en un link WAN privado, mediante encapsulación de Frame Relay:

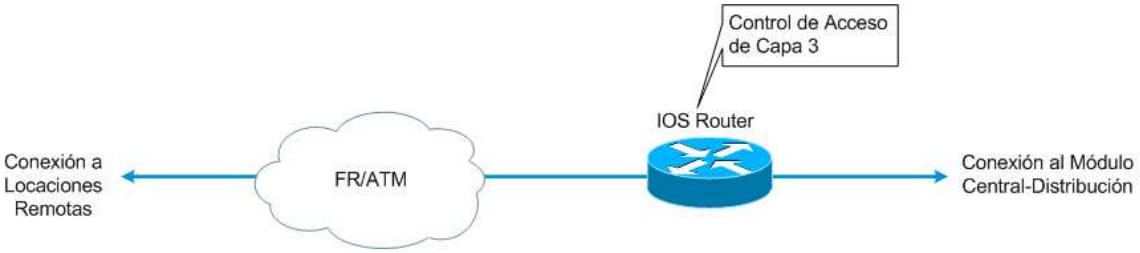

Figura 3-14: Módulo de WAN

Descripción de los dispositivos del diseño:

- ***Router IOS.-*** utiliza el enrutamiento, el control de accesos y mecanismos de QoS.

Amenazas que combate este diseño:

- ***Ataques de falsificación (spoofing) de IP.-*** combatidos a través de los filtros de la Capa 3.

- ***Acceso no autorizado.-*** el control de acceso simple del router puede limitar los tipos de protocolos a los que tienen acceso las redes externas con las que se establece conexión.

El diseño basado en el uso de IPsec VPN de ubicación a ubicación es realizado a través del módulo de Internet que como ya se explicó, dicho módulo está diseñado para soportar conexiones VPN, siendo en este caso innecesaria la implementación del módulo WAN.

3.1.1.3 Red de Datos

El diseño de la Red de Datos comprende los protocolos que van a ser usados en la red para el tráfico de la información. Los protocolos, su direccionamiento, enrutamiento y configuración son definidos de acuerdo a los requerimientos establecidos en el SLA referente a los grupos de usuarios que conforman la red. Para cada grupo de usuario se asigna una VLAN específica, la misma que es configurada de acuerdo a los permisos otorgados para caga grupo en el servidor RADIUS, además nos permite administrar y monitorear el número de clientes que se encuentra conectado en cada VLAN en un momento determinado.

Protocolos

El protocolo a usarse para la conexión entre subredes VLAN's, servidores y clientes es TCP/IP a partir del cual se configuran las respectivas direcciones asignadas a los elementos antes mencionados. Para el enrutamiento interno se usa el protocolo de Cisco EIGRP[36] el mismo que nos proporciona un enrutamiento

[36] Enhanced Interior Gateway Routing Protocol

dinámico, finalmente para la salida a Internet se utiliza el protocolo de gateway fronterizo BGP[37]. El protocolo para la comunicación del Módulo WAN depende del protocolo usado por la red con la cual se desea establecer la conexión, dicha especificación se establecerá en el SLA respectivo.

3.1.1.3.1 Direccionamiento

El tipo de red a usarse depende del número de usuarios definido en el SLA. Una vez definido el tipo de red se crean las diferentes VLAN's para cada grupo de usuario configurado en el servidor RADIUS, las VLAN's para los servidores y la VLAN para administración.

El número de VLAN's dependerá de la disponibilidad establecida y de los grupos de usuarios definidos en el SLA. Los permisos asignados para cada grupo de usuarios se citan en el segmento de Diseño de Seguridades desarrollado más adelante en este capítulo.

A continuación se muestra en la siguiente tabla los grupos de usuarios principales definidos en el SLA:

Grupos de Usuarios
Expositores
Congresistas
Periodistas
Invitados

Tabla 3-8: Grupos de Usuarios

Dependiendo del porcentaje de disponibilidad establecida en el SLA se determinará si cada servidor necesita de una subred única o no. Para los porcentajes de 98% y 99% todos los servidores estarán en una sola subred VLAN. Para los porcentajes de 99.5% y 99.9% a cada servidor se le asignará una

[37] Border Gateway Protocol

subred VLAN para asegurar la disponibilidad de los mismos. Dependiendo del nivel de seguridad se muestran el número de servidores empleados en las siguientes tablas:

Seguridad Alta:

Servidores
Servidor FTP/HTTP
Servidor de Correo Electrónico
Servidor DHCP
Servidor RADIUS
Servidor OTP

Tabla 3-9: Servidores para Red con Seguridad Alta

Seguridad Media y Baja:

Servidores
Servidor FTP/HTTP
Servidor de Correo Electrónico
Servidor DHCP
Servidor RADIUS

Tabla 3-10: Servidores para Red con Seguridad Media y Baja

Refiriéndonos a las consideraciones anteriores para el diseño de la red con disponibilidad y seguridad alta se requerirán de la implementación de 8 VLAN's. Si la red requiere disponibilidad baja y seguridad alta el número de VLAN's serán 5. Para una disponibilidad alta y seguridad Media o Baja el número de VLAN's serán 8. Para una disponibilidad baja y seguridad Media o Baja el número de VLAN's serán 5. Cabe señalar que no se consideran usuarios adicionales.

3.1.1.3.2 Enrutamiento

El enrutamiento en la red se realiza de dos formas: estático y dinámico. El enrutamiento estático se usa para la conexión a Internet hiendo del switch del módulo central al router con firewall del módulo de Internet y de este al router del ISP y viceversa. De igual forma se usa el enrutamiento estático para la conexión con redes externas hiendo del switch del módulo central al router del módulo WAN y de este a la red externa y viceversa. Adicionalmente el enrutamiento estático se usa para el enrutamiento entre subredes y servidores en el switch del módulo central.

El enrutamiento dinámico se usa para el enrutamiento entre los clientes de la red en el switch del módulo central, debido a la gran movilidad de los clientes y a la naturaleza de la red.

3.1.1.3.3 Configuración

La configuración de las direcciones IP's de los dispositivos tanto servidores como clientes, de la red se realiza de dos formas: estática y dinámica. La configuración de direcciones IP estática se usa para la asignación de IP’s a cada uno de los servidores de la red y a cada VLAN establecida según como se estableció en el segmento de Direccionamiento. La configuración de direcciones IP dinámica se usa para la asignación, a través de DHCP, de las direcciones IP’s para cada uno de los clientes de la red.

3.1.1.4 Aplicaciones

3.1.1.4.1 Servicio Web

Este servicio se establecerá en el servidor FTP/HTTP cuyas características y dimensionamiento se estableció en el Módulo de Servidores desarrollado previamente en este capítulo. El servicio Web estará disponible para todos los

usuarios de la red, con las respectivas restricciones para navegar a páginas con contenido sexual y las restricciones a puertos que utilizan los programas P2P y bittorrent.

Para proporcionar un gran rendimiento se considera el almacenamiento en caché de las páginas web visitadas con mayor frecuencia, debido al poco tiempo de funcionamiento de la red no se consideran políticas sobre la actualización de dichas páginas.

3.1.1.4.2 Servicio FTP

El servicio FTP permitirá a los usuarios descargar los archivos disponibles, de acuerdo a los permisos que dichos usuarios tengan dependiendo del grupo al que pertenezcan. De esta forma los archivos serán clasificados de acuerdo al interés y necesidad de cada uno de los grupos de usuarios ya establecidos. Se establecerá el tamaño máximo de los archivos para descarga en base al número de usuarios, con el propósito que la descarga de archivos demasiado grandes, no ocasionen cuellos de botella y degraden el rendimiento de la red. Este servicio reside en el servidor FTP/HTTP.

3.1.1.4.3 Servicio de Correo Electrónico

El correo electrónico será para uso externo e interno, y será un servicio temporal que durará el tiempo que dure el evento. Se limitará el tamaño del buzón y el tamaño máximo de los archivos adjuntos en función del número de usuarios, además se consideran las especificaciones de seguridad establecidas en el Módulo de Servidores, Módulo de Edificio y en el Módulo de Internet.

3.2 DISTRIBUCIÓN DE PUNTOS DE ACCESO

La distribución de los puntos de acceso se realiza basándonos en los requerimientos de despliegue establecidos en el Capítulo II. Se considera el diseño de las edificaciones, la tecnología seleccionada, las capacidades de rango y cobertura de los access points de acuerdo a la tecnología elegida y las áreas en donde se prestará el servicio.

Las edificaciones del CEQ no presentan problemas de atenuación y de interferencia. El Área de Exposiciones del CEQ tiene un techo alto y en su interior no existen edificaciones que puedan causar atenuación en la señal de los Access Points a ser distribuidos. El área de cafetería tampoco tiene edificaciones que puedan causar interferencia. Para el área de parqueaderos y descanso que son áreas exteriores, no existe problemas en la propagación de la señal ya que son áreas abiertas.

La tecnología seleccionada se indicó en el diseño de la Red de Infraestructura, luego de una respectiva comparación entre las tecnologías existentes. La tecnología elegida nos proporciona el número de access points a ser utilizados, las capacidades de rango y cobertura de los mismos indicados en el diseño de la Red de Infraestructura antes mencionada. Además considerando la movilidad de los usuarios se solapan los rangos de los Access Points para crear una señal más fuerte.

Se puede incrementar el throughput por usuario disminuyendo el número de usuarios litigantes, para el throughput agregado que es proporcionado por un solo Access Point. Esto se realiza añadiendo un segundo Access Point en un canal no solapado en la misma área de cobertura. Esto implica que se necesiten más access point por cada área. Adicionalmente se establece que cada access point manejará un número máximo de 25 usuarios, basándonos en las recomendaciones del documento “*Cisco Enterprise Distributed Wireless Solutions Reference Network Design*”.

La cobertura del servicio solamente se proporciona donde es requerido, la cantidad de cobertura en las áreas donde no sea requerido es minimizado por la colocación de los access points.

La distribución de los puntos de acceso es un proceso dinámico que requiere un constante monitoreo y depende de la densidad y movilidad de los clientes y del rendimiento de la red en un momento determinado. Dependiendo de la movilidad de los usuarios y del rendimiento de la red en cierto momento puede ser necesario que los access points deban ser reubicados, para esto nos basamos en la utilización del modelo de Gestión de Servicios de ITIL enfocándonos solamente en los bloques de *"Prestación de Servicios*" y "*Soporte a los Servicios"* y de la utilización de un sistema formal de gestión como COBIT en el cual nos enfocaremos en los dominios de "*Despliegue y Soporte"* y "*Monitoreo y Control"* con el fin de cumplir con los requisitos establecidos en el SLA.

Para la realización de este monitoreo constante y soporte de servicios se incluye en el diseño un dispositivo WLSE (Wireless LAN Solution Engine) el cual proporciona un rol crítico como una interfaz de alto nivel de administración con access points autónomos. El objetivo de WLSE es proporcionar integración en un solo dispositivo como también la configuración y administración de los access points de la red inalámbrica.

Las funcionalidades de WLSE se dividen en las siguientes áreas funcionales:

Configuración y Administración

- Administrar la configuración y software de los Access Points.
- Proporcionar un repositorio histórico de configuraciones

Administración de Seguridad

- Coleccionar y analizar información 802.11 recibida desde los clientes y los Access Points
- Asegurar la red inalámbrica de Access Points clientes mal intencionados.
- Reporte de eventos críticos vía SNMP o correo electrónico.

La inclusión del dispositivo WLSE Express se indicó en el diseño del Módulo de Edificio, para todos los diseños especificados en el mismo. El dispositivo WLSE Express es integrado con el servidor RADIUS y soporta hasta 100 Access Points. Tanto los access points como el WLSE deben comunicarse de una forma segura, para lo cual los access points deben estar configurados con direcciones IP estáticas y un único host name, además deben estar configurados para administración SNMP, las direcciones de los access points deben estar configurados en el WLSE en conjunto con la correcta cadena SNMP en el access point. De esta forma se puede administrar fácilmente un gran número de access points, sin tener que configurarlos o realizar cambios en cada uno de estos de forma individual. La configuración de WLSE se la realiza a través de una herramienta la misma que proporciona una interfaz GUI que crea la configuración que será aplicada a todos los access points.

La característica más importante para el desarrollo de nuestro diseño se centra en la capacidad de WLSE para generar reportes automáticamente y enviarlos a través de correo electrónico. Estos reportes están agrupados en las siguientes categorías:

- ***Reporte de Dispositivos.-*** genera reportes de dispositivos individuales, incluyendo configuración, defectos e historia. Además genera un resumen de reportes de todos los access points.

- ***Reportes de administración de señal.-*** el reporte de administración de señal es enfocado en el ambiente de radio de frecuencia y puede proporcionar reportes de señal de caminos perdidos, carga de canales y eventos de detección de radar.

- ***Reporte de Clientes.-*** genera reportes detallados de clientes, incluyendo la asociación/autenticación de clientes, eventos de roaming de los clientes y autenticación de clientes fallidos.

- ***Reporte de tendencias.-*** proporciona información histórica para medir la utilización de la red inalámbrica. Puede proporcionar estadísticas de la utilización de la señal, los clientes más frecuentes, las asociaciones más frecuentes, y otras capacidades relacionadas a los reportes.

- ***Reportes de tiempo real.-*** estos reportes son los más utilizados para la resolución de problemas de asistencia técnica en un access point específico, estos detallan el CPU, memoria, intentos de asociación, y utilización en tiempo real.

- ***Reportes en curso.-*** estos reportes pueden retorna la configuración o reportes de estado en grupos de access points. Estos reportes pueden resumir la configuración de un edificio, o alternativamente, reportar una lista de clientes asociados a un grupo de Access Points. Aplicando la capacidad para generar reportes de los grupos de usuarios, creados y especificados en el diseño de la Red de Datos, se puede generar muchos reportes personalizados.

A continuación se muestra la ubicación inicial de los access points considerando los parámetros antes indicados, considerando que la densidad de los clientes es uniforme para todas las áreas:

Figura 3-15: Distribución de puntos de acceso de acuerdo al área de cobertura

Área 1: Área de Exposiciones

Área 2: Área de Descanso

Área 3: Cafetería

Área 4: Parqueaderos

La ubicación de los access points mostrada no es una ubicación definitiva, ya que como se explicó anteriormente la distribución de los mismos es un proceso dinámico.

3.3 DISEÑO DE SEGURIDADES

Para el diseño de Seguridades emplearemos dos tipos de modelos de seguridades, que son aplicadas al diseño de la red. Los modelos de seguridades se usaron anteriormente en el diseño del Módulo de Edificio desarrollado en este capítulo, las cuales son EAP con TKIP e IPsec VPN, ambos modelos son implementados en conjunto con VLAN's.

A continuación se detalla el proceso de autenticación que es utilizado por cada modelo y la seguridad que los mismos brindan a la red en general. La especificación de los dispositivos utilizados y la mitigación de amenazas fueron explicadas en detalle en el diseño del Módulo de Edificio en donde se utilizaron ambos modelos.

3.3.1 EAP CON TKIP

Autenticación 802.1x/EAP

Consiste en el desarrollo de un framework que proporciona autenticación centralizada y distribución dinámica de claves. Este enfoque está basado en IEEE 802.11 en el grupo de trabajo "i" usando 802.1x y Extensible Authentication Protocol (EAP) para proporcionar esta funcionalidad aumentada. Los tres principales elementos de 802.1x y EAP se enfocan en las siguientes consideraciones:

- Autenticación mutua entre el cliente y el servidor RADIUS (Remote Access Dial-In User Service) de autenticación.
- Encriptación de claves dinámica, generada luego de la autenticación.

- Políticas centralizadas de control, donde las sesiones caducadas se reautentican mediante triggers y la generación de nuevas claves encriptadas.

Protocolos de Autenticación EAP

Numerosos tipos EAP están disponibles para la autenticación de usuario sobre redes cableadas e inalámbricas. Los principales protocolos son los siguientes:

EAP-Cisco Wireless (LEAP)
EAP-Transport Layer Security (EAP-TLS)
Protected EAP (PEAP)
EAP-Tunneled TLS (EAP-TTLS)
EAP-Subscriber Identity Module (EAP-SIM)

De los tipos anteriores, seleccionamos EAP-Cisco Wireless (LEAP) para el diseño de seguridad de la red dependiendo del nivel requerido, como ya se especificó en el Módulo de Edificio.

3.3.1.1 Cisco LEAP

Cisco LEAP soporta los tres elementos de 802.1x y EAP mencionados anteriormente, opera en la capa de conexión (Capa 2) para proporcionar autenticación, autorización, manejo de cuentas y codificación. Con LEAP, la autenticación mutua se basa en un secreto compartido, el password del usuario, el cual es conocido por el cliente y la red. El servidor RADIUS envía un desafío de autenticación al cliente. El cliente usa una combinación del password proporcionado por el usuario para modelar una respuesta al desafío y enviar dicha respuesta al servidor RADIUS. Usando información de la base de datos de usuarios, el servidor RADIUS crea su propia respuesta y la compara con la respuesta del cliente. Cuando el servidor RADIUS autentica al cliente, el proceso se realiza a la inversa, permitiendo al cliente autenticar al servidor RADIUS.

Cuando el proceso se ha completo, un mensaje EAP de éxito es enviado al cliente y ambos el cliente y el servidor RADIUS derivan la clave WEP dinámica.

La secuencia de eventos antes mencionados se detalla a continuación. Véase la Figura 3-16.

- Un cliente inalámbrico asociado con un access point, entre ambos se realiza encriptación en la capa de conexión.

- El access point bloquea todos los intentos del cliente para ganar acceso a los recursos de la red hasta que el cliente se autentifique en la red.

- El usuario en el cliente suministra sus credenciales de logeo de re (ID de usuario y password) vía un suplicante EAP.

- La autorización es controlada por la VLAN o por la admisión del grupo de usuario en combinación con accesos de control aplicados en el switch de capa 3 que limita la VLAN o el grupo de usuario.

- Usando 802.1x y EAP, el cliente inalámbrico y un servidor RADIUS en la red cableada desarrollan una mutua autenticación a través del access point en dos fases. En la primera fase de autenticación EAP, el servidor RADIUS verifica las credenciales del cliente, o viceversa. En la segunda fase la mutua autenticación es completada por el cliente verificando las credenciales del servidor RADIUS, o viceversa.

- Cuando la autenticación mutua es exitosamente completada, el servidor RADIUS y el cliente determinan una clave WEP que es distinta por cliente. El cliente carga esta clave y se prepara a usarla para su inicio de sesión.

- El servidor RADIUS envía la clave WEP, llamada clave de sesión, sobre la red cableada al access point.

- El access point codifica su clave broadcast con la clave de sesión y envía la clave codificada al cliente, el cual usa la clave de sesión para decodificarla.

- El cliente y el access point activan WEP y usan la clave de sesión y la clave broadcast WEP para todas las comunicaciones durante el resto de la sesión o hasta que se caduque la misma y nuevas claves WEP sean generadas.

- La clave de sesión y broadcast son cambiadas en intervalos regulares. El servidor RADIUS al final de la autenticación EAP especifica el tiempo de duración de las claves de sesión al access point y el tiempo de rotación de la clave broadcast puede ser configurada en el access point.

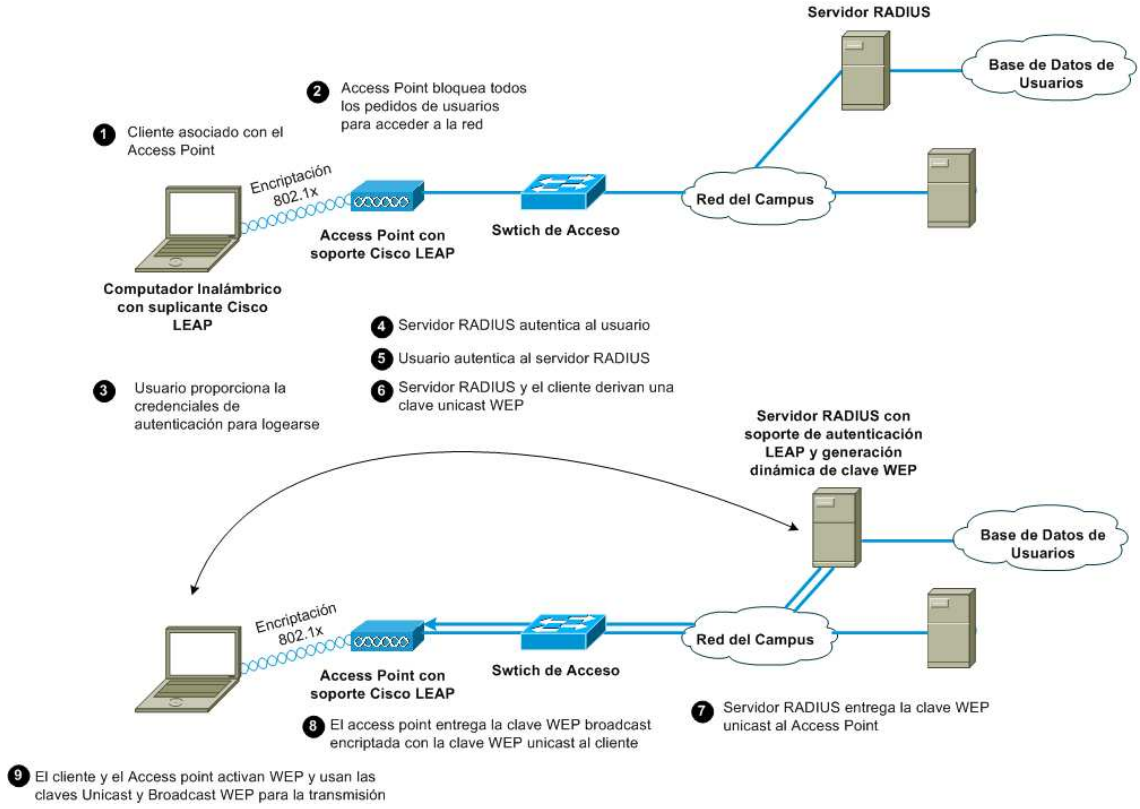

Figura 3-16: Proceso de autenticación LEAP

3.3.1.2 TKIP (Temporal Key Integrity Protocol)

Es un conjunto de mejoramientos de software basado en RC4 WEP, para mitigar las vulnerabilidades de WEP.

La mayoría de ataques contra WEP se basan en explotar múltiples vulnerabilidades en la inicialización de vectores. El uso de diferentes claves por paquete es una manera potencial de mitigar esta amenaza. Como se ilustra en la Figura 3-17, la inicialización del vector y la clave WEP son combinados para producir una clave de paquete única (llamada clave temporal), la cual es combinada con el vector de inicialización y corrida a través de una función matemática llamada XOR con el texto en claro.

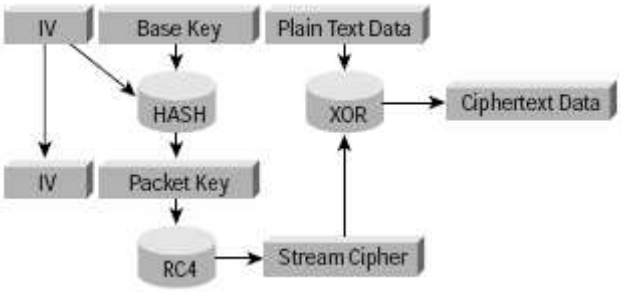

Figura 3-17: Codificación de claves con TKIP

Este escenario previene la inicialización de vectores vulnerables de ser usados para determinar la clave WEP. Para prevenir ataques debido a la colisión de inicialización de vectores, la clave base debe ser cambiada antes que se repita la inicialización de vectores. Porque la inicialización de vectores en una red ocupada puede repetirse en cuestión de horas, se determinó el uso de este modelo en conjunto con la autenticación EAP la misma que desempeña la operación de regenerar las claves.

La clave de transmisión, citada en la autenticación EAP es también susceptible a ataques debido a la colisión de inicialización de vectores. Los access point de Cisco soportan la rotación de claves de transmisión para mitigar esta vulnerabilidad, como se explicó anteriormente en la autenticación EAP.

Cisco TKIP—Message Integrity Check

Otra preocupación con WEP es su vulnerabilidad a los ataques de repetición. MIC protege a los frames de WEP que se dañen a si mismos. MIC está basado en un valor semilla, destinación MAC, y carga útil (es decir cualquier cambios para éstos que afectarán el valor de MIC). MIC está incluido en la encriptación WEP. MIC

usa un algoritmo de combinación que deriva el valor resultante. Este es un mejoramiento a la función de suma de control del chequeo de redundancia cíclica (CRC)-32 desarrollado por estándares basados en WEP.

3.3.2 IPSEC VPN

El uso de túneles IPsec VPN es una alternativa a la implementación de 802.1x/EAP. La razón de elegir esta implementación en lugar de 802.1x/EAP se debe a razones que implican mayor seguridad en la red, por lo que dicha implementación fue seleccionada para el diseño del Módulo de Edificio para un nivel de seguridad Alta. IPsec es un estándar bien arraigado que es aprobado por varias organizaciones de seguridad. La primera ventaja de una solución basada en IPsec VPN es el mecanismo de codificación. IPsec incluye soporte para 3DES (Triple Data Encryption Standard) y encriptación AES, mientras que 802.1x/EAP actualmente depende de WEP o WEP reservado más TKIP y MIC.

La topología de red hasta el concentrador VPN es considerado inseguro por lo cual una apropiada política de seguridad es creada, configurada y mantenida en todos los puntos que se encuentran en contacto con esta red insegura. La política de seguridad se basa en la utilización de firewalls personales en cada cliente.

La autenticación ocurre entre el cliente y el concentrador VPN. Múltiples tipos de autenticación son soportados por el framework IPsec. La encriptación ocurre en la capa de red usando 3DES o AES, y es negociada entre el cliente y el concentrador VPN.

Las capacidades de VPN proporcionan capacidades adicionales de seguridad relacionadas con AAA[38]:

[38] Authentication, Authorization, and Accounting services

La autorización es controlada por el concentrador VPN y es determinada al momento de la autenticación. Las políticas de acceso son proporcionadas por el servidor RADIUS mediante los permisos para grupos de usuarios.

Las cuentas de usuarios son proporcionadas por el servidor RADIUS y por el concentrador VPN.

A continuación se muestra el diagrama de autenticación para VPN:

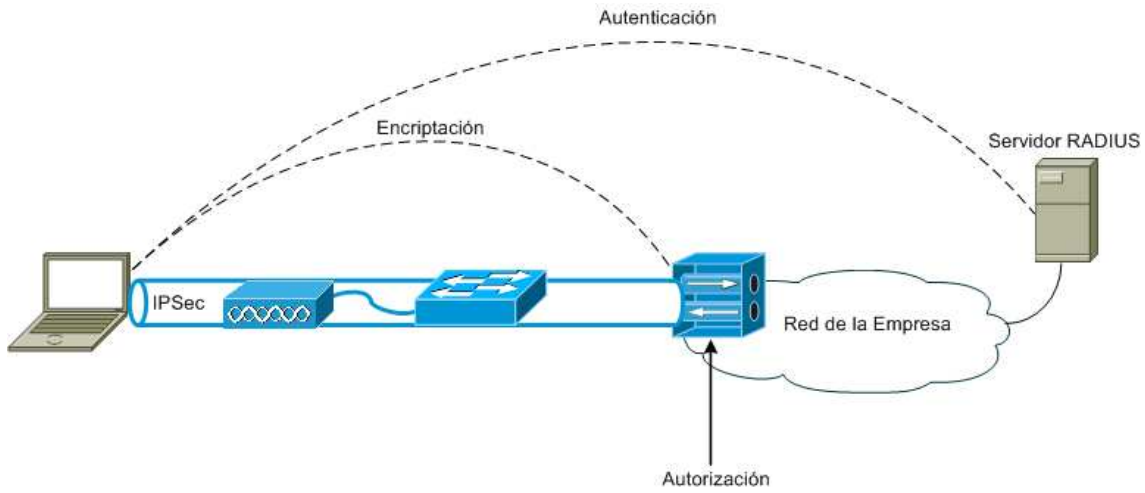

Figura 3-17: Proceso de autenticación IPsec VPN

El cliente IPsec VPN tiene varias características que ayudan a la transparencia para el usuario, proporcionando así servicios equivalentes a esos disponibles con la solución 802.1x/EAP, las cuales son:

- ***Auto iniciación.-*** El cliente VPN puede es configurado para ser iniciado automáticamente para rangos de direcciones particulares.

- ***Integración con el Sistema Operativo.-*** El cliente VPN puede capturar el nombre del usuario y el password al momento del logeo y usar esta información como parte del logeo del cliente VPN. Esto es similar al proceso usado en Cisco LEAP. Estas características unidas con el auto iniciación proporcionan un alto nivel de transparencia para el usuario.

3.3.3 VLAN

El uso de VLAN's en ambos modelos citados anteriormente, proporciona un nivel más de seguridad para el diseño de la red. A continuación se detalla la forma y las características que proporciona el uso de esta tecnología.

Simples o múltiples puentes virtuales pueden ser definidos en el switch de capa 3 del Módulo Central-Distribución. Cada puente virtual creado en el switch define un nuevo dominio de transmisión (VLAN). Las interfaces del switch asignadas manualmente a las VLAN's son enviadas como VLAN's basadas en interfaz o VLAN's basadas en admisiones estáticas. Estas VLAN's están asociadas con subredes IP definidas en el diseño de la Red de Datos. El switch de capa 3 utilizado en los diseños no enruta el tráfico de transmisión de una VLAN a otra.

Con el uso de Cisco Access Points, se puede determinar el protocolo de enlace 802.1q en cada uno de ellos, permitiendo el acceso de hasta 16 VLAN's cableadas, asociadas a cada grupo de usuario definidos previamente en el diseño de la Red de Datos. Un único SSID (Service Set Identifier) define una VLAN inalámbrica en el Access Point. Cada SSID es correlacionado a un ID-VLAN en la parte cableada.

Para cada VLAN se establecen políticas de seguridad, de acuerdo a los grupos de usuarios que operarán en la red y citadas en el desarrollo de este capítulo. Las políticas son definidas en los Access Points con el propósito de establecer restricciones apropiadas para cada VLAN. Los siguientes parámetros son configurados en el SSID (VLAN inalámbrica):

- ***Nombre SSID.-*** Configura un único nombre por cada VLAN inalámbrica
- ***VLAN ID por defecto.-*** VLAN ID por defecto correlacionado en el segmento cableado.
- ***Tipos de Autenticación.-*** Solamente se utiliza Cisco-EAP con TKIP para todos los diseños.

- ***Autenticación MAC.-*** a través del uso de EAP.

- ***Autenticación EAP.-*** varios tipos de EAP, se usa Cisco-EAP para todos los diseños.

- ***Número máximo de asociaciones.-*** capacidad de determinar el número máximo de clientes por SSID.

Los siguientes parámetros son configurados en el segmento VLAN cableado:

- ***Encriptación de Clave.-*** Esta es la clave usada para el tráfico por cada VLAN. El tipo de autenticación utilizada para todas las VLAN's es EAP con TKIP.

- ***Políticas de Seguridad por grupo.-*** Aplicación de políticas de seguridad para cada grupo por VLAN. Los permisos para cada grupo de usuarios definidos son establecidos en el servidor RADIUS. Cada filtro (dentro de cada grupo) puede ser configurado para permitir o negar cierto tipo de tráfico.

En la siguiente tabla se muestran las VLAN's con su respectivo SSID para los posibles grupos de usuarios que utilizarán los servicios de la red, y su tipo de autenticación para cada una, como se estableció en el diseño de la Red de Datos.

SSID	*Tipo de Autenticación*
Expositores	EAP Cisco con TKIP
Congresistas	EAP Cisco con TKIP
Periodistas	EAP Cisco con TKIP
Invitados	EAP Cisco con TKIP

Tabla 3-11: Tipo de Autenticación de cada VLAN

En el diseño de la Red de Datos se estableció la creación de una VLAN para la administración, la cual también es conocida como la VLAN nativa/por defecto. Esta VLAN está configurada y relacionada a la VLAN del enlace cableado lo cual

permite al Access Point recibir y comunicarse usando IAPP (Inter-Access Point Protocol) con otros Access Point en la misma red inalámbrica. Todo el tráfico de administración ruteado al Access Point se lo realiza a través de la VLAN nativa. El acceso a esta VLAN es restringido mediante el Switch de Capa 3 del Módulo Central-Distribución a través del uso de ACL's. A continuación se muestra el diseño lógico, con la inclusión de la VLAN de Administración:

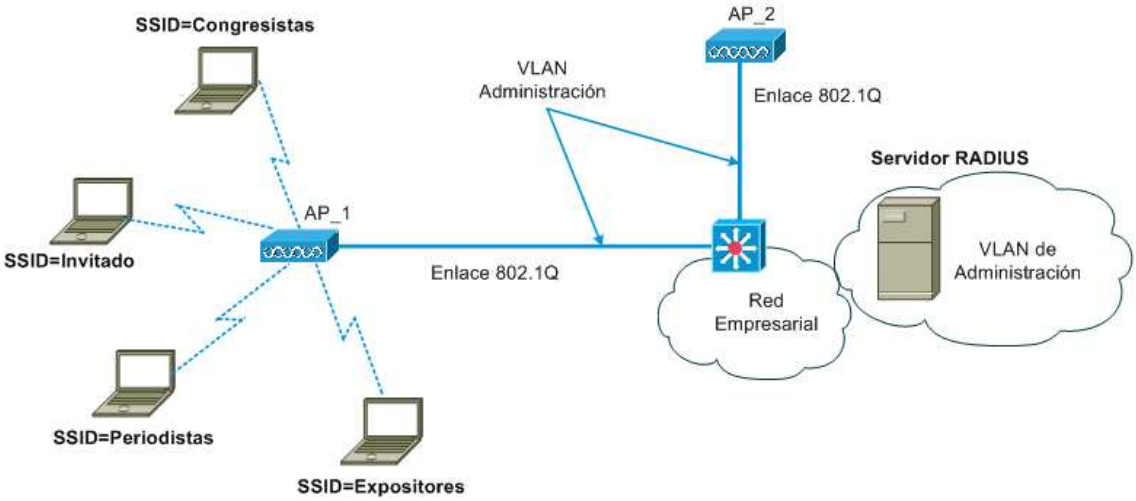

Figura 3-18: Diseño lógico de VLAN's

Como se especificó anteriormente la implementación de las VLAN's están basadas en el servidor RADIUS para el control de acceso usando 802.1x. Esto permite que cada grupo de usuario este asignado a una sola VLAN, por lo tanto no tenga acceso a las demás VLAN's .

Luego de una exitosa autenticación el servidor RADIUS asigna al usuario un predeterminado VLAN-ID en el segmento cableado. El SSID usado para el acceso WLAN no importa porque el usuario siempre está asignado a su VLAN-ID predeterminado. Esto permite que el servicio sea transparente para el usuario.

A continuación se muestra el modo en que se realiza el proceso antes mencionado:

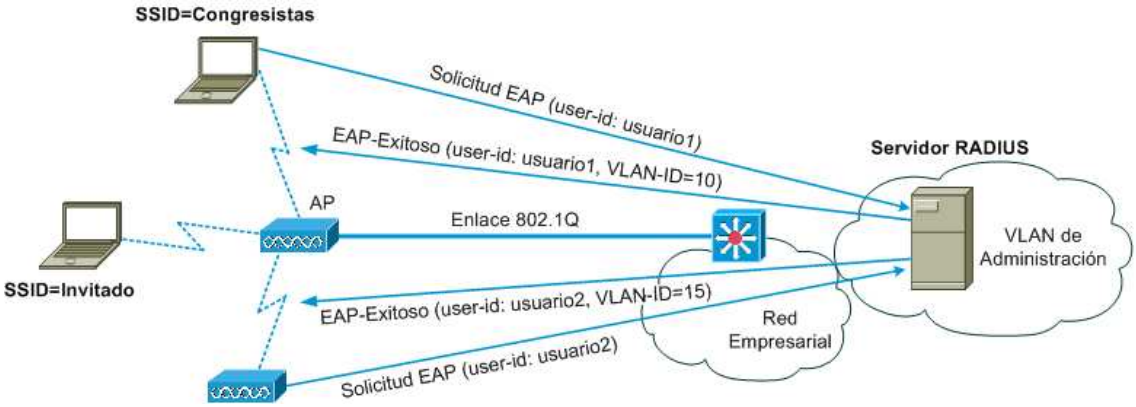

Figura 3-19: Autenticación usando VLAN's

Como se puede apreciar en el gráfico anterior dos usuarios denominados usuario1 y usuario2, luego de una exitosa autenticación son asignados a su respectivo VLAN-ID predeterminados con anterioridad y por lo tanto no pueden acceder a ninguna otra VLAN.

El uso de VLAN's es detallado específicamente para cada uno de los diseños establecidos en el Módulo de Edificio.

Criterios para la asignación de Permisos para los diferentes grupos de usuarios

- Todos los usuarios tendrán acceso a Internet. Se realiza el bloqueo de direcciones a páginas con contenido sexual, bloqueo de puertos para aquellos programas que permitan la descarga de música, programas, películas, etc.

- Los grupos de Expositores, Congresistas y Periodistas podrán descargar archivos que estén asignados a su respectivo grupo. El grupo de Invitados no podrá realizar la descarga de ningún archivo.

- El servicio de correo electrónico está disponible solamente para los grupos de Congresistas y Expositores.

- Se establece el estándar del uso de claves fuertes, las mismas que deben tener una longitud mínima de 6 caracteres, los mismos que deben ser una

combinación de letras mayúsculas, minúsculas, números y signos (¡, #, €, @, etc.). El grupo de Invitados no tiene clave.

3.4 APLICACIÓN DEL DISEÑO PARA EL CEQ (CENTRO DE EXPOSICIONES QUITO)

Una vez realizado el diseño de la Red de Infraestructura, Distribución de los Puntos de Acceso y el Diseño de Seguridades, aplicaremos en conjunto los diseños antes mencionados, que fueron desarrollados a lo largo de este capítulo, como caso de estudio al Centro de Exposiciones Quito (CEQ).

Se presentarán alternativas de diseño de acuerdo al nivel de seguridad, disponibilidad y requerimientos de las aplicaciones que requiere la red. Primeramente se considerará valores ficticios para las variables independientes relacionadas al número de usuarios, las aplicaciones y los parámetros definidos en los SLA's. Como resultado obtendremos un diseño en el cual se considerarán la Seguridad, Disponibilidad y Rendimiento. Luego se presentarán los diseños de la red en base a los diferentes niveles de seguridad y disponibilidad que se nos podría presentar.

Para definir el rendimiento de la red estableceremos las variables independientes relacionadas al número de usuarios y a las aplicaciones. Una vez definidos los diseños en base a los niveles de seguridad y disponibilidad procederemos a realizar un solo diseño en conjunto con el rendimiento de las aplicaciones asignando valores ficticios al número de usuarios y las aplicaciones. Se considera para este diseño una Seguridad Media y una disponibilidad de 99%. Las áreas de cobertura donde se necesita el servicio son todas aquellas definidas en el SLA.

A continuación se muestran dichos valores:

DATOS	
Evento:	***Contacto:***
Dirección del Contacto (Empresa):	
Teléfono:	***e-mail:***
Celular:	***Fax:***
SELECCIÓN DE APLICACIONES	
Aplicaciones: ☑ Web ☐ FTP ☑ E-mail	
Horas de operación:	
Número de Usuarios: Mínimo: **80** Máximo: **130**	
CONECTIVIDAD EXTERNA	
A otras redes ☐ Si ☑ No	

Tabla 3-12: Selección de Aplicaciones y Definición de número de usuarios

La tecnología seleccionada es 802.11g con una velocidad de transferencia de 54Mbps, considerando el número de usuarios y las aplicaciones definidas en la tabla anterior. A continuación se muestra el diseño de la red considerando los requerimientos anteriores:

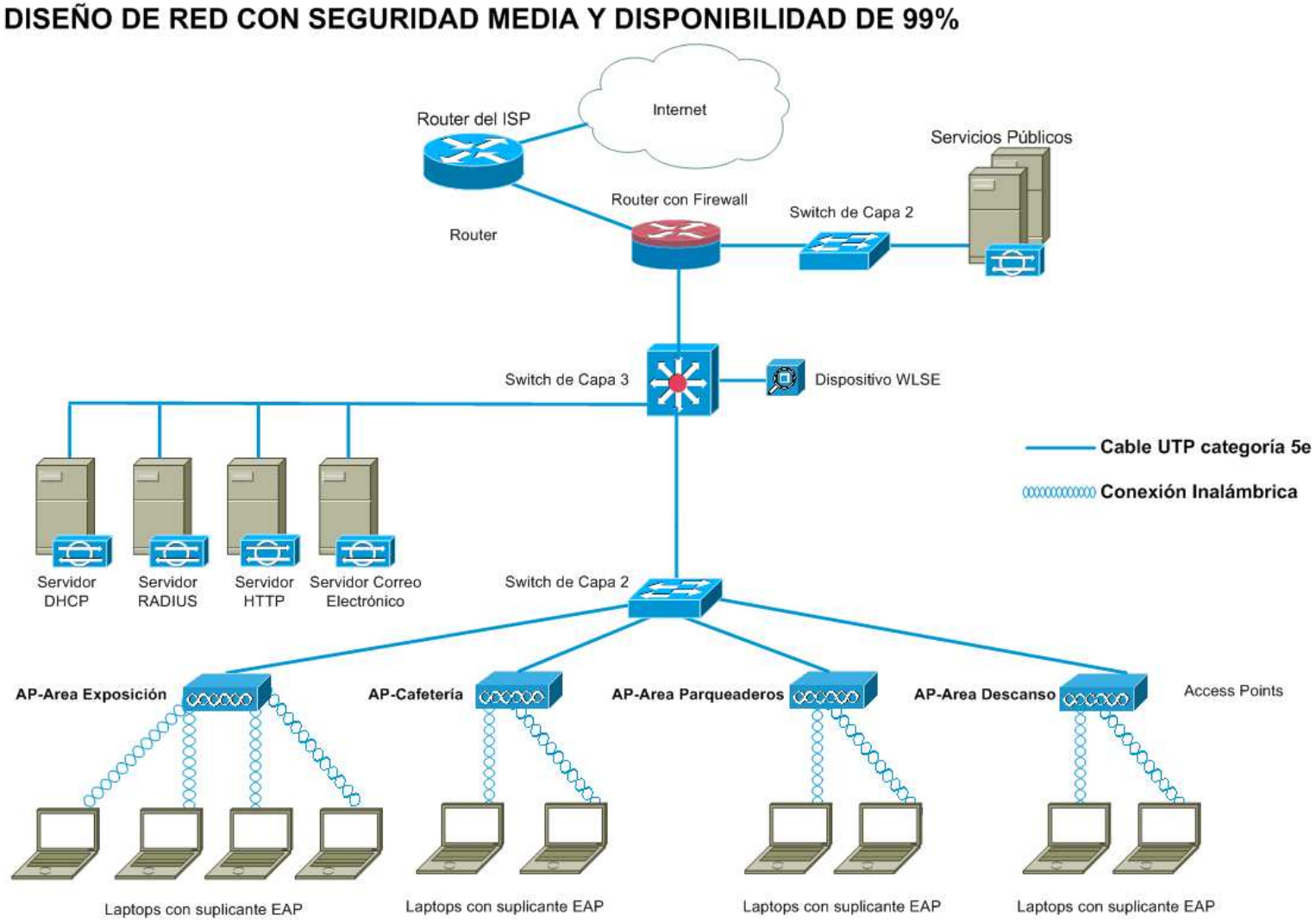

Figura 3-25: Diseño de Red con Seguridad Media y Disponibilidad 99%

A continuación se muestra la distribución inicial de los puntos de acceso en las áreas de cobertura en base a la tecnología 802.11g.

A continuación se muestran los Diseños de la Red Móvil para los diferentes niveles de Seguridad y Disponibilidad que se nos podría presentar:

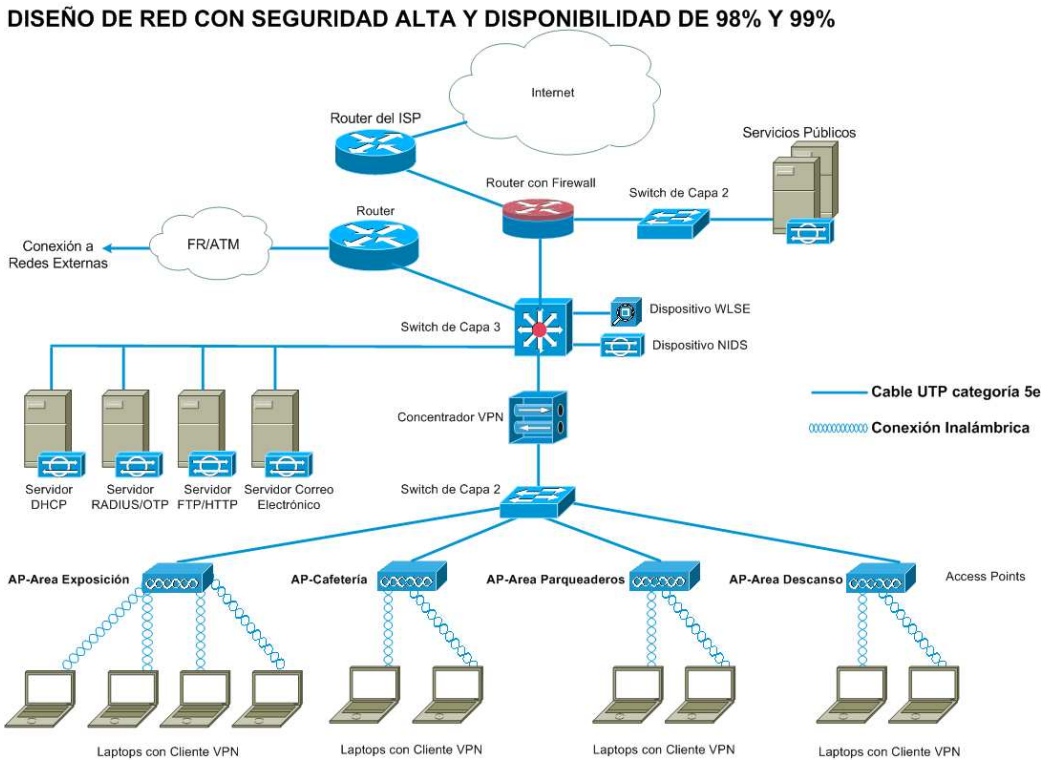

Figura 3-19: Diseño de Red con Seguridad Alta y Disponibilidad de 98% y 99%

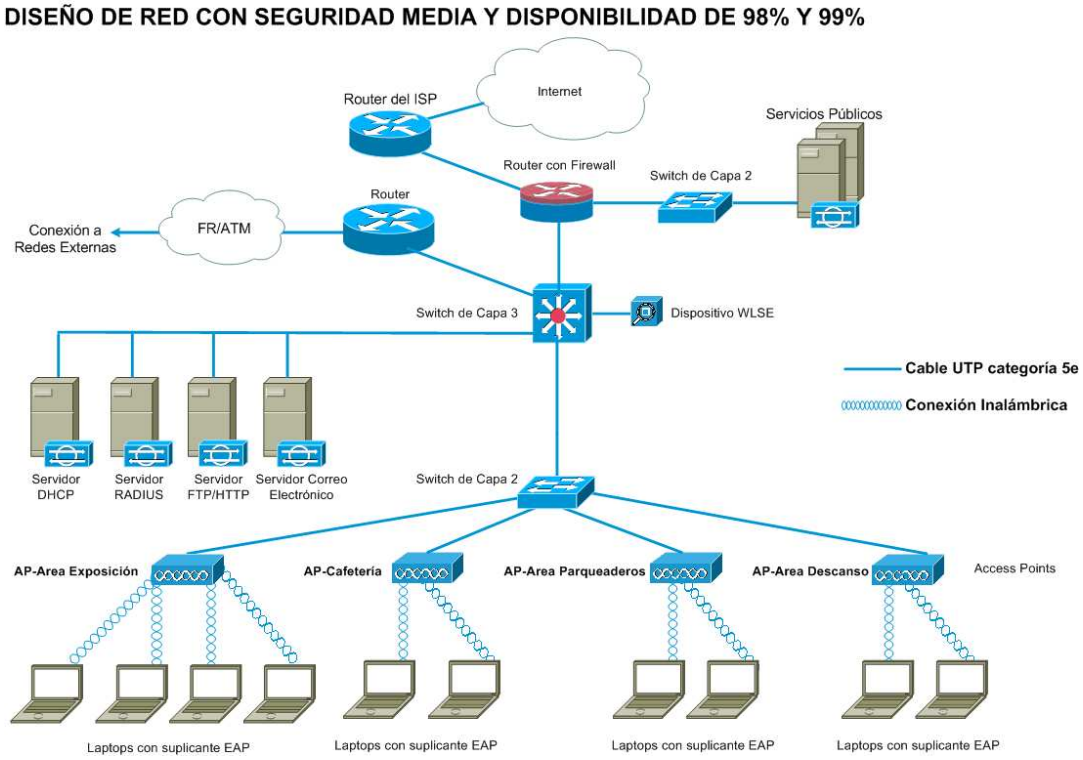

Figura 3-20: Diseño de Red con Seguridad Media y Disponibilidad de 98% y 99%

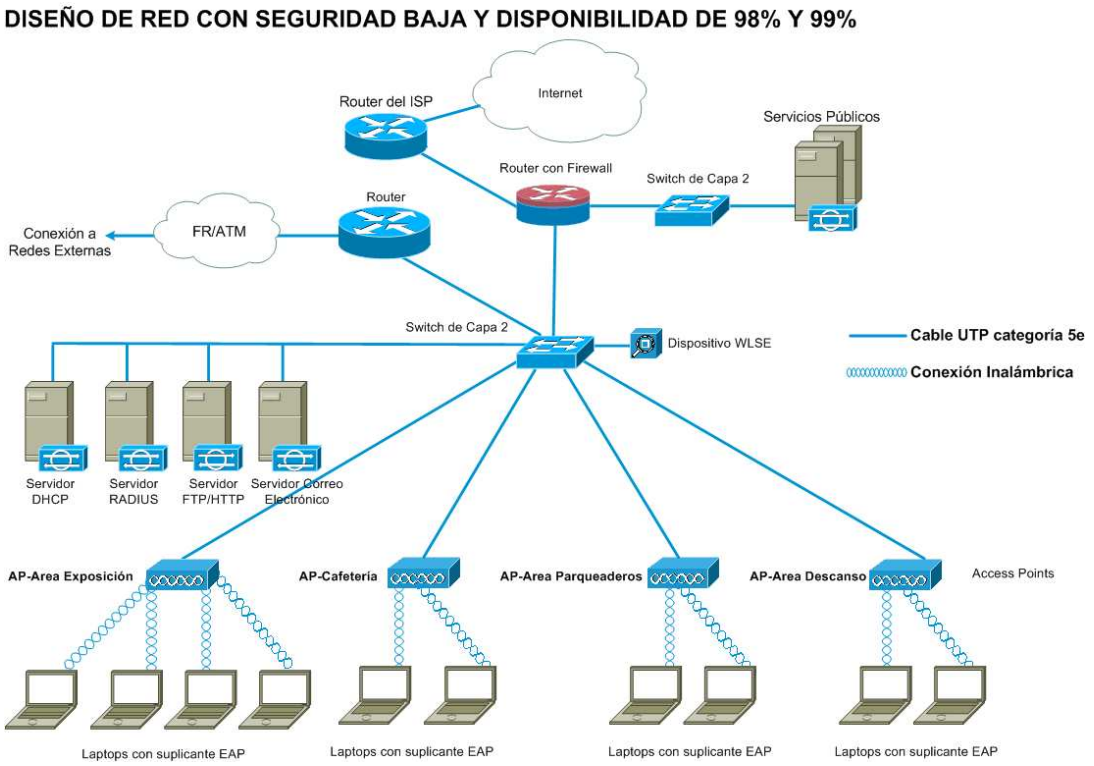

Figura 3-21: Diseño de Red con Seguridad Baja y Disponibilidad de 98% y 99%

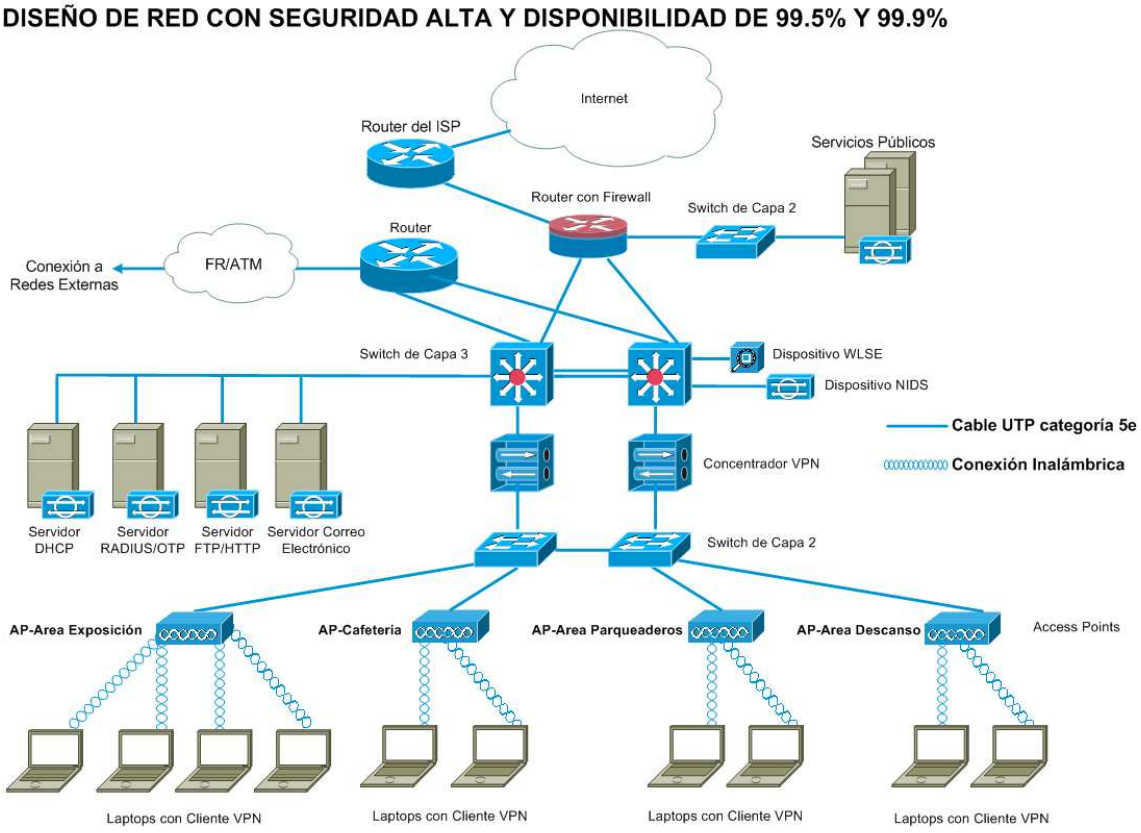

Figura 3-22: Diseño de Red con Seguridad Alta y Disponibilidad de 99.5% y 99.9%

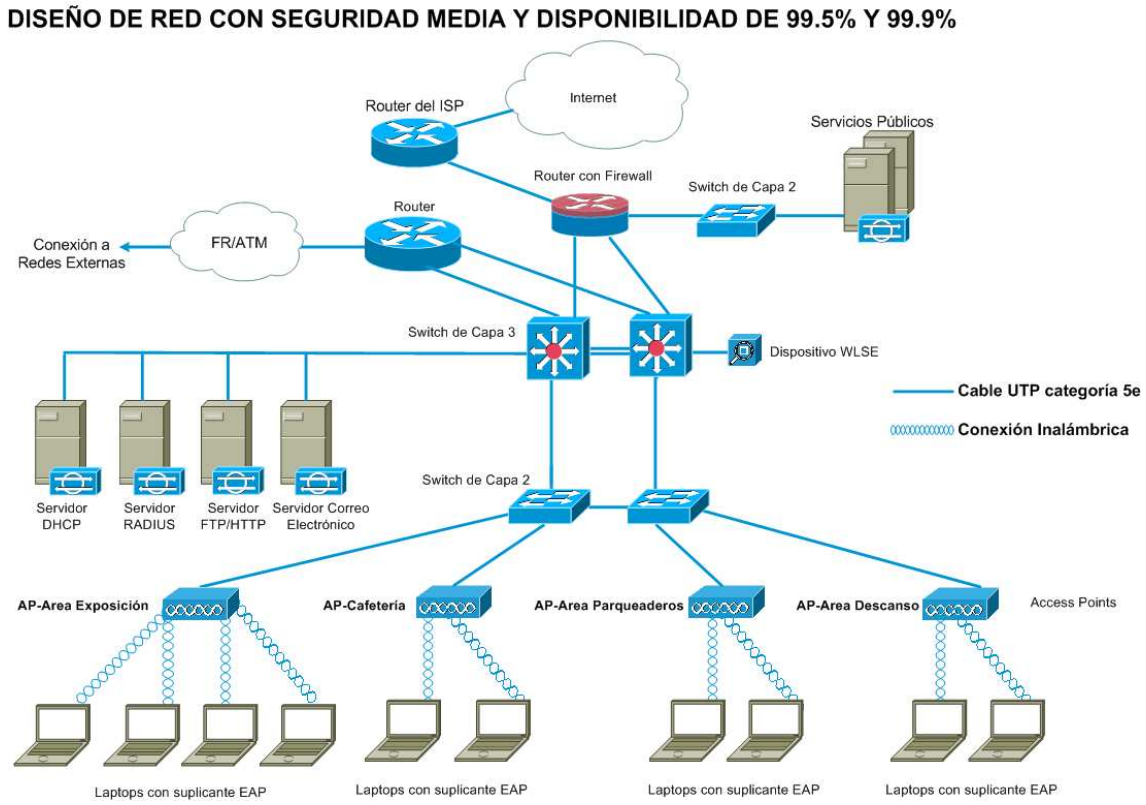

Figura 3-23: Diseño de Red con Seguridad Media y Disponibilidad de 99.5% y 99.9%

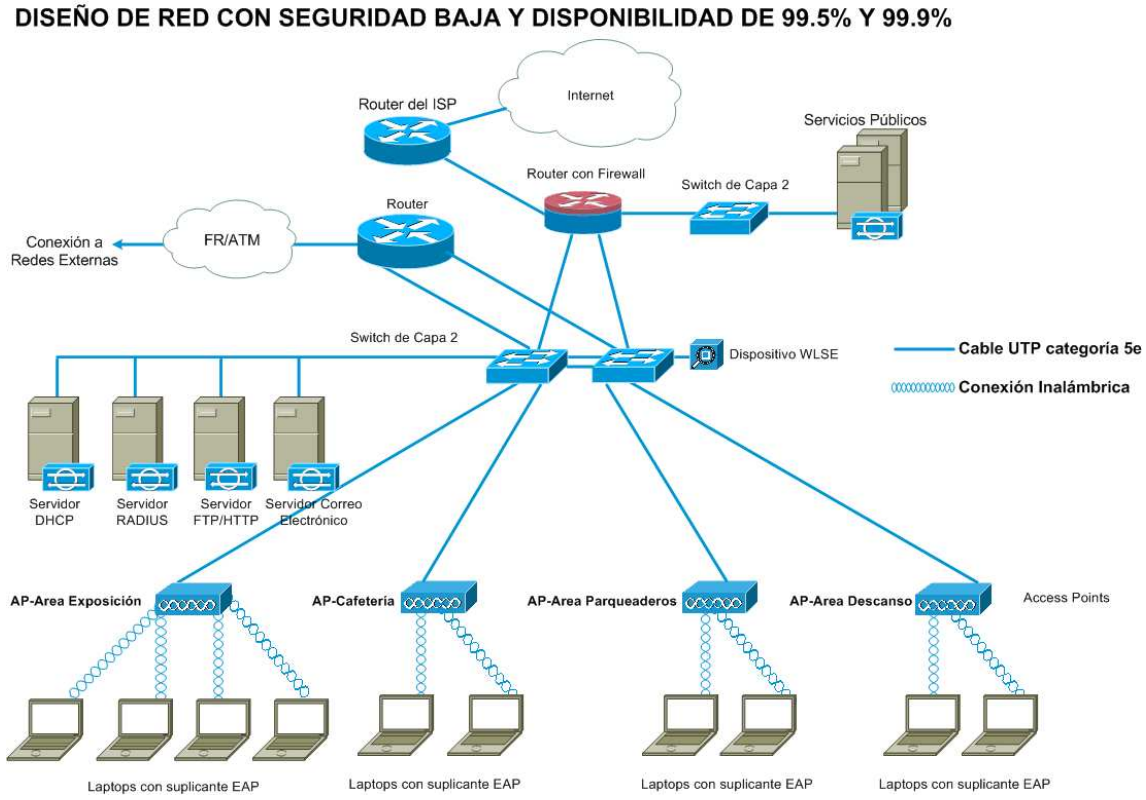

Figura 3-24: Diseño de Red con Seguridad Baja y Disponibilidad de 99.5% y 99.9%

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Los diseños de seguridad de la red fueron realizados basándonos en tres aspectos; primeramente mediante el uso de una arquitectura modular de seguridad, SAFE y su respectiva extensión par redes inalámbricas SAFE PARA WIRELESS; segundo con el uso de modelos de seguridad para la autenticación de usuarios como EAP, TKIP e IPsec VPN; y por último mediante el uso de segmentación de información de usuarios e información de administración a través de VLAN's.

La utilización del modelo OSI en conjunto con la arquitectura de seguridad SAFE con su extensión para redes inalámbricas, nos permitió obtener como resultado un diseño de red modular basado en varios niveles de seguridad y disponibilidad como lo podemos observar en capitulo 3.

El análisis de requerimientos fue realizado mediante el uso de SLA's, debido a que no todos los eventos o congresos a ser realizados tienen los mismos requerimientos sobre los servicios que necesitan. Por lo cual es imprescindible llenar un acuerdo de nivel de servicios donde el usuario pueda escoger sus diferentes necesidades de servicios, como lo podemos observar en la sección 3.4 y además en los anexos.

Debido al corto tiempo de funcionamiento de las redes móviles ad-hoc, no se incluye en el diseño un módulo de administración como lo especifica la arquitectura SAFE, en su lugar se emplea el uso de un monitoreo constante y el uso de reportes para la administración de la red.

El uso del modelo de Gestión de Servicios de ITIL nos permitió el manejo de los servicios proporcionados utilizando solamente los bloques relacionados a la *"Prestación de Servicios*" y "*Soporte a los Servicios"* debido al funcionamiento temporal de la red.

Gracias a la modularización que nos proporciona SAFE podemos efectuar un diseño detallado por cada sección de la infraestructura, además si se encontrara un problema podríamos localizarlo fácilmente y de la misma forma solucionarlo.

4.2 RECOMENDACIONES

Los diseños de la red móvil presentados en este trabajo no son diseños definitivos, o diseños que deban ser seguidos estrictamente, los mismos pueden estar sujetos a cambios que sean factibles en cada uno de los módulos diseñados al momento de ser implementados, pero se recomienda que sean usados como diseños base para su implementación.

Los diseños establecidos no garantizan que las redes sean 100% seguras, los diseños proporcionan un alto grado de seguridad, pero se recomienda que los mismos sean implementados en conjunto con políticas de seguridad las cuales depende de la organización en donde vayan a ser implementados.

Todas las modificaciones y requerimientos adicionales que sean realizados a los SLA's presentados en este proyecto, se recomienda que sean elaborados dentro de los parámetros citados en el desarrollo de los mismos.

BIBLIOGRAFÍA

TESIS:

[1] MUÑOZ, Cristina; TORRES, Jenny. Análisis y Diseño Orientado a Servicios de una Red Wlan para el Campus de la EPN. Código: 010902. Septiembre 2006.

LIBROS:

[2] WHEAT, Jeffrey; HISER, Randy; TUCKER, Jackie; NEELY, Alicia; MCCULLOUGH, Andy. Designing a Wireless Network. Syngress Publishing, Inc. ISBN: 1-928994-45-8. 2001.

[3] OUELLET, Eric; PADJEN, Robert; PFUND, Arthur; FULLER, Ron; BLANKENSHIP, Tim. Building a Cisco Wireless LAN. Syngress Publishing, Inc. ISBN: 1-928994-58-X. 2002.

[4] BASAGNI, Stefano; CONTI, Marco; GIORDANO, Silvia; STOJMENOVIC, Ivan. Mobile Ad Hoc Networking. John Wiley & Sons, Inc. ISBN: 0-471-37313-3. 2004.

[5] MOHAPATRA, Prasant; KRISHNAMURTHY, Srikanth V. AD HOC NETWORKS Technologies and Protocols. Springer.ISBN: 0-387-22689-3. 2005.

[6] ILYAS, Mohammad. The Handbook of Ad Hoc Wireless Networks. CRC Press. ISBN: 0-8493-1332-5. 2003.

WHITE PAPERS:

[7] CONVERY, Sean; TRUDEL, Bernie. SAFE: A Security Blueprint for Enterprise Networks. Cisco Systems, 2000.

[8] CONVERY, Sean; SAVILLE, Roland. SAFE Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. Cisco Systems, 2001.

[9] CONVERY, Sean; MILLER, Darrin; SUNDARALINGAM, Sri; DOERING, Mark; ROSHAN, Pej; ALBERT, Stacey; McMURDO, Bruce; HALPERN, Jason. Cisco SAFE: Wireless LAN Security in Depth. Cisco Systems, 2003.

[10] Cisco Enterprise Distributed Wireless Solutions Reference Network Design. Cisco Systems, 2005.

WEB:

[11] SPEC. http://www.spec.org.

[12] ITIL. http://www.itil.

[13] CISCO SYSTEMS. http://www.cisco.com