FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

REINGENIERÍA DE LA RED CONMUTADA E IMPLEMENTACIÓN DE UNA SOLUCIÓN QUE PERMITA SERVICIOS DE RED BASADOS EN IDENTIDAD (IBNS) PARA LA AEROLÍNEA TAME EN SU EDIFICIO MATRIZ.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones

Profesor guía

Ing. Mario Andrés Jaramillo Astudillo

Autores

Mayra Lucía Álvarez Figueroa
César Luis Valdivieso Salazar

Año

2014

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con los estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Mario Andrés Jaramillo Astudillo
Ingeniero
CI: 0102424207

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____	_____
Mayra Lucía Álvarez Figueroa	César Luis Valdivieso Salazar
CI: 1104398522	CI: 1722734801

AGRADECIMIENTOS

A mi madre, por ser siempre el apoyo que necesito, por sus palabras de aliento y por siempre estar para mí.

A mis hermanos por su ayuda de siempre, porque de una u otra manera me ayudan y alientan a continuar siempre con una sonrisa.

Al Ing. Mario Jaramillo por ser un excelente docente por compartir su conocimiento y por guiarnos en la elaboración del presente proyecto de la mejor manera.

A ti César, por ayudarme siempre por ser mi complemento y mi apoyo incondicional.

Mayra

AGRADECIMIENTOS

A mis papis Luis y Rosalía por su esfuerzo y apoyo, quienes nunca han dejado de esforzarse a pesar de las dificultades de la vida y de quienes aprendí a nunca dejarme vencer, yo solo soy el resultado de su esfuerzo.

A la familia Megasupply S.A. donde me estoy formando profesionalmente, donde se encuentran los mejores especialistas y donde encontré más que un trabajo, una familia.

A mi esposa Mayra Álvarez por estar conmigo en las buenas y en las malas, te amo!!

César Valdivieso Salazar

DEDICATORIA

El esfuerzo de este trabajo va dedicado a mi esposo por la paciencia, por el amor y sobre todo por ser el motor de mi vida impulsándome y empujándome a siempre continuar eres lo mejor que me ha pasado Te amo.

A mi papi por sus bendiciones y cuidados y por desde el cielo siempre guiarme por el mejor camino.

A mis 4 sobrinos porque con su inocencia ternura y travesuras alegran cada uno de mis días.

Mayra

DEDICATORIA

A las personas que siempre confiaron en mí: mis papis, mi familia y mis amigos, en especial a mi mami, la Dra. Rosalía Salazar por ser un ejemplo a seguir y la mejor mamá del mundo.

A mis ñañitas María Fernanda y Dianita Carolina, ustedes son la inspiración para alcanzar mis objetivos y metas.

A mi esposa Mayra Álvarez por ser mi mano derecha, mi mejor amiga y mi confidente, además de demostrarme con su amor y ternura que el mundo es un lugar hermoso para vivir.

A mi abuelito César, espero que desde el cielo me veas y estés orgulloso de mí.

César Valdivieso Salazar

RESUMEN

El presente proyecto está enfocado en mejorar el rendimiento de la red y la seguridad de la información de la empresa TAME EP en su edificio matriz, debido a que en la actualidad cuenta con una infraestructura de red que no permite brindar un servicio eficaz y cuenta con un deficiente sistema de seguridad de la información a nivel interno, lo que pone en riesgo su información sensible y la disponibilidad de los servicios; con ello pierde la capacidad de brindar un servicio óptimo y de calidad a sus empleados y clientes.

Como punto de partida se estableció diferentes fases para poder cumplir con el objetivo. En el primer capítulo, se presenta los conceptos básicos de cada tema concerniente al proyecto, con el objeto de aclarar los fundamentos teóricos para la realización del mismo.

En segundo capítulo, se realizó un levantamiento de información en sitio, lo que permite identificar las principales vulnerabilidades, falencias y puntos críticos. Se detalla el estado actual de la red conmutada, de la seguridad perimetral, seguridad interna; adicional se presenta un diseño que muestra la topología actual de la red.

En el tercer capítulo, se expone el nuevo diseño de la red conmutada y del servicio de red basado en identidad (IBNS), con el que se busca solventar los problemas y falencias encontrados en el capítulo anterior.

En el cuarto capítulo, se presenta un análisis técnico económico del proyecto, en el que se detalla los diferentes componentes, servicios y equipos con su respectivo valor económico en el mercado, que son necesarios para poder plasmar la solución presentada.

En el quinto capítulo se realiza y se documenta la implementación del nuevo diseño descrito en el capítulo tres, se configuran los diferentes equipos, se ejecutan distintas pruebas y se realizan afinamientos hasta verificar la correcta

operación de la nueva red conmutada y del servicio de red basado en identidad.

Para finalizar con el proyecto, en el sexto capítulo se listan las conclusiones más importantes y recomendaciones que se obtuvieron como fruto de la realización e implementación del presente proyecto.

ABSTRACT

This project focuses on improving the performance of the network and security of the information of enterprise TAME EP in its parent building, because the actual network infrastructure is unable to provide an effective service and has a poor internal system of information security, putting at risk the sensitive information and the availability of services; thereby loses the ability to provide superior and quality service to its employees and customers.

As a starting point different phases to meet the goal were established. In the first chapter, the basic concepts of each topic concerning the project were presented, in order to clarify the theoretical foundations for the realization of this project.

In the second chapter, gathering information on site was performed, allowing to identify key vulnerabilities, flaws and critical points. The current state of the switched network, perimeter security and internal security were detailed. Additional design is presented that shows the current network topology.

The third chapter presents the new design of the switched network and Identity Based Networking Services (IBNS), with which it seeks to solve the problems and shortcomings encountered in the previous chapter.

In the fourth chapter, a financial technical analysis of the project was made, this chapter specifies the different components, services and equipment with their economic value in the market, which are necessary to implement the solution presented.

The fifth chapter describes the implementation of the new design that was documented in chapter three, the different configuration are set, different tests run and tune-ups are performed to verify proper operation of the new switched network and Identity Based Networking Services (IBNS).

To finish the project, in the sixth chapter the main conclusions and recommendations, that were obtained as the result of the completion and implementations of this project, are listed.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

TAME EP es una empresa que brinda servicios aéreos, con presencia en algunos países de América Latina y en el Ecuador desde el año 1962. Se especializa en fomentar el desarrollo comercial, social, turístico y cultural; actualmente cuenta con varias sucursales a nivel nacional, la matriz está ubicada en Quito en la avenida Amazonas y Colón y una de sus sucursales principales está ubicada en el nuevo aeropuerto de Quito en Tababela.

TAME EP ha logrado establecerse como una empresa seria y confiable, además, al ser el único medio de transporte aéreo en algunas zonas del país, es necesario que su información y los servicios que oferta tengan la mayor disponibilidad posible. TAME EP necesita una infraestructura de red de primer nivel para que sus usuarios, internos y externos puedan obtener la información de una manera clara, eficaz y segura.

El manejo de información sensible de cualquier entidad, sea ésta pública o privada, es un factor determinante y esencial para el buen funcionamiento y operación de la empresa. Toda red de información presenta vulnerabilidades ya sean internas o externas que implican un riesgo informático en especial para la información confidencial y para la disponibilidad de servicios. No se puede asegurar una red al 100% ya que la seguridad de información es un proceso dinámico y evolutivo pero se puede aumentar el nivel de seguridad de la red previniendo ataques y pérdida de información al mínimo.

Debido a que las amenazas en seguridad, las habilidades y herramientas que utilizan los atacantes son más sofisticadas, las empresas buscan fortalecer día a día su sistema de seguridad y TAME EP no es la excepción, ya que la seguridad de la información juega un papel vital para mantener la confianza de los usuarios y poder brindar un servicio de calidad.

Con la ejecución de este proyecto, al realizar la reingeniería de la red conmutada se mejorará el rendimiento de la red y el *throughput* de la misma, del mismo modo nos brindará algunas ventajas como son: escalabilidad y

menores tiempos de caída de la red. Además se logrará reforzar la seguridad de la información de la empresa mediante el uso de IBNS, esta solución permite establecer un mecanismo de seguridad interna tanto a nivel LAN como WLAN que permita el acceso seguro a la red de TAME EP basado en la identidad y el estado de autenticación de todos los usuarios que conforman la red. Esto posibilita tener visibilidad y el control de acceso de cada uno de los usuarios que ingresan a la red reforzando así el nivel de seguridad.

1. Capítulo I. Marco teórico

1.1. Modelo OSI y modelo TCP/IP

Un modelo de red se ve reflejado en su funcionamiento. Los modelos TCP/IP y OSI son los modelos principales que se utilizan cuando se analiza la funcionalidad de red.

El uso de un modelo en capas facilita el diseño de redes complejas, muestra el funcionamiento y la interacción de varios protocolos. A continuación se ilustra la comparación entre los dos modelos.

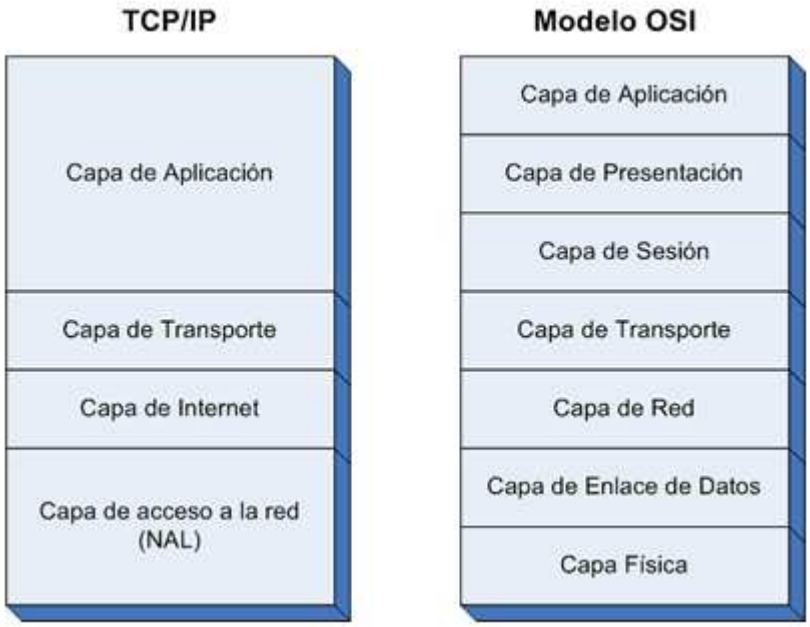


Figura 1. Comparación entre el Modelo OSI y TCP/IP

Tomado de http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

1.1.1. OSI

El modelo OSI (*Open System Interconnection*) es un modelo de referencia que fomenta la competencia al ser abierto. Es utilizado con fines didácticos, es decir para entender con mayor facilidad el funcionamiento dentro de cada capa, la interacción entre cada una de ellas e identificación de problemas.

El modelo OSI está distribuido en 7 capas como se puede observar en la siguiente figura, cada una con funciones definidas que se detallará a continuación.

Figura 2. Modelo OSI

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 2.4.2.1.

1.1.1.1. Capa Física

"La capa física de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red." (Cisco Systems, CCNA Exploration 4.0, 2007).

Abarca diferentes aspectos como son los físicos, eléctricos, mecánicos, medios de transmisión, cables, conectores, etc.; recibe una trama completa de la capa enlace de datos y la representa en una secuencia de señales como se muestra en la figura a continuación.

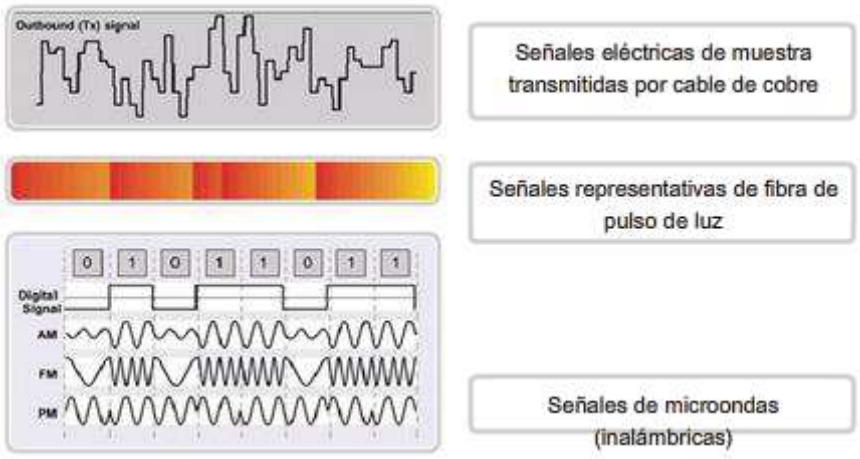


Figura 3. Representación de señales en los medios físicos

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 8.1.2.1.

El objetivo de la capa física es crear una señal óptica, eléctrica o de microondas que represente a los bits en cada trama, luego recuperarlas y representarlas nuevamente en bits para finalmente enviar los datos a la capa superior. El PDU (*Protocol Data Unit*) de la capa física son los bits. Resumiendo, las funciones esenciales de ésta capa son tres: componentes físicos, codificación de datos y señalización, como se observa en el siguiente gráfico.

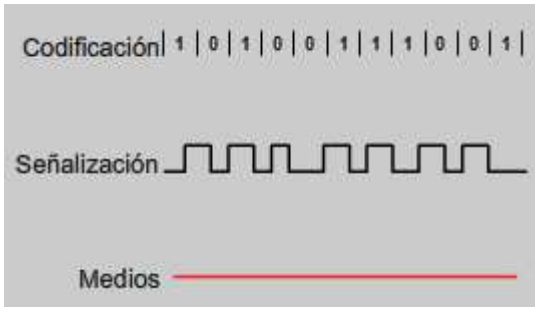


Figura 4. Funciones esenciales capa física

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 8.1.4.1.

1.1.1.2. Capa Enlace

La capa enlace de datos es la segunda capa del modelo OSI, su función principal es preparar los paquetes de la capa superior, es decir la capa de red, para ser transmitidos a través de los medios, encapsulándolos con un encabezado y un tráiler para crear una trama, controla el acceso a los medios físicos y además provee chequeo de errores mediante FCS (*Frame Checking Sequence),* utiliza 3 algoritmos CRC (*Cyclic Redundancy Check)*, LRC (*Longitudinal Redundancy Check)* y *Checksum*. El CRC es el algoritmo más fuerte y popular del FCS, verifica de manera lógica si la trama entregada contiene errores, el emisor calcula un valor lógico al enviar la trama y el receptor lo recalcula al recibir la trama, de ésta manera, si el valor lógico coincide, la trama es entregada, caso contrario se descarta. La PDU de la capa enlace es la trama y está conformada por tres partes:

i. Paquete: PDU de la capa superior
ii. Encabezado: Contiene información de control como direccionamiento y está ubicado al inicio de la PDU
iii. Tráiler: Contiene información de control agregada al final de la PDU

En la siguiente figura se puede observar la distribución de la trama.

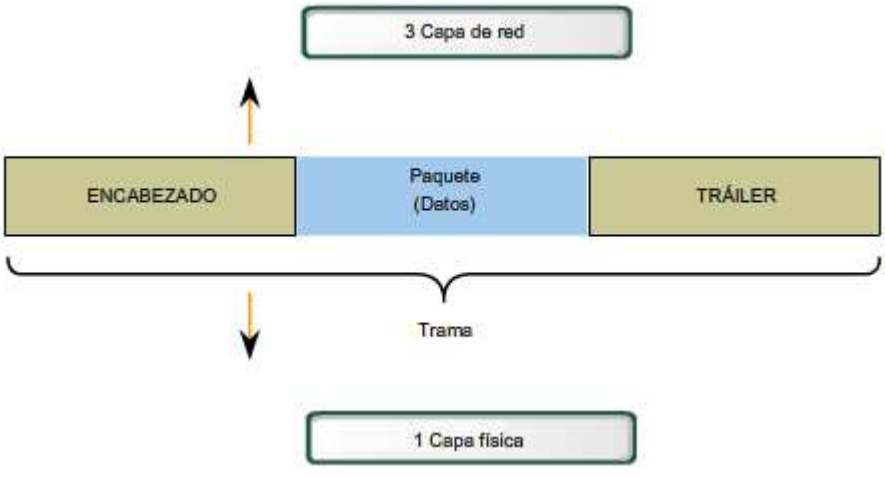


Figura 5. Distribución de la trama

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 7.1.3.1.

Entre los equipos que trabajan a nivel de la capa 2 podemos ubicar los *bridges* y *switches*; entre los protocolos utilizados podemos encontrar HDLC (*High Level Data Link Control)* y LLC (*Logical Link Control)*.

La capa enlace de datos interconecta las capas superiores *software* y la capa inferior *hardware*, como se lo puede observar a continuación.

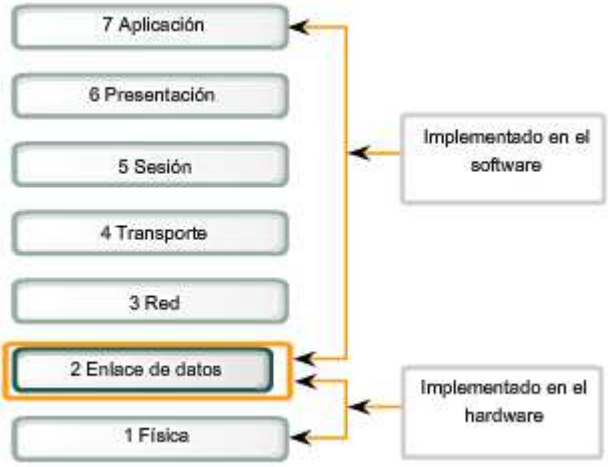


Figura 6. Interconexión capas superior e inferior

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 7.1.4.1.

La capa enlace de datos se divide en dos subcapas:

i. LLC (*Logical Link Control*): El control de enlace lógico coloca información en la trama que identifica qué protocolo de capa de red está siendo utilizado por la trama. (Cisco Systems, 2007, p. 7.1.4.2).
ii. MAC (*Media Access Control*): El control de acceso al medio proporciona a la capa de enlace de datos el direccionamiento, cada dirección MAC consta de 48 bits o 6 bloques hexadecimales que identifican de manera única a una tarjeta o interface.

A continuación se ilustra la subdivisión de la capa enlace de datos.

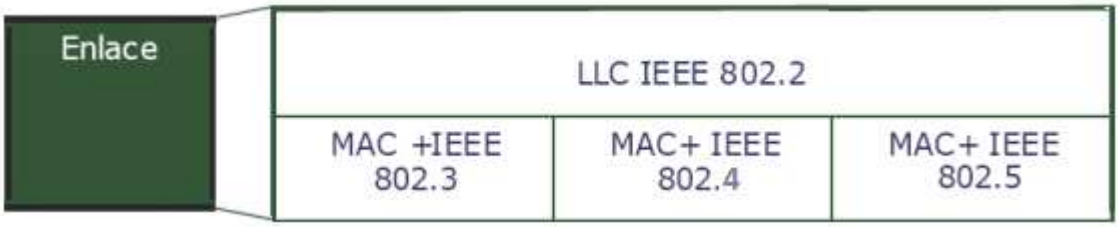


Figura 7. Subcapas de la capa Enlace de datos

Tomado de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf

1.1.1.3. Capa Red

La capa de red es la tercera capa del modelo OSI, su principal función consiste en buscar y seleccionar la mejor ruta para transportar los paquetes hacia su destino, este procedimiento es conocido como *routing*.

En esta capa podemos encontrar *routers* y *switches* de capa 3, provee un mecanismo para identificar los equipos finales conocido como dirección IP, que consiste en una serie de 32 bits distribuidos en 4 octetos y separados por un punto.

La capa de red prepara un segmento o datagrama (PDU de la capa transporte) para transmitirlo a través de los medios locales añadiendo un encabezado, creando así un paquete, como se muestra a continuación.

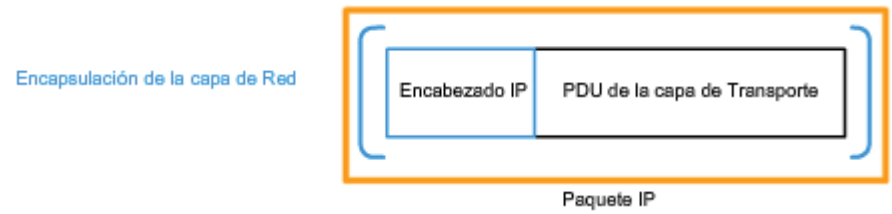


Figura 8. Distribución del paquete IP

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 5.1.6.1.

El paquete cuenta con seis campos primordiales en el encabezado como se puede observar y detallar a continuación.

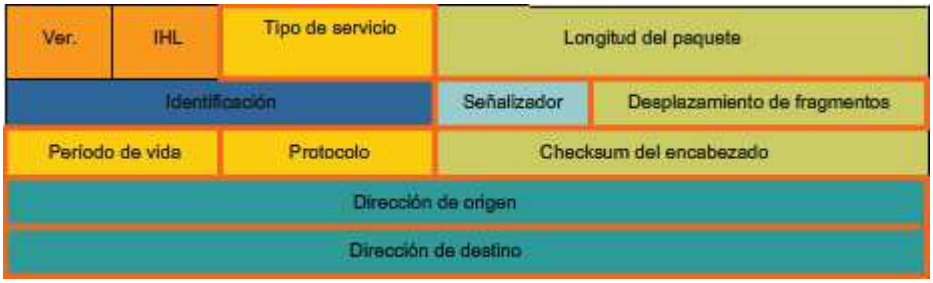


Figura 9. Encabezado del paquete IP

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 5.1.7.1.

i. Desplazamiento de Fragmentos: Un *router* puede tener que fragmentar un paquete cuando lo envía desde un medio a otro medio que tiene una MTU (*Maximun Transmission Unit)* más pequeña. Cuando se produce una fragmentación, el paquete IPv4 utiliza el campo desplazamiento de fragmento y el señalizador MF (*More Fragments)* en el encabezado IP para reconstruir el paquete cuando llega al *host* destino. El campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción (Cisco Systems, 2007, p. 5.1.7.1). MF es un único bit utilizado en conjunto con el campo desplazamiento de fragmentos en el encabezado IP para fragmentar y reconstruir paquetes.

ii. Tipo de Servicio: El campo de tipo de servicio contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de QoS (*Quality of Service)* a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía. El *router* que procesa los paquetes puede ser configurado para decidir qué paquete es enviado primero basado en el valor del tipo de servicio (Cisco Systems, 2007, p. 5.1.7.1).

iii. Protocolo: Este valor binario de 8 bits indica el tipo de relleno de carga que el paquete traslada. El campo de protocolo permite a la capa de red pasar los datos al protocolo apropiado de la capa superior (Cisco Systems, 2007, p. 5.1.7.1).

iv. Tiempo de Vida: TTL (*Time to Live)*, es el número de saltos antes de que el paquete sea descartado. Este valor disminuye en uno cada vez que el paquete es procesado por un *router,* es decir, en cada salto; cuando el valor se vuelve cero, el *router* descarta o elimina el paquete. El valor por defecto del TTL es 255.

v. Dirección IP Origen: Este campo contiene una serie binaria de 32 bits que representa la dirección origen del paquete, esta dirección permanece inalterable a lo largo del recorrido del paquete por la red.

vi. Dirección IP Destino: Este campo contiene una serie binaria de 32 bits que representa la dirección hacia donde debe llegar el paquete, de la misma manera que la dirección IP origen, éste campo permanece inalterable a lo largo del recorrido del paquete por la red.

1.1.1.4. Capa de Transporte

La capa transporte es la cuarta capa del modelo OSI, su función primordial consiste en aceptar los datos de la capa de sesión, dividirlos en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente a su destino de una manera óptima. Las principales responsabilidades que esta capa debe cumplir son:

i. Seguimiento de la comunicación individual entre aplicaciones en los *hosts* origen y destino
ii. Segmentación de datos
iii. Ensamble de segmentos en flujos de datos de aplicación
iv. Identificación de las diferentes aplicaciones

La capa de transporte segmenta los datos y administra la separación de datos para diferentes aplicaciones, divide los datos en segmentos para administrarlos y transportarlos con mayor facilidad.

Para identificar todos los segmentos de datos, la capa de transporte agrega un encabezado a la sección que contiene datos binarios, este encabezado contiene campos de bits. Son los valores de estos campos los que permiten

que los distintos protocolos de la capa de transporte lleven a cabo las diversas funciones (Cisco Systems, 2007, p. 4.1.1.3).

La capa transporte del modelo OSI cuenta con dos protocolos: TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*), la diferencia entre ellos es que TCP es un protocolo orientado a conexión, es decir necesita establecer una conexión para empezar a transmitir; UDP es un protocolo no orientado a conexión es decir, que puede empezar a transmitir datos sin la necesidad de establecer con antelación una conexión. A continuación se podrá observar el encabezado del segmento y se detallará algunos de los campos más importantes.

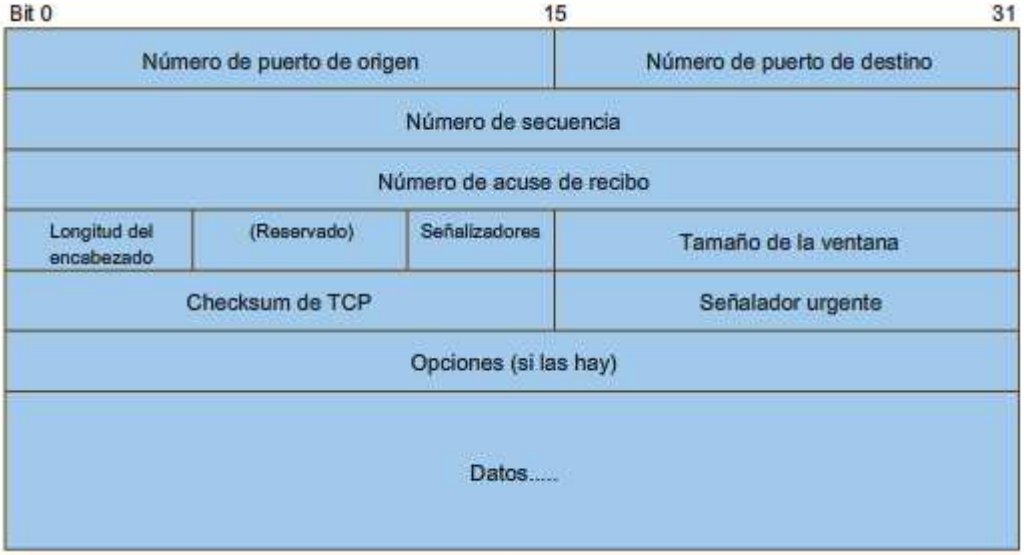


Figura 10. Encabezado del segmento

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless, 2007 p. 4.2.1.1.

i. Número de Puerto Origen: Sesión TCP en el dispositivo que abrió una conexión. Normalmente es representado por un valor aleatorio superior a 1023.
ii. Número de Puerto Destino: Identifica el protocolo de la capa superior o la aplicación del sitio remoto.
iii. Número de Secuencia: Identifica el número del último octeto en un segmento.

iv. Número de Acuse de Recibo: Especifica el próximo octeto esperado por el receptor.

v. Tamaño de la Ventana: Es el valor de la ventana dinámica, es decir la cantidad de octetos que pueden enviarse antes de esperar el acuse de recibo.

La segmentación permite la multiplexación de sesiones, es decir, las diferentes aplicaciones pueden utilizar la red al mismo tiempo y además facilitar el transporte de datos por parte de las capas de red inferiores.

Puede realizarse la verificación de errores en los datos del segmento para verificar si el segmento se cambió durante la transmisión.

1.1.1.5. Capa Sesión

Es la quinta capa del modelo OSI, esta capa permite crear y mantener sesiones entre usuarios de diferentes puntos (origen y destino); permite acceder a un sistema de tiempo compartido a distancia, transferir un archivo entre dos máquinas, se encarga de la sincronización entre el origen y destino de los datos; es decir establece, administra y termina sesiones entre aplicaciones. A continuación se puede observar la ubicación de la capa sesión y una breve descripción de sus funciones.

Figura 11. Capa Sesión

Tomado de http://www.talktoanit.com/c_old/index.php?option=com_content&view=article&id=1:las-7-capas&catid=36:redes&Itemid=82

1.1.1.6. Capa Presentación

La sexta capa del modelo OSI se ocupa de temas como su nombre lo indica, de la presentación, aspectos como la sintaxis y semántica de la información que se transmite. En esta capa a más del formato también está presente la encriptación y la compresión. La capa presentación debe garantizar que los datos puedan ser legibles para el destino, entre otros aspectos importantes de esta capa tenemos cifrar y descifrar los mensajes, expandir o comprimir el mensaje para que viaje de una manera más eficiente y traducir el contenido, como se observa a continuación.

Figura 12. Capa Presentación

2. Tomado de http://www.talktoanit.com/c_old/index.php?option=com_content&view=article&id=1:las-7-capas&catid=36:redes&Itemid=82

1.1.1.7. Capa Aplicación

La capa aplicación provee la interfaz final al usuario. Así, esta capa proporciona acceso al entorno OSI para los usuarios y los procesos de las aplicaciones para acceder a servicios de red. En esta capa se encuentra lo que el usuario puede ver como el explorador de internet y el correo electrónico, entre algunas de la funciones de esta capa tenemos mensajes electrónicos, FTP, *web browser*, acceso remoto a impresoras, etc., como se ilustra en la imagen a continuación.

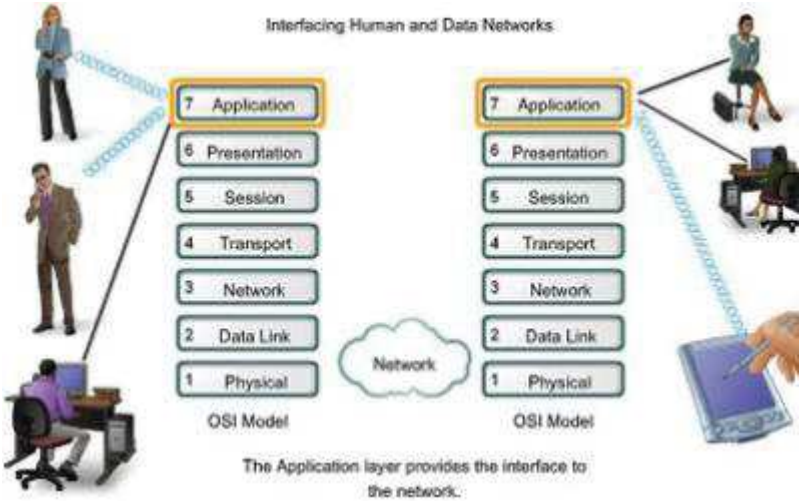


Figura 13. Capa Aplicación

Tomado de http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/documentos/index7.html

1.1.2. TCP/IP

El modelo TCP/IP es un modelo de protocolo que describe las funciones que ocurren en cada capa de protocolos dentro del conjunto TCP/IP. Fue creado por el año 1970 y se le conoce como el modelo de Internet; a continuación se mostrará y se describirá brevemente las cuatro capas que conforman el modelo.

Figura 14. Modelo TCP/IP

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless, 2007 p. 2.4.2.1.

1.1.2.1. Capa Acceso a la Red

La capa acceso a la red del modelo TCP/IP representa a las dos primeras capas del modelo OSI (física y enlace de datos), asimila sus funciones y comportamiento. Se encarga de la transmisión de bits, características físicas y eléctricas en el medio de transmisión, como se ilustra a continuación en la imagen.

Figura 15. Capa Acceso a la Red

Tomada de http://edwcifu.blogspot.com/

1.1.2.2. Capa Internet

De la misma manera tiene similitud con la capa de red del modelo OSI, entre sus funciones principales están el *routing* de los paquetes y evitar la congestión, como se observa en la siguiente figura.

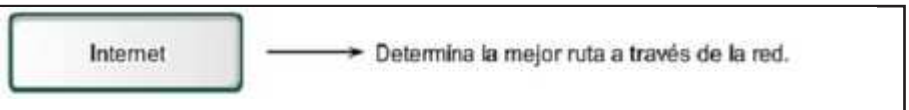


Figura 16. Capa Internet

Tomada de http://edwcifu.blogspot.com/

1.1.2.3. Capa Transporte

La capa transporte del modelo TCP/IP tiene las funciones similares a la del modelo OSI, es decir regula el flujo de información, asegura el transporte confiable de datos, como se observa en la siguiente imagen.

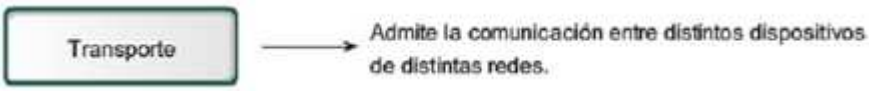


Figura 17. Capa Transporte

Tomada de http://edwcifu.blogspot.com/

1.1.2.4. Capa Aplicación

Las tres capas superiores aplicación, presentación y sesión del modelo OSI se agrupan en ésta última capa del modelo TCP/IP, sus funciones principales abarcan proporcionar servicios como FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), TELNET (*Telecomunication Network*) y HTTP (*Hyper Text Transfer Protocol*).

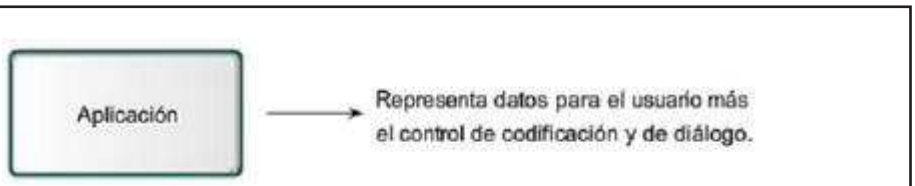


Figura 18. Capa Aplicación

Tomada de http://edwcifu.blogspot.com/

1.2. Conmutación (*Switching*)

El término conmutación se aplica a la interconexión de redes a nivel de capa dos del modelo OSI. Para facilitar la administración y tener una mejor visibilidad de la red se utiliza un modelo de diseño jerárquico.

En la siguiente gráfica se observa como el modelo jerárquico divide la red en tres capas independientes, cada capa debe cumplir funciones específicas para mejorar el rendimiento y brindar escalabilidad de una manera ordenada.

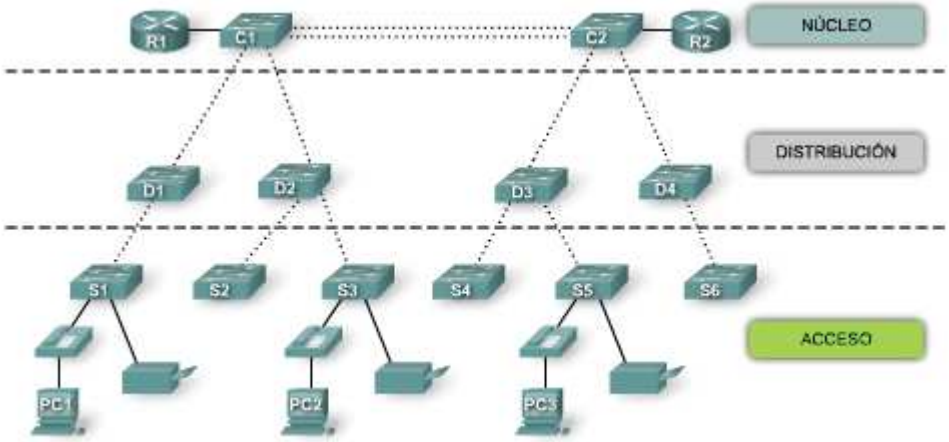


Figura 19. Modelo de red jerárquico

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 1.1.1.1.

La capa de acceso es la capa a la que se conectan directamente los dispositivos finales como PC, impresoras o teléfonos IP. Además se identifica y se debe tomar en cuenta otros factores como el número de puertos de acceso, la distancia del equipo final hasta el *switch*, la seguridad en los puertos, etc.

La capa de distribución es la capa intermedia, en esta capa se tiene puertos que trabajan a mayor velocidad, además se tiene otras características importantes como el control de flujo de tráfico, velocidades de transmisión mayores, redundancia y permite la comunicación a nivel de VLANs. Es el enlace desde la capa acceso hasta su destino final en la capa de núcleo.

En la capa de núcleo se puede encontrar equipos más robustos, mayor procesamiento, alta disponibilidad, mayor velocidad, altamente redundante y maneja *routing*.

Entre los principales beneficios de una red jerárquica tenemos:

i. Escalabilidad: Expansión sencilla de la red, por ejemplo se puede añadir un *switch* en la capa de distribución al que se pueden conectar varios *switches* de acceso.

ii. Redundancia: Se puede realizar conexiones de nuevos equipos para tener un respaldo a nivel de las tres capas, asegurando de esa forma la disponibilidad de la ruta para la información.
iii. Rendimiento: El agregado del enlace entre las capas núcleo y distribución permite transmitir a una mayor velocidad en la red.
iv. Seguridad: Permite aumentar el nivel de seguridad de la red, por ejemplo se puede configurar *port security* y políticas de seguridad en la capa de acceso y distribución respectivamente.
v. Administración: Simplifica la administración al tener la red distribuida en capas.
vi. Mantenimiento: Permite brindar un soporte de una manera más simplificada.

1.2.2. Conceptos de redes conmutadas

1.2.2.1. IEEE 802.3

IEEE 802.3 opera en las dos capas inferiores del modelo OSI, específicamente en la capa física y en la subcapa MAC (*Media Access Control*) de la capa enlace de datos, como se ilustra a continuación.

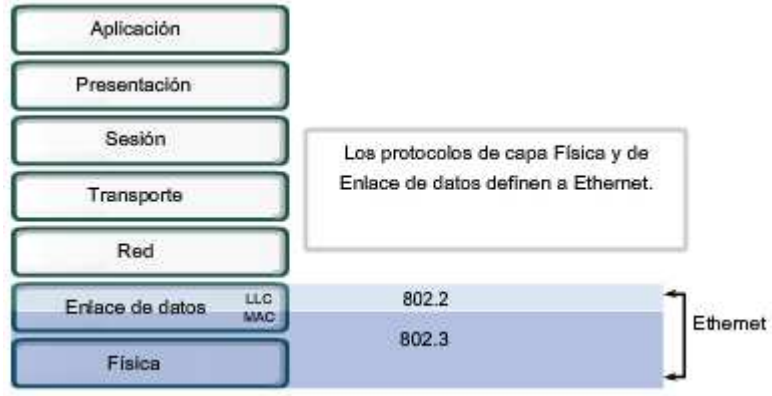


Figura 20. Capas de IEEE 802.3

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 9.1.1.1.

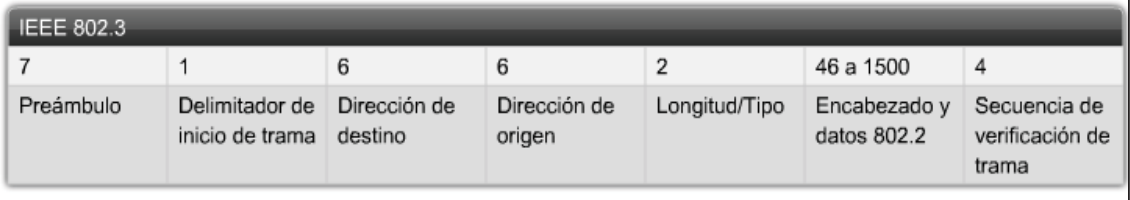
La subcapa MAC tiene dos responsabilidades principales: encapsulación de datos y control de acceso al medio.

La encapsulación de datos proporciona tres funciones principales:

i. Delimitación de trama: Identifica un grupo de bits que conforman una trama.
ii. Direccionamiento: Agrega la dirección física (MAC) lo que posibilita que la trama pueda ser entregada a su destino.
iii. Detección de errores: Cada trama contiene un tráiler que agrega FCS y como se mencionó anteriormente se utiliza el algoritmo más fuerte que es CRC (*Cyclic Redundancy Check*) para compararla con la trama original y verificar si la trama se recibió sin errores.

El control de acceso al medio controla la colocación y el retiro de tramas en los medios, como su nombre lo indica, administra el control de acceso al medio.

A continuación se puede observar con mayor detalle la estructura de la trama IEEE 802.3, sus respectivos campos y un detalle de los mismos.



IEEE 802.3						
7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud/Tipo	Encabezado y datos 802.2	Secuencia de verificación de trama

Figura 21. Trama IEEE 802.3

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 9.3.1.1.

i. Preámbulo: Es utilizado para la sincronización entre los dispositivos que envían y reciben, fundamentalmente indican al receptor que se prepare para que reciba una trama, su longitud es de 7 bytes.
ii. Delimitador de inicio de trama: SFD (*Start Frame Delimitation)* su longitud es de 1 byte, trabaja conjuntamente con el preámbulo para sincronizar la trama de recepción.

iii. Dirección de destino y origen: Cada campo contiene 6 *bytes* e identifican la dirección a la que está destinada la trama y la interface que origina la trama.

iv. Longitud/Tipo: Su longitud es de 2 *bytes* y define la longitud exacta del campo datos de la trama, si el objetivo es designar un tipo, definirá que protocolo se implementa.

v. Datos: De 46 a 1500 *bytes* contiene los datos encapsulados de la capa superior, si los datos de la trama son insuficientes se utilizan *bytes* de relleno para completar la longitud mínima.

vi. Secuencia de verificación de trama: FCS (*Frame Check Sequence)* su longitud es de 4 *bytes* y tiene 3 algoritmos para verificar posibles errores al recibir una trama CRC (*Cyclic Redundancy Check),* LRC *(Longitudinal Redundancy Check) y Checksum*.

IEEE 802.3 se crea a partir de modificaciones que fueron realizadas al estándar *Ethernet*; la diferencia más significativa entre las dos tramas es que IEEE 802.3 agrega el campo SFD. En un medio compartido todos los dispositivos tienen garantizado el acceso al medio, pero si dos de ellos transmiten simultáneamente se producen colisiones, es por ello que *Ethernet* provee un método para detectar las colisiones y reanudar la comunicación. CSMA (*Carrier Sense Multiple Access)* es un método de control de acceso al medio, mejora el rendimiento cuando el medio es altamente utilizado, antes de transmitir se escucha si el medio está libre para transmitir, pero esto no es suficiente puesto que puede haber dos equipos de red que escuchan el medio libre y transmiten simultáneamente causando una colisión que corrompe la trama; es ahí cuando un segundo elemento entra en acción, se utiliza para detectar una colisión y se conoce como CD (*Colition Detect)* formando juntos un mecanismo de control de acceso al medio con detección de portadora*;* a continuación se podrá observar el funcionamiento de CSMA/CD.

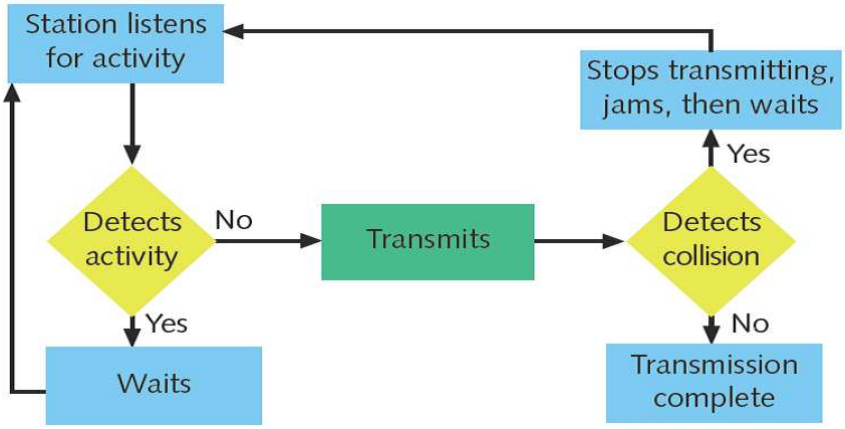


Figura 22. Funcionamiento de CSMA/CD

Tomado de http://cis155al.blogspot.com/2013/02/chapter-5-topologies-and-ethernet.html

Los equipos de la red antes de transmitir deben escuchar, si el medio está libre entonces transmite, caso contrario, es decir si el medio está ocupado el dispositivo continúa escuchando hasta que encuentre libre el canal y transmite inmediatamente, si detecta una colisión durante una transmisión, el equipo transmite una señal corta de alerta para asegurarse que los otros equipos detecten la colisión y suspendan la transmisión, después de transmitir la señal de alerta se espera un tiempo aleatorio para iniciar nuevamente con el proceso. Este mecanismo era utilizado anteriormente cuando se tenía comunicación *half-duplex*, en la actualidad debido a que la comunicación es *full-duplex* su uso ya fue descontinuado.

1.2.2.2. Virtual Local Area Network (VLAN)

Una LAN virtual se define como un dominio de *broadcast* creado por uno o más *switches*. Se entiende como dominio de *broadcast* a un conjunto de equipos, dentro del cual, uno de ellos transmite y todo el resto escucha; en otras palabras es un conjunto formado por equipos de red que pueden escuchar una trama enviada por cualquier otro dispositivo dentro de la misma red. El concepto de VLAN permite a un administrador de red crear grupos de dispositivos conectados a la red de manera lógica y éstos actuarán como si estuviesen en una red independiente, de la misma manera pueden existir

varias VLANs en una misma área geográfica que es la principal ventaja frente a las redes convencionales como se puede observar a continuación.

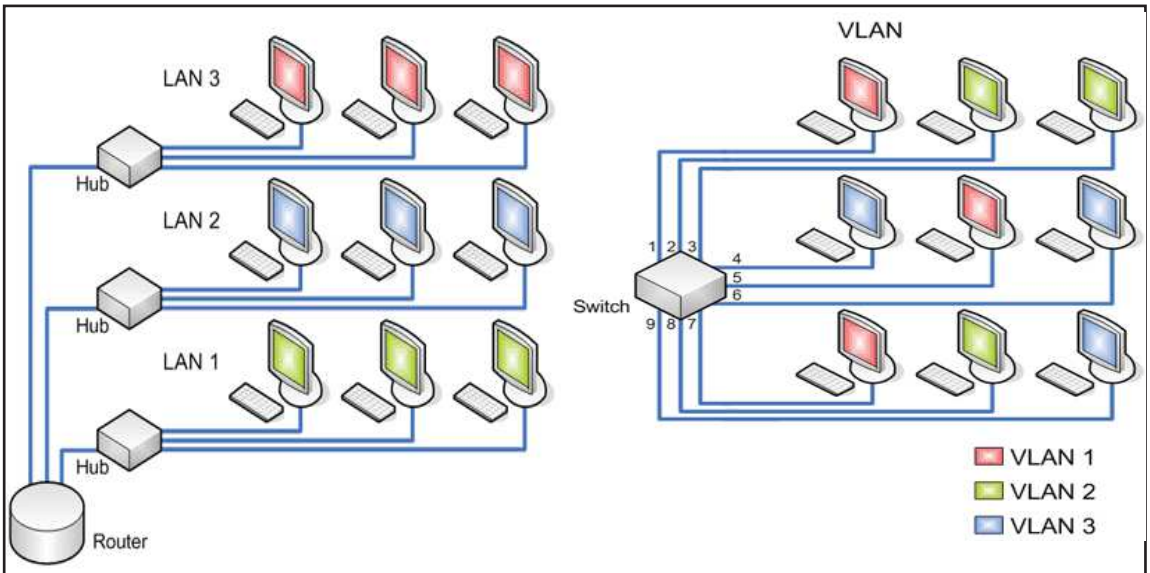


Figura 23. LAN Tradicional vs. VLAN

Tomada de http://www.textoscientificos.com/redes/redes-virtuales

1.2.2.2.1. Ventajas de las VLAN

Entre las principales ventajas que nos ofrecen las VLANs tenemos las siguientes:

i. Seguridad: Se puede separar en una VLAN diferente los datos que sean sensibles para una corporación del resto de la información.
ii. Reducción de costos: La reducción se representa en la optimización del ancho de banda y usos más eficientes de los enlaces.
iii. Mejor rendimiento: La división de redes en diferentes grupos lógicos reduce el tráfico innecesario y además potencia el rendimiento.
iv. Mitigación de la tormenta de *broadcast*: Al dividir una red en VLANs se reduce la cantidad de dispositivos que participan en una tormenta ya que la segmentación impide que una tormenta de *broadcast* se propague a través de toda la red.
v. Mayor eficiencia del personal: La administración de la red se facilita ya que los usuarios con similares requerimientos se asignan a una misma VLAN.

1.2.2.2.2. Características de las VLAN

Para identificar las VLAN en los diferentes equipos, se utiliza un identificador conocido como ID, a continuación se describe los distintos rangos:

I. Rango normal: comprende desde la 1 hasta la 1005.
II. Rango extendido: comprende desde la 1006 hasta la 4094 y son utilizados por los ISP (*Internet Service Provider*) ya que les permiten aumentar su infraestructura.

Los ID 1 y el rango 1002 - 1005 se crean automáticamente y no es posible eliminarlas. Las VLANs desde la 1002 a la 1005 son reservadas para Token Ring y FDDI (*Fyber Distributed Data Interface*).

1.2.2.2.3. Tipos de VLAN

Para determinar los tipos de VLAN se basa en el tipo de tráfico que se va a transportar o la función que desempeña una VLAN, a continuación se detalla los diferentes tipos de VLAN:

1.2.2.2.3.1. VLAN de datos

Las VLAN de datos se configuran cuando se va a enviar únicamente tráfico de datos. Es una buena práctica separar el tráfico por seguridad y por facilitar la administración.

1.2.2.2.3.2. VLAN predeterminada

Se habla de una VLAN predeterminada cuando todos los puertos de un *switch* pertenecen al mismo dominio de *broadcast*, en Cisco la VLAN predeterminada es la 1 y tiene las mismas características que cualquier otra VLAN a excepción de renombrarla o eliminarla.

1.2.2.2.3.3. VLAN nativa

Una VLAN es nativa cuando está configurada en un puerto troncal; un puerto está configurado como troncal cuando por él pasan diferentes VLANs, es decir

tráfico etiquetado de diferentes VLANs y el tráfico limpio o no etiquetado es el que pertenece a la VLAN nativa.

1.2.2.2.3.4. VLAN de administración

La VLAN de administración puede ser cualquiera que se configure como tal, con el objetivo de tener gestión del equipo. Una buena medida de seguridad es configurar una IP y una máscara en una VLAN diferente a la VLAN 1, debido a que por defecto todos los puertos de un *switch* pertenecen a la VLAN 1; luego de ello la gestión puede ser mediante HTTP, Telnet, SNMP (*Simple Network Management Protocol*) o SSH (*Secure SHell*).

1.2.2.2.4. Configuración de VLAN

Para configurar una VLAN se le debe asociar un número de ID y un nombre que por buena práctica facilita la administración pero no necesariamente es obligatorio; un puerto de un *switch* se lo puede configurar de distintas maneras como a continuación se describe.

1.2.2.2.4.1. VLAN estática

Una VLAN es estática cuando la asignación de puertos de un *switch* a una VLAN se la realiza manualmente, esto se lo puede realizar a través de la utilización de CLI (*Command Line Interface*). A continuación se podrá observar un ejemplo de configuración de una VLAN estática.

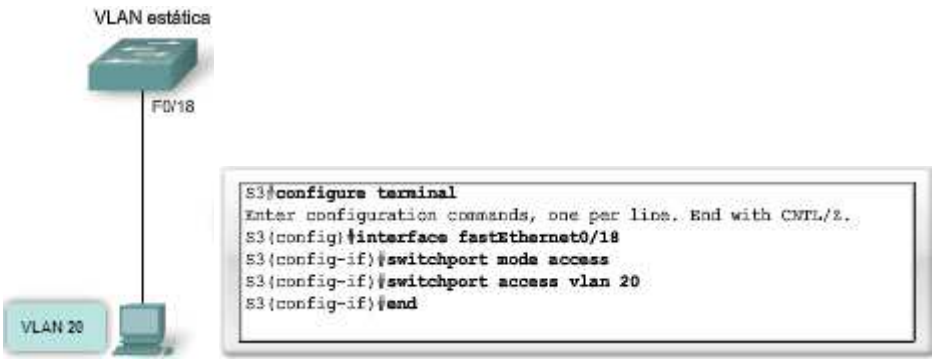


Figura 24. Configuración en modo estático

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 3.1.3.1.

1.2.2.2.4.2. VLAN dinámica

Una VLAN dinámica se configura utilizando VMPS (*VLAN Membership Policy Server)*, con este servidor se asigna puertos de *switch* a las VLAN basados en la dirección MAC de origen del dispositivo que se encuentra conectado al puerto. A continuación se podrá observar un ejemplo del funcionamiento de una VLAN dinámica usando VMPS.

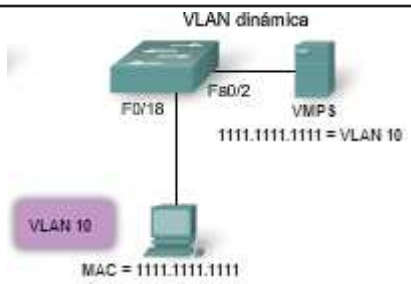


Figura 25. Configuración en modo Dinámico

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 3.1.3.1.

1.2.2.2.4.3. VLAN de voz

Se configura un puerto de un *switch* en modo de voz para que permita que un teléfono IP pueda conectarse a él, antes de configurar la VLAN de voz en el puerto del *switch*, es necesario crear una VLAN de voz y una de datos. A continuación se podrá observar un ejemplo de la configuración detallada.

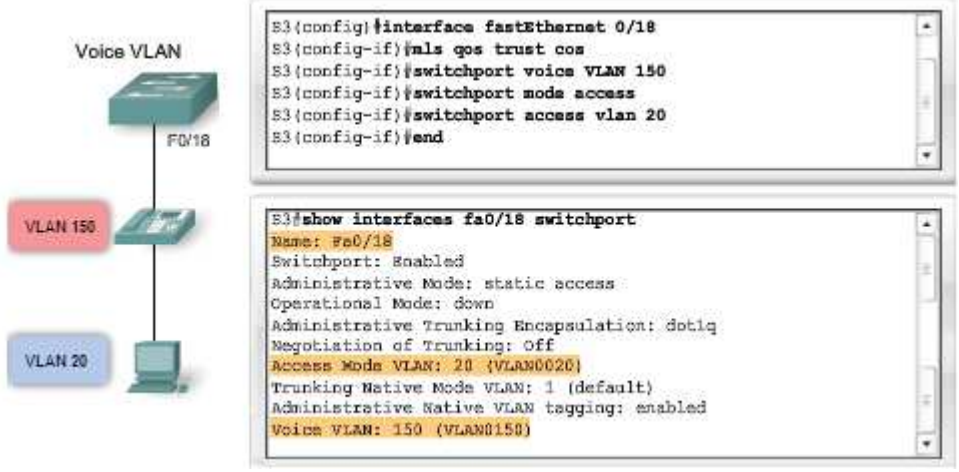


Figura 26. Configuración VLAN de voz

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 3.1.3.1.

1.2.2.2.5. IEEE 802.1Q

El estándar IEEE 802.1Q define un enlace troncal punto a punto entre dispositivos que transportan varias VLAN.

La principal ventaja que ofrece el enlace troncal es el poder ahorrar recursos, directamente puertos libres en un *switch*, ya que como podemos observar en la figura a la izquierda se requiere una conexión física entre los *switches* para cada VLAN mientras que utilizando el enlace troncal es necesario una única conexión física entre los *switches* como se observa a la derecha.

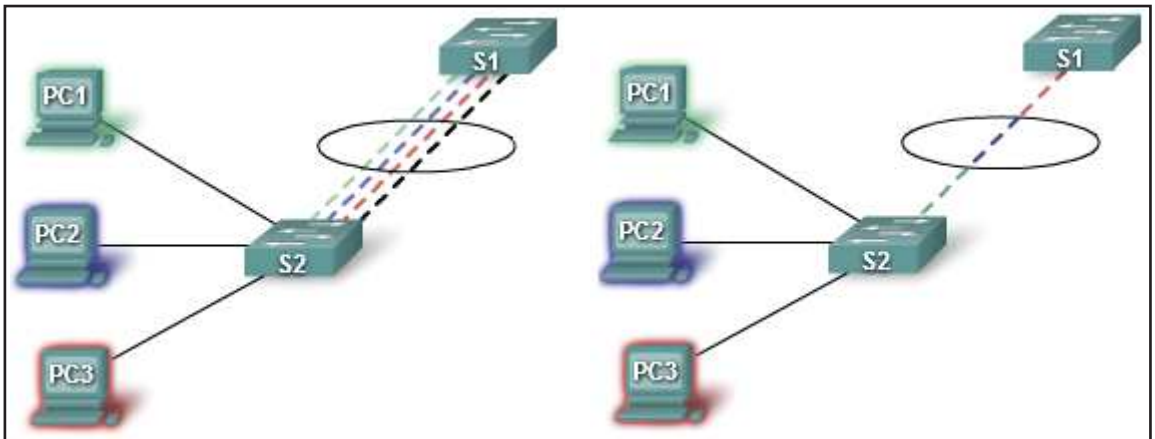


Figura 27. Enlace normal vs. Enlace IEEE 802.1Q

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 3.2.1.2.

El encabezado de la trama *Ethernet* no contiene información para el transporte de las VLAN, para solventar esto se utiliza el encabezado de encapsulación 802.1Q, este encabezado agrega una etiqueta a la trama original en la que especifica la VLAN a la que pertenece cada trama.

A continuación se puede observar los campos que se agregan a la trama para poder identificar a las VLANs y después un detalle de los mismos.

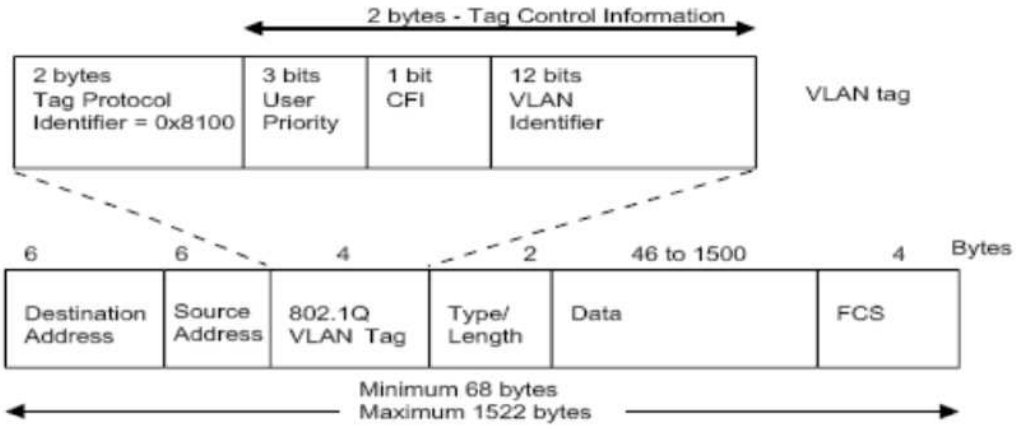


Figura 28. Trama IEEE 802.1Q

Tomada de Lammle,T. (2011). *Cisco Certified Network Associate*. Indianapolis, USA:Wiley p.14

i. Los tres bits del campo *Priority* van desde el 0 al 7 e indican el nivel de prioridad, siendo siete la mayor prioridad.
ii. El campo CFI de sus siglas en inglés *Canonical Format Indentifier* de 1 bit permite que las tramas *Token Ring* se transporten a través de la red con facilidad.
iii. Los doce bits del campo VLAN *Identifier* corresponden al identificador de VLAN con que se marcarán los paquetes, dos de estos valores se encuentran reservados el 0x000 y el 0xFFF; admite hasta 4096 ID de VLAN.

La configuración de un puerto en modo troncal se la realiza en pocos pasos y de una manera sencilla, a continuación se mostrará un ejemplo de la configuración en modo troncal de los puertos que interconecta al *switch* 1 y 2 de la topología expuesta.

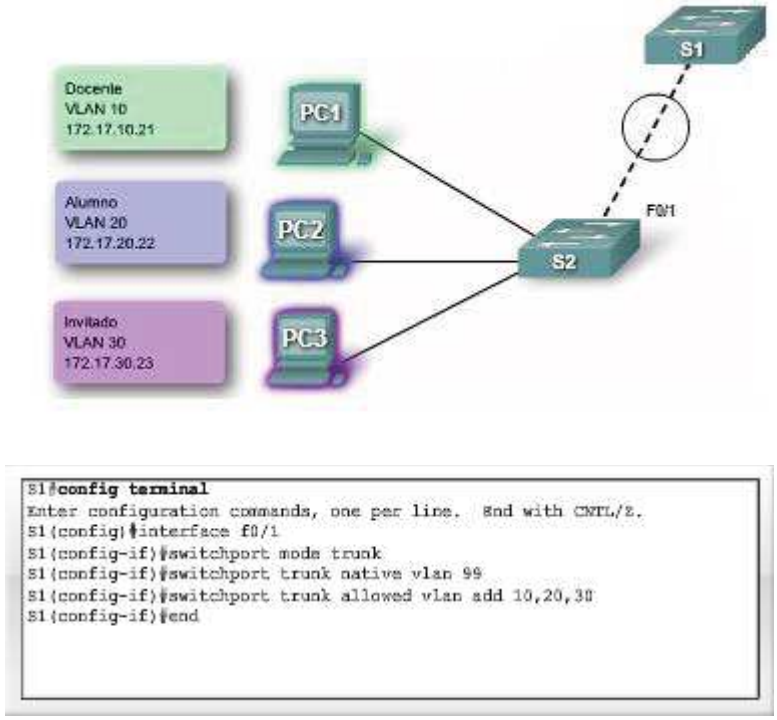


Figura 29. Configuración puerto en modo troncal

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 3.3.4.1.

En la configuración mostrada se asegura que el tráfico de las VLAN 10, 20 y 30 va a ser permitido por el enlace entre el *switch* 1 y el *switch* 2.

1.2.2.3. STP

Spanning Tree Protocol o IEEE 802.1D es un protocolo para evitar *loops* o bucles en redes redundantes a nivel de capa dos.

Cada interface dentro del protocolo STP asume algunos estados entre ellos bloqueo o envío para evitar bucles en el tráfico, ya que al existir varias rutas entre dos equipos debido a la redundancia está propenso a generar *loops*.

El viaje de los paquetes IP a través de la red está limitado por el campo TTL (*Time to Live*) pero la trama *Ethernet* al no poseer un TTL viaja a través de la red indefinidamente, creando así *loops* en la red. Para solventar estos inconvenientes STP fue desarrollado.

STP bloquea intencionalmente los puertos para asegurar que exista una única ruta lógica hacia el destino.

1.2.2.3.1. Puertos STP

En STP se puede encontrar 5 asignaciones para los puertos, a continuación se detallará brevemente cada estado:

i. *Blocking*: Bloquea el tráfico de entrada y de salida y envía una BPDU (*Bridge Protocol Data Unit*) estable. No envía tramas pero si las escucha.
ii. *Listening*: Escucha BPDU's. Recibo BPDU's pero no se forma la tabla MAC.
iii. *Learning*: No deja pasar tráfico, aprende la MAC en base a la dirección MAC origen. En este estado se construye la tabla MAC.
iv. *Forwarding*: Pasa las tramas y aprende direcciones MAC. Óptimo para transmitir y recibir tráfico de usuario.
v. *Disable*: Está deshabilitado administrativamente.

La BPDU (*Bridge Protocol Data Unit*) es un mensaje del protocolo STP que se envía a intervalos que pueden ser configurables para intercambiar información entre los *switches* de la red.

1.2.2.3.2. Roles STP

En STP se tiene cuatro diferentes roles en el proceso STP, los cuales se detallan brevemente a continuación:

i. *Root*: El puerto *root* se encuentra en los *non-root bridge* y es el puerto de *switch* con el mejor camino hacia el *root bridge*.
ii. *Designated*: El puerto designado existe en un *root* y en un *non-root bridge*. En un *root bridge* todos los puertos son designados.
iii. *No Designated*: Un puerto no designado es bloqueado en el proceso.
iv. *Disabled*: Un puerto deshabilitado es un puerto que administrativamente se lo configuró en *shutdown* y éste no participa en el proceso STP.

Un *root bridge* intercambia información en una topología donde se haya implementado STP, para notificar a los otros *switches* de la red si es necesario realizar cambios en la red.

El *non-root bridge* es el equipo o los equipos dentro de la misma red que no cumplen como *root bridge*, por tener un bridge ID más alto.

1.2.2.3.3. Funcionamiento

Primeramente se elige el *root bridge*, esta elección se determina por el menor *bridge ID*.

El *bridge ID* es el resultado de la combinación de la prioridad y la dirección MAC; en caso de que los equipos tengan la misma prioridad, la MAC (el menor valor) será el factor decisivo para determinar el *bridge ID*. A continuación se ilustran los campos mencionados.

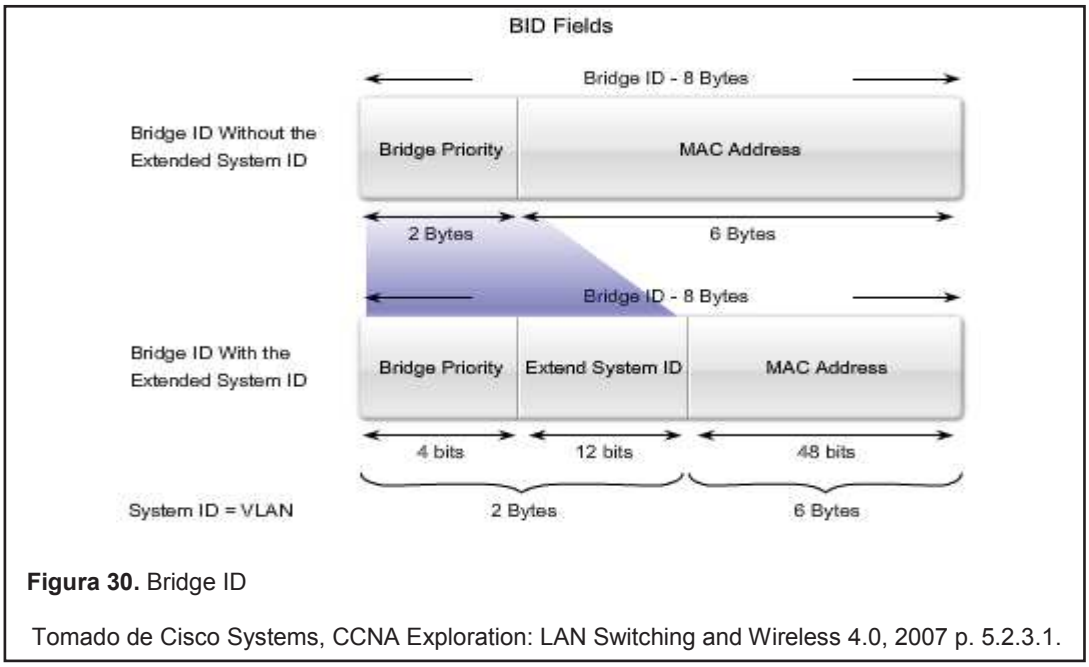


Figura 30. Bridge ID

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 5.2.3.1.

El *bridge ID* consta de 3 campos, el *bridge priority*, el *extend system ID* y *MAC address*. Inicialmente en STP se omitía el campo de *extended System ID* para redes que no utilizaban VLANs; con el paso del tiempo el uso de las VLANs se tornó común y STP fue mejorado para manejar VLANs, es ahí cuando el campo *extend system ID* forma parte del *bridge ID* ya que en él está contenido el ID de

la VLAN. Con el valor del *bridge priority* se puede cambiar y definir la elección del *root bridge*.

Se elige el *root port* en base al *path cost*, éste debe ser el más bajo para llegar al *root bridge*; si éstos son iguales se elige por la prioridad de interfaz más baja, si esta es igual se fija por la interface más baja; a continuación se ilustra los costos de STP.

Link Speed	Cost (Revised IEEE Specification)
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

Figura 31. Path Cost STP

Tomado de Cisco Systems, CCNA Exploration: LAN Switching and Wireless 4.0, 2007 p. 5.2.1.4.

Se busca los puertos no designados en los segmentos donde no se tiene asignado los roles. Para identificar ese rol se ubica el *switch* con el *bridge ID* más alto en ese segmento o se ubica el *switch* con el *bridge* ID más bajo y el puerto no designado es el opuesto.

1.2.2.4. VTP

Es un protocolo propietario de Cisco utilizado para intercambiar información de VLANs entre *switches* y trabaja sobre enlaces troncales. VTP son las siglas de *VLAN Trunking Protocol*, es un protocolo de capa dos y es de gran ayuda ya que en redes pequeñas administrar las VLAN puede resultar una tarea sencilla, pero a medida de que la red crece se dificulta la administración.

VTP trababa de manera centralizada, es decir las actualizaciones se realizan en un *switch* y éste es el encargado de difundir la información al resto de *switches* dentro del dominio.

1.2.2.4.1. Dominio VTP

Un dominio VTP es un conjunto de *switches* interconectados que comparten el mismo nombre de dominio VTP, pudiendo un *switch* pertenecer a un solo dominio VTP.

Por defecto un *switch* no tiene configurado ningún dominio y se mantiene en ese estado hasta que le llega un anuncio de un dominio a través de un enlace troncal o hasta que se le configura un nombre de dominio, formando parte desde ese momento del dominio VTP anunciado.

1.2.2.4.2. Modos VTP

Un *switch* de VTP puede ser configurado de tres modos diferentes de operación, a continuación se detallará cada uno de ellos:

i. Modo Servidor: Tiene la potestad de crear, modificar y borrar VLANs.
ii. Modo Cliente: Recibe la información proveniente del servidor y modifica esta información de las VLANs.
iii. Modo Transparente: El modo transparente también tiene la potestad de crear, modificar y borrar VLANs pero esto únicamente dentro de su dominio. Además propaga mensajes VTP pero no tiene la capacidad de modificar la información de las VLAN.

1.2.2.4.3. Funcionamiento

Dentro del dominio VTP, el *switch* configurado como servidor distribuye y sincroniza la información de las VLAN a los *switches* dentro del dominio VTP a través de la red conmutada, esto nos ayuda a reducir al mínimo las configuraciones incorrectas y las inconsistencias que se puedan digitar al configurar cada *switch*.

VTP fue diseñado para trabajar en un ambiente donde los cambios se realizan de manera centralizada en un solo *switch* y se envían a través de VTP al resto de *switches* del dominio, actualizando los cambios que sean necesarios a lo largo de la red.

Cuando se configura un nombre de dominio en un *switch* el número de revisión se encuentra en cero, este número incrementa en uno cada vez que se agrega o se borra una VLAN, es decir, cada vez que se realiza un cambio en la VLAN *database*. Cuando se instala un nuevo *switch* en la red, o se regresa alguno de un mantenimiento es importante revisar el número de revisión en el *switch*

antes de ponerlo en producción, debido a que generalmente vienen con un número de revisión más alto que el resto y ello puede causar que se eliminen las VLAN existentes dentro del dominio VTP.

1.3. Seguridad de la información

Hoy en día se busca transmitir la información de una manera fácil pero segura, se busca proteger y restringir el acceso a la información vulnerable del cliente.

Los tipos de amenazas de acuerdo a la procedencia se clasifican en internas y externas. Para un ataque externo, por ser más complicado el acceso desde afuera, el atacante debe tener conocimientos relacionados a las TI (Tecnologías de Información), al igual que acceso a software especializado y recursos, para realizar ataques e intentar violar las seguridades de la red y tener acceso a recursos e información deseada. Las amenazas internas son aún más peligrosas que las externas, ya que además de los requisitos descritos anteriormente, los atacantes tienen acceso directo a los recursos internos de la red, causando de esta manera un mayor daño sobre la red, ya que por lo general no atraviesan ningún tipo de filtro porque se considera que son usuarios verificados.

1.3.1. Conceptos de la seguridad de la información

Para mantener una red segura es importante distinguir entre los diferentes tipos de ataques de red de los que se puede ser objeto, los principales los citamos a continuación:

i. Vulnerabilidad: Es una debilidad en el sistema, puede ser de carácter tecnológico o político que puede ser explotado.
ii. Amenaza: Es un peligro potencial para la información.
iii. Riesgo: Es la probabilidad de que una vulnerabilidad pueda ser explotada por un ataque específico.

1.3.2. Elementos de la seguridad de la información

Para que la seguridad de la información sea administrada de una manera correcta se debe tener en cuenta requerimientos que aseguren que la información no sea vulnerada, para ello es importante cumplir con lo siguiente:

i. Confidencialidad: Mediante la confidencialidad se asegura que solamente las personas autorizadas tengan acceso a la información y prevenir el acceso no autorizado ya sea de manera intencional o no intencional.
ii. Integridad: La integridad garantiza que la información no haya sido alterada por personal no autorizado, además de que los datos sean consistentes interna y externamente.
iii. Disponibilidad: Asegura el acceso a la información sin interrupciones maliciosas, de una manera segura y oportuna.

Entre las mejores recomendaciones para mitigar los riesgos de seguridad se debe poner en práctica lo siguiente:

i. Deshabilitar los puertos que no se utilizan.
ii. Usar contraseñas que contengan una combinación de caracteres especiales, alfanuméricos y cambiar las contraseñas cada cierto tiempo.
iii. Cifrar la información sensible.
iv. Desarrollar y seguir una política de seguridad.
v. Limitar las contraseñas a mínimo 10 caracteres.
vi. No debe ser una contraseña que se puede encontrar en el diccionario.

1.3.3. AAA

En una red, para evitar que las personas no autorizadas puedan acceder a recursos reservados y confidenciales es necesario implementar seguridades, limitaciones y generar controles de acceso a aplicaciones e información sensible de la red.

Authentication, Authorization and Accounting (autenticación, autorización y contabilización), permite controlar quién accede a la red, qué puede realizar y

qué acciones realizó. Es un componente primordial en la infraestructura de seguridad de una empresa. La autenticación es un proceso que se lleva a cabo en distintos ámbitos, permite que los usuarios de una red demuestren si efectivamente son quienes dicen ser, esto se lleva a cabo mediante uso de sus credenciales que pueden ser usuario/contraseña como se observa en la gráfica, o mediante pregunta/respuesta, *token*, etc.

Figura 32. Autenticación usuario

Tomado de http://www.indsol.com.mx/Soluciones.html?target=Autenticacion

La autorización es el proceso que prosigue a la autenticación, una vez que el usuario ha sido autenticado se valida a qué recursos dentro de las red puede tener acceso.

La contabilización es el proceso que continúa luego de que un usuario es autenticado y autorizado a acceder a los recursos de la red, la contabilización consiste en llevar un registro organizado de las actividades que el usuario o administrador realizaron con los accesos, los diferentes recursos a los que tuvieron acceso, identifica como están siendo utilizados los recursos, la fecha y la hora, el tiempo en el que permanecen en dichos recursos, nombre y dirección IP del dispositivo.

El modelo AAA puede ser configurado de dos maneras, las mismas se describen a continuación:

i. Servicios AAA locales: Como su nombre lo indica utiliza una base de datos local para autenticar, almacenando los nombres de usuario y sus

respectivas contraseñas en el equipo local; estos servicios locales únicamente son recomendables para redes pequeñas. La siguiente imagen ilustra el proceso de autenticación de manera local.

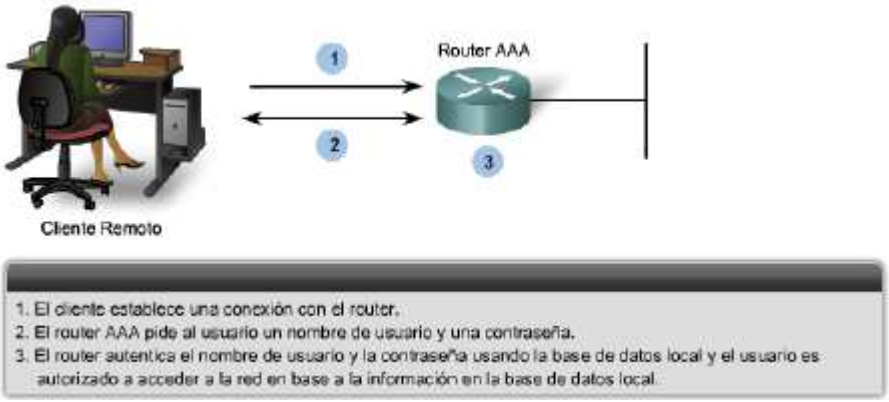


Figura 33. Servicios AAA locales

Tomado de *Cisco Certified Network Associate* Security Versión 1.1

ii. Servicios AAA basados en servidor: Utiliza un servidor externo mediante los protocolos RADIUS o TACACS+ que son los protocolos predominantes utilizados por dispositivos de seguridad para implementar AAA; ésta opción es la recomendable cuando la red tiene más de un equipo. La siguiente imagen ilustra el proceso de autenticación utilizando un servidor externo.

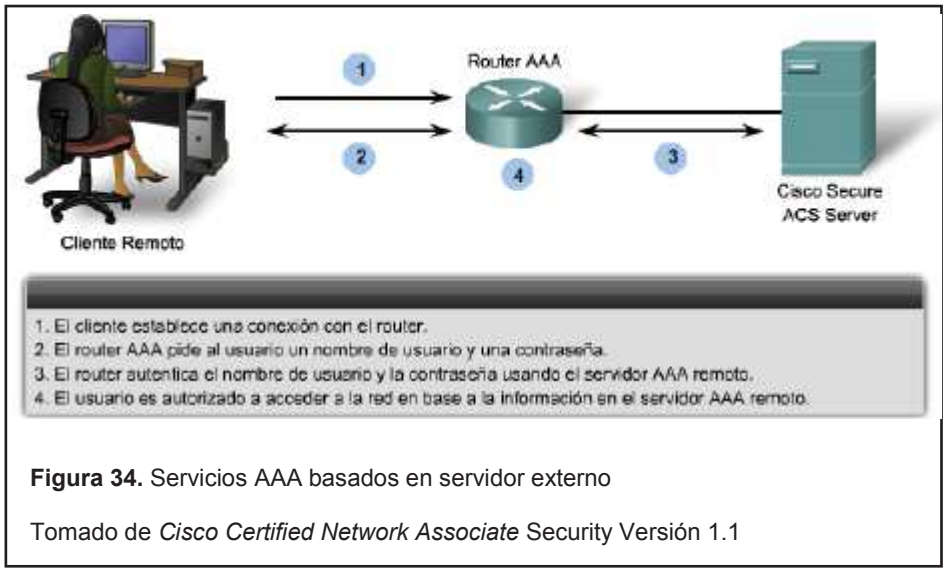


Figura 34. Servicios AAA basados en servidor externo

Tomado de *Cisco Certified Network Associate* Security Versión 1.1

1.3.4. IEEE 802.1X

IEEE 802.1X es un estándar diseñado para que brinde control de acceso a la red basado en puertos.

Este estándar permite autenticar a cada *host* (de manera única) que se conecta a los puertos del *switch* para habilitar o no el puerto y permitir, de ser el caso, el acceso a la red a nivel de capa enlace de datos ya que se configura en cada puerto. Tiene la capacidad de permitir o denegar conectividad, controlar el acceso o aplicar políticas de tráfico dependiendo de la identidad del usuario o de la PC.

La autenticación IEEE 802.1X se basa en EAP (*Extensible Authentication Protocol*), esta autenticación es utilizada en redes *wireless* y cableadas.

EAP fue diseñado para utilizarse en la autenticación para acceso a la red, donde la conectividad de la capa red (direcciones IP) puede no encontrarse disponible. Dado que EAP no requiere conectividad IP, solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación a nivel de capa dos. Es un protocolo de autenticación y control de acceso del tipo cliente/servidor que previene que un usuario/*host* conectado a la LAN (puerto del *switch* o vía inalámbrica) pueda acceder a los recursos de la red, a menos que éste sea autenticado.

El servidor AAA, autentica a cada usuario/host conectado a la LAN antes de que éste pueda acceder a los servicios de la LAN. A continuación se puede observar una imagen en la que se maneja una operación por defecto, es decir sin IEEE 802.1X, en la que se tiene libre acceso a la red.

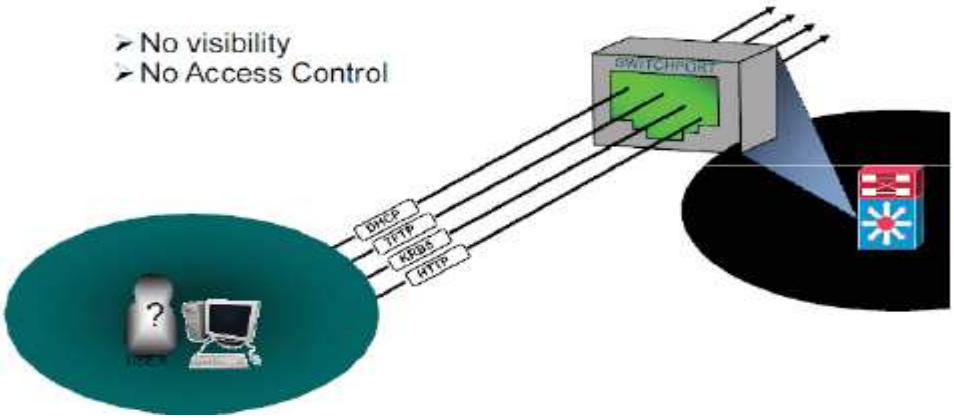


Figura 35. Puerto sin 802.1X

Tomado de http://www.cisco.com/c/en/us/products/ios-nx-os-software/802-1x/index.html

En la siguiente gráfica se puede observar un puerto configurado con IEEE 802.1X, en primera instancia, es decir antes de la autenticación, el tráfico (DHCP, TFTP, KRBS, HTTP) es descartado, permitiendo únicamente el paso del tráfico EAPoL.

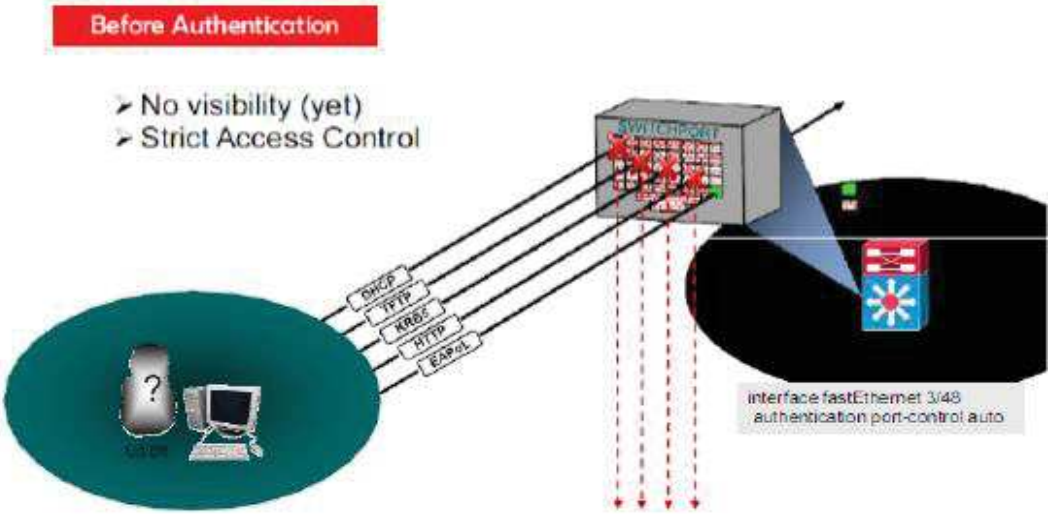


Figura 36. Puerto con IEEE 802.1X antes de la autenticación

Tomado de Cisco Systems, IBNS

En la siguiente gráfica se puede observar un puerto configurado con IEEE 802.1X, en el cual la autenticación es exitosa, razón por la cual permite el paso del tráfico de los protocolos que anteriormente eran descartados.

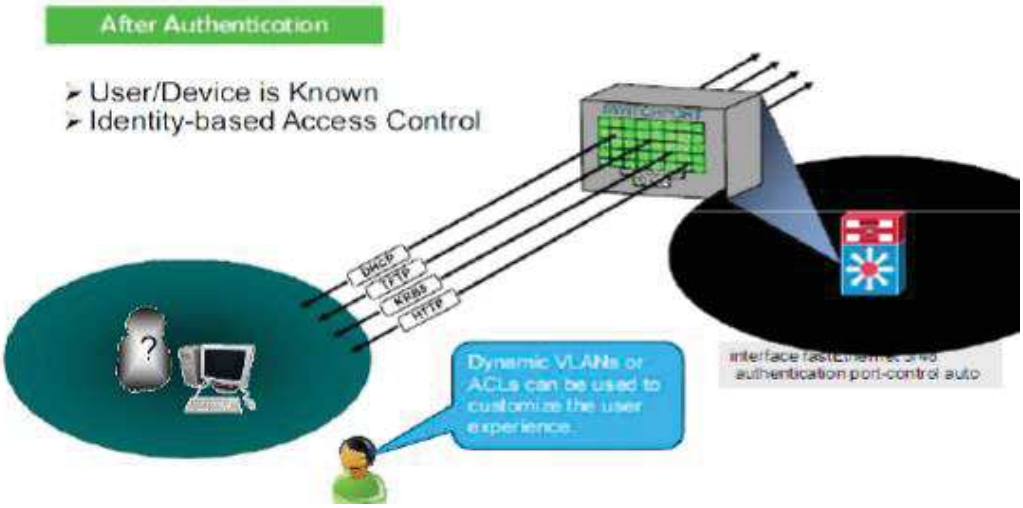


Figura 37. Puerto con IEEE 802.1X después de la autenticación

Tomado de Cisco Systems, IBNS

Para el estándar se maneja tres roles, los cuales se describen brevemente a continuación:

i. Suplicante: Es el cliente IEEE 802.1X, conocida también como estación de trabajo, *host* o usuario.
ii. Autenticador: Es el dispositivo de acceso, puede ser un *switch*, un *access point* autónomo, una *Wireless LAN Controller*, es el dispositivo al cual se pide autorización.
iii. Servidor de Autenticación (AAA): El AAA realiza la autenticación, la autorización y la contabilización.

En la siguiente imagen se ilustra los roles indicados previamente.

Figura 38. Roles de los dispositivos IEEE 802.1X

Tomado de Cisco Systems, IBNS

IEEE 802.1X proporciona una mayor visibilidad en la red, ya que el proceso de autenticación proporciona una manera de vincular un nombre de usuario con una dirección IP, dirección MAC, *switch* y el puerto. Esta visibilidad es útil para las auditorías de seguridad, análisis forense de la red, estadísticas de utilización de la red y solución de problemas.

1.3.5. TACACS+

TACACS+ (*Terminal Access Controller Access Control System Plus)* es un protocolo de seguridad que permite la validación centralizada de usuarios que requieren acceso remoto como TELNET o SSH a *router*s, *switches*, etc., su objetivo es proveer un servicio AAA.

Está orientado a ser utilizado por organizaciones que tienen varios grupos de usuarios porque tiene la ventaja de poder aplicar políticas de autorización ya sea por grupo o por usuario.

Entre las principales características que presenta TACACS+ tenemos que puede separar la autenticación y la autorización, utiliza TCP y que además puede cifrar las comunicaciones.

El proceso utilizado por TACACS+ se describe a continuación con la siguiente gráfica.

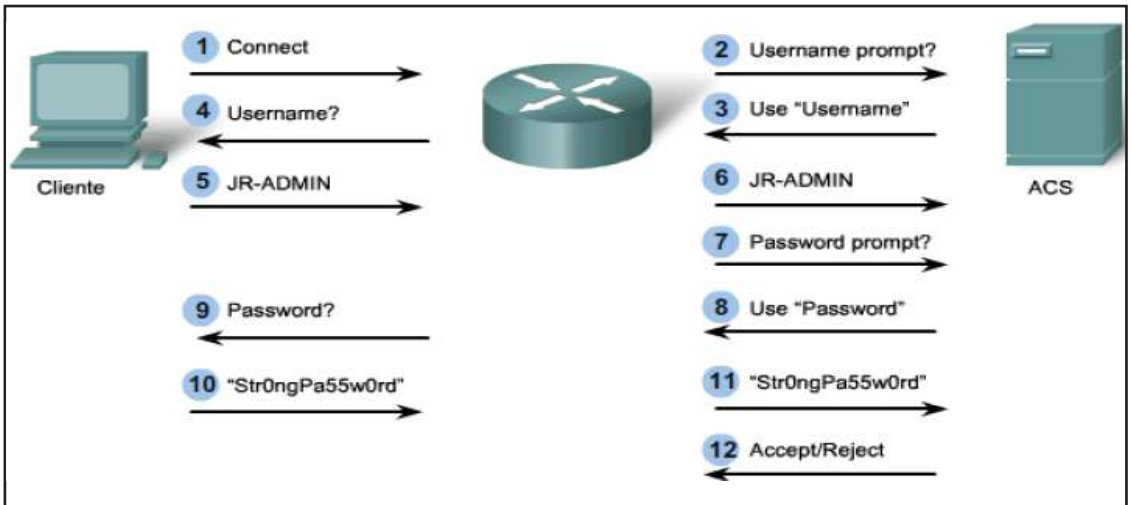


Figura 39. Protocolo TACACS+

Tomado de *Cisco Certified Network Associate* Security Versión 1.1

TACACS+ es propietario de Cisco, proporciona servicios AAA separados. Separar los servicios AAA proporciona flexibilidad en la implementación, ya que es posible usar TACACS+ para autorización y registros de contabilización mientras se usa otro método para la autenticación.

Cuando un usuario requiere acceso a un dispositivo *router*, *switch*, etc, a través del protocolo TACACS+, ocurre el siguiente proceso: cuando la conexión es establecida, se solicita al usuario ingresar sus credenciales (*user* and *password*), dicha información es enviada para la validación de las credenciales y en general para proveer los servicios AAA. Como respuesta del TACACS+ *server* se puede obtener las siguientes respuestas:

i. *ACCEPT*: Las credenciales del usuario son correctas y los otros servicios AAA pueden ser iniciados.
ii. *REJECT*: El usuario falla la autenticación, le es denegado el acceso al usuario.
iii. *ERROR*: Un error ha ocurrido durante el proceso de autenticación, es decir se presentaron problemas de conectividad entre el dispositivo de red y el TACACS+ *server*.

1.3.6. RADIUS

RADIUS (*Remote Autentication Dial-In User Services*) al igual que TACACS+ es un protocolo de administración, RADIUS soporta un registro de auditoría detallado con lo que se puede calcular lo que se debe facturar al usuario, esto es muy útil y utilizado por los ISP (*Internet Service Provider*).

Entre las principales características de RADIUS tenemos que la autenticación y la autorización son combinadas en un solo proceso, utiliza UDP y solamente cifra la contraseña. En la siguiente figura se ilustra el proceso de autenticación de RADIUS.

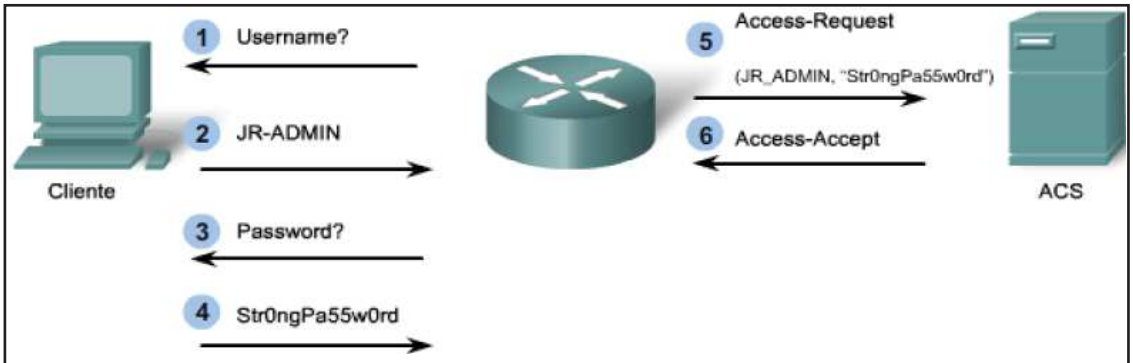


Figura 40. Protocolo RADIUS

Tomado de *Cisco Certified Network Associate* Security Versión 1.1

El protocolo RADIUS esconde las contraseñas durante la transmisión, sin embargo, el resto del paquete se envía en texto plano. RADIUS es un protocolo estándar de la IETF (*Internet Engineering Task Force),* se lo define en los RFCs 2865, 2866, 2867 y 2868. A continuación se presenta una comparación entre RADIUS y TACACS+.

Tabla 1. RADIUS vs TACACS+

COMPARACIÓN ENTRE RADIUS Y TACACS+		
CARACTERÍSTICAS	**RADIUS**	**TACACS+**
Protocolo de transporte	UDP, puertos 1645, 1646, 1812, 1813	TCP, puerto 49
Encriptación de paquetes	Cifra solo la contraseña	Cifra el usuario y contraseña
Autenticación y autorización	Combina autenticación y autorización, la contabilización la maneja por separado.	Separa los 3 elementos de AAA
Recursos	Usa menos memoria y procesamiento	Usa más recursos que RADIUS
Interoperatibilidad	Abierto	Propietario de Cisco

1.3.7. IBNS

IBNS (*Identity Based Networking Services*) está basado en estándares de seguridad de puertos como IEEE 802.1X y *Extensible Authentication Protocol* (EAP), es una solución unificada de Cisco que permite la autenticación, control de acceso y aplicación de políticas de usuarios basadas en identidad, extiende

la seguridad desde el perímetro de la red a todos los puntos de conexión dentro de la LAN para poder así acceder de forma segura a la red.

IBNS permite que las empresas asignen y mantengan, de una manera organizada y segura, el control de accesos de sus usuarios ya sea a nivel cableado, inalámbrico o acceso remoto basado en identidad, permite asignar a los usuarios un perfil de autorización según su identidad.

IBNS maneja tres distintos tipos de autenticación:

i. IEEE 802.1X: Permite la autenticación de los usuarios/*host* conectados a los puertos LAN del *switch* permitiendo o no el acceso a la red.
ii. MAB (MAC *Authentication Bypass*): Permite o niega el acceso basado en la dirección MAC del dispositivo que se conecta el puerto.
iii. *Web Authentication*: Proporciona una página web para que el usuario ingrese sus credenciales y de acuerdo a ellas se permitirá o negará el acceso.

En la gráfica siguiente se puede observar los componentes de un esquema IBNS.

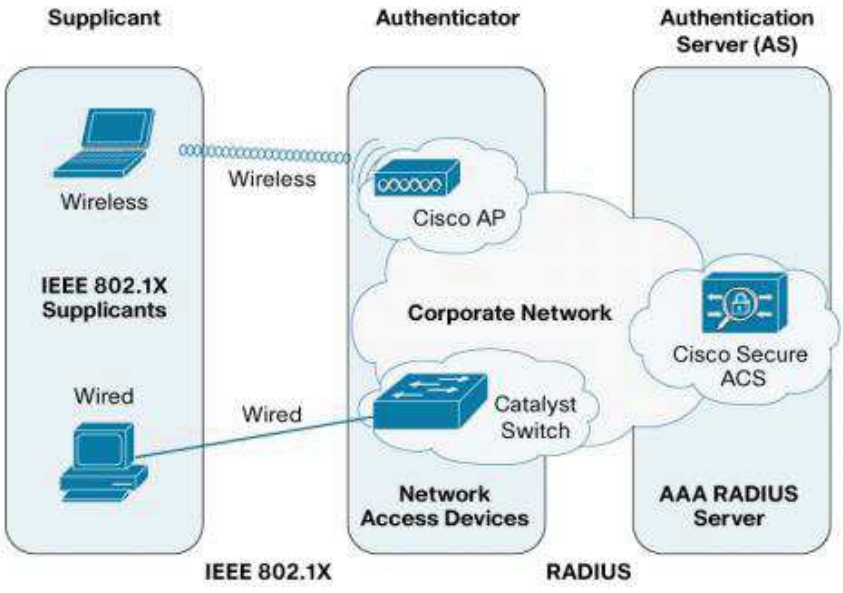


Figura 41. Componentes básicos de un esquema IBNS.

Tomado de http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/data_sheet_c78-542121.pdf

Los elementos constitutivos de la solución de IBNS son:

i. Suplicante: Cliente final (PC, laptop, host) que soporta IEEE 802.1X o no y que envía requerimientos de acceso a la LAN (*switch*/WLC) y responde a los *requests* del *switch*/WLC.
ii. Autenticador: Dispositivo de acceso, *switch*/WLC, que controla el acceso físico a la red basada en el estado de autenticación del suplicante, estos dispositivos actúan como un intermediador entre el cliente y el servidor de autenticación.
iii. Servidor de autenticación: El servidor AAA, en Cisco conocido como *Cisco Secure Access Control Server* (CSACS) es el dispositivo que realiza la autenticación, valida la identidad del suplicante (usuario/*host*), sea en la base de datos interna o en una base de datos externa y notifica al *switch* o WLC si el cliente está autorizado para acceder a la LAN.

En la figura a continuación, se muestra de forma detallada el funcionamiento de una de las características de IBNS, en este caso la autenticación de un usuario final (suplicante) se la realiza mediante el uso de EAP como mecanismo de autenticación, para ello EAP se encapsula en EAPoL entre el suplicante y el autenticador para luego re-encapsularse en RADIUS entre el autenticador y el servidor AAA.

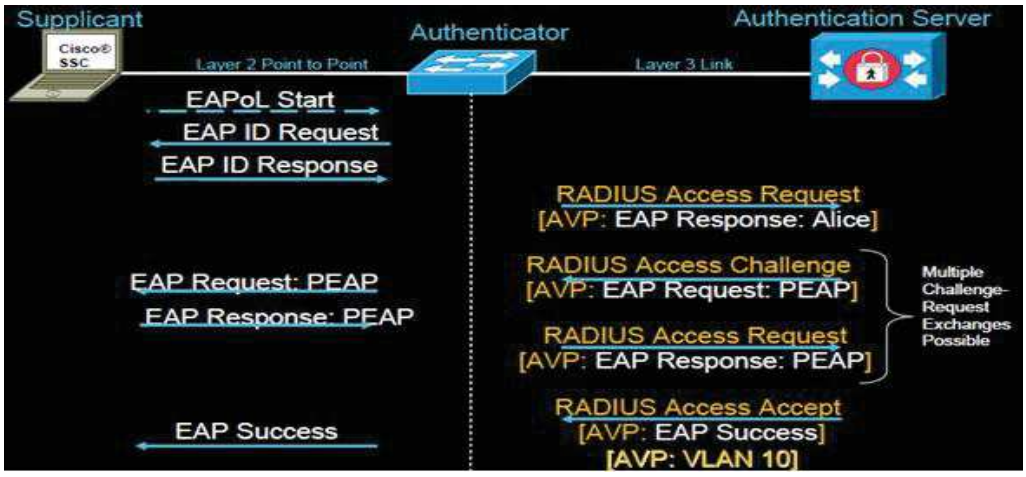


Figura 42. Funcionamiento IBNS (autenticación usuario final)

Tomado de *Cisco Certified Network Associate* Security Versión 1.1

Entre los principales beneficios de utilizar IBNS tenemos:

i. Se crea un ambiente seguro y confiable, tanto para el uso de personal interno como externo de la empresa.
ii. Se reduce situaciones arriesgadas en las que puede verse inmersa la pérdida de información, ya que se crea políticas de usuario de acuerdo a la identidad, definiendo en ellas el nivel de acceso otorgado a los recursos de la infraestructura de red.
iii. Gestiona mejor la movilidad de los empleados, ya que las políticas de acceso están directamente asociadas con la identidad de los usuarios y no con los puertos físicos a los cuales se conectan.
iv. Reduce los gastos que abarca la seguridad del acceso a la red, mediante una solución global de acceso seguro a la red.
v. Ofrece verificación de identidad de manera rigurosa, puesto que puede identificar cada dispositivo y asociarlo con su usuario o las funciones que éste realice.
vi. Permite llevar una contabilización organizada, debido a que se puede obtener reportes de toda la red de la empresa, lo que nos ayuda en algunas tareas como por ejemplo auditorías.

2. Capítulo II. Situación actual de la LAN (Local Area Network)

2.1. Introducción

La LAN actual está conformada por equipos de *networking* de capa dos y capa tres del modelo OSI de distintas marcas como son: 3Com, D-LINK, FORTIGATE, ENTERASYS, entre otras.

El *backbone* es de fibra óptica pero en ciertos pisos los *switch*es se conectan en forma de cascada usando cable UTP, lo que implica una degradación en el rendimiento de la red y un grave punto de falla, para futuras referencias la red conmutada actual se llamará como “red conmutada 3Com”.

En cuanto a seguridad perimetral la LAN cuenta con un *firewall* de características UTM (*Unified Threat Management* o Gestión Unificada de Amenazas) y no tienen ningún mecanismo de seguridad para la red interna tanto cableada como inalámbrica.

Además para el manejo de usuarios y políticas cuentan con un directorio activo levantado sobre un servidor Microsoft Windows Server; las computadoras corporativas tienen instalado en su mayoría el sistema operativo Microsoft Windows XP, pero también cuentan con computadoras con Microsoft Windows 7 (Ultimate, Enterprise y Profesional) y con Windows 8.

2.2. Levantamiento de información de la actual LAN (Local Area Network)

Para el análisis de la actual LAN se procederá a dividir la misma en distintas áreas, para poder analizar cada una con más detalle y de forma más específica. Se dividirá en 7 partes:

i. Red conmutada
ii. Sistema de cableado estructurado
iii. Red inalámbrica
iv. Red telefónica
v. Seguridad perimetral

vi. Seguridad interna

vii. Servicios de *networking*

2.2.1. Red conmutada

La red conmutada está conformada por equipos de *networking* (*switches*) de capa dos y capa tres del modelo OSI de distintas marcas como son: 3Com, D-LINK, ENTERASYS, entre otras. Los *switches* de acceso ubicados en los *rack* de cada piso en su mayoría son de la marca 3Com al igual que el *switch* de núcleo ubicado en el *data center*. El *backbone* es de fibra óptica pero en ciertos pisos los *switches* se conectan en forma de cascada usando cable UTP, lo que implica una degradación en el rendimiento de la red. A continuación en la tabla 2 se listan los equipos implementados por piso, función, nombre, capa dentro del modelo jerárquico de Cisco y marca en la red conmutada actual.

Tabla 2. Red conmutada 3Com – Marca y funcionalidad (1)

RED CONMUTADA 3COM (1) – MARCA Y FUNCIONALIDAD				
PISO	**DESCRIPCIÓN / FUNCIÓN**	**NOMBRE**	**CAPA MODELO JERÁRQUICO**	**MARCA**
Piso 1	*Switch* de núcleo principal con funciones de capa 3 del modelo OSI (L3)	SW_CORE_MATRIZ	Núcleo	3Com
	Switch de acceso con funciones de capa 2 del modelo OSI (L2)	SW_PISO_TI	Acceso	3Com
	Switch de acceso con funciones de capa 2 del modelo OSI (L2)	SW_PISO_1	Acceso	3Com
Piso 2	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	SW_PISO_2	Acceso	3Com
	Switch de acceso con funciones de capa 2 del modelo OSI (L2)		Acceso	3Com
Piso 4	*Switch* de acceso con funciones de capa 2 del modelo	SW_PISO_3y4	Acceso	3Com

	OSI (L2)			
Piso 5	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	SW_PISO_5	Acceso	3Com
Piso 6	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	PISO6	Acceso	3Com
Piso 7	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	SW_PISO_7	Acceso	3Com
Piso 8	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	PISO8	Acceso	3Com
	Switch de acceso con funciones de capa 2 del modelo OSI (L2)	PISO8_1	Acceso	ENTERASYS
Piso 9	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2)	PISO9	Acceso	3Com

Cabe recalcar que en algunos pisos se tienen conectados *switches* no administrables de marca D-LINK en puertos de acceso (en especial en el área de IT), debido a que no existe la suficiente cantidad de puntos de red en algunos pisos para la cantidad de usuarios cableados. La forma en que este tipo de conexiones degrada la eficiencia de la red de información y no es compatible con una solución de seguridad para la red interna como IBNS se describen en la sección falencias encontradas. La siguiente imagen muestra la red actual 3Com simulada en el software Cisco *Packet Tracer*.

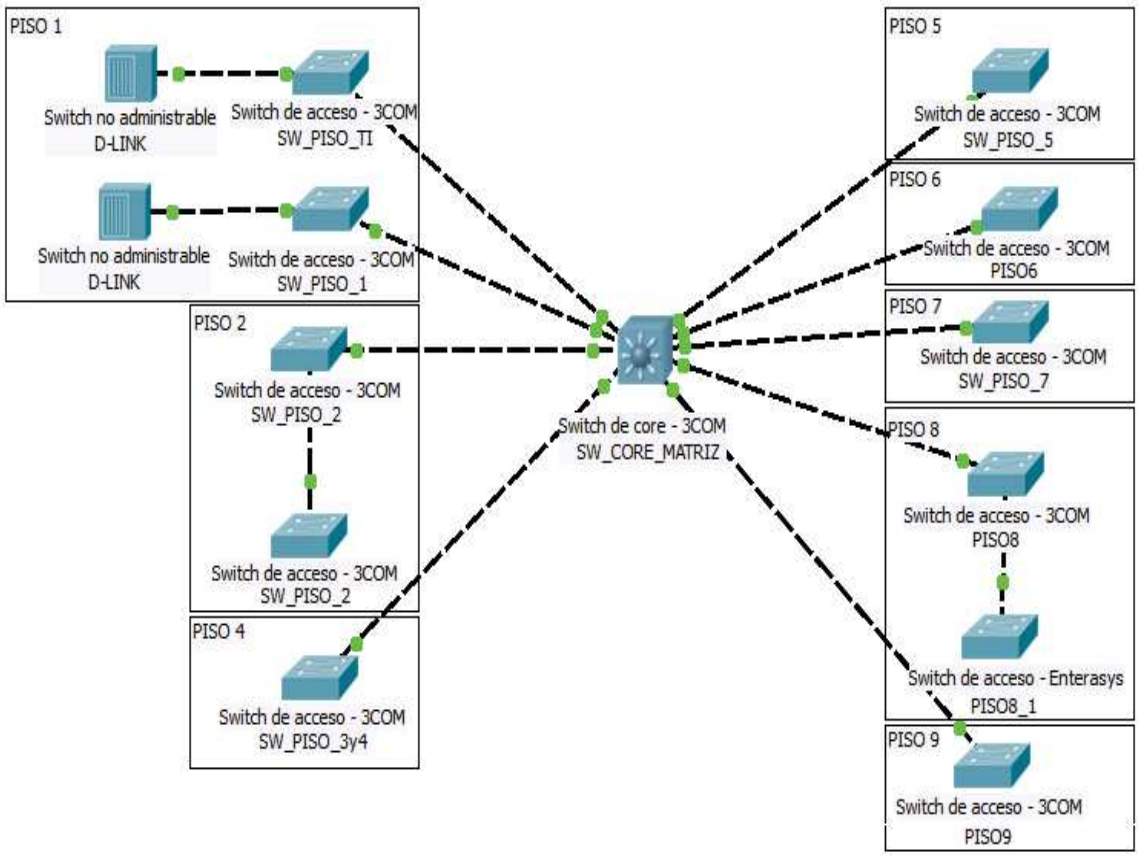


Figura 43. Red actual 3Com simulada en Cisco *Packet Tracer*

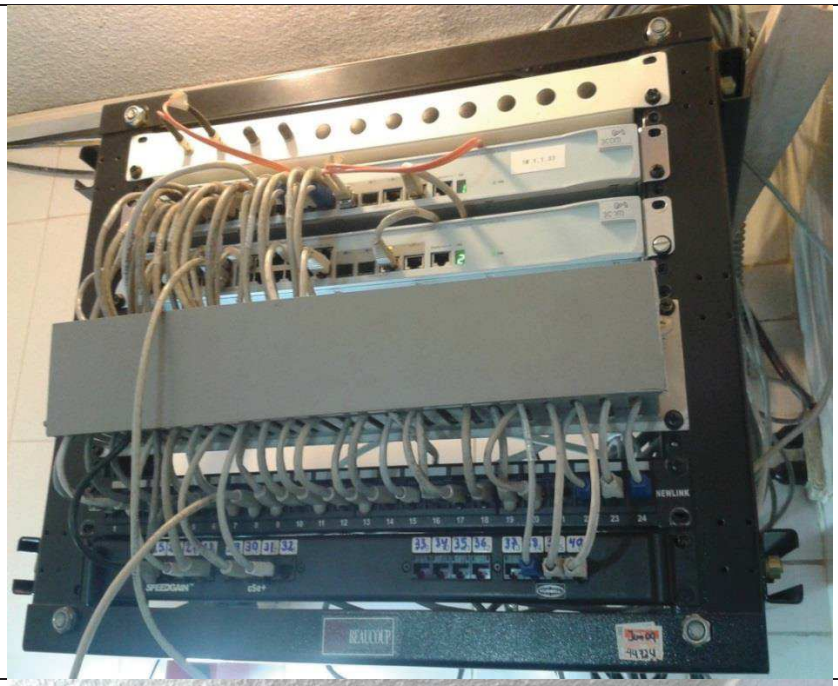
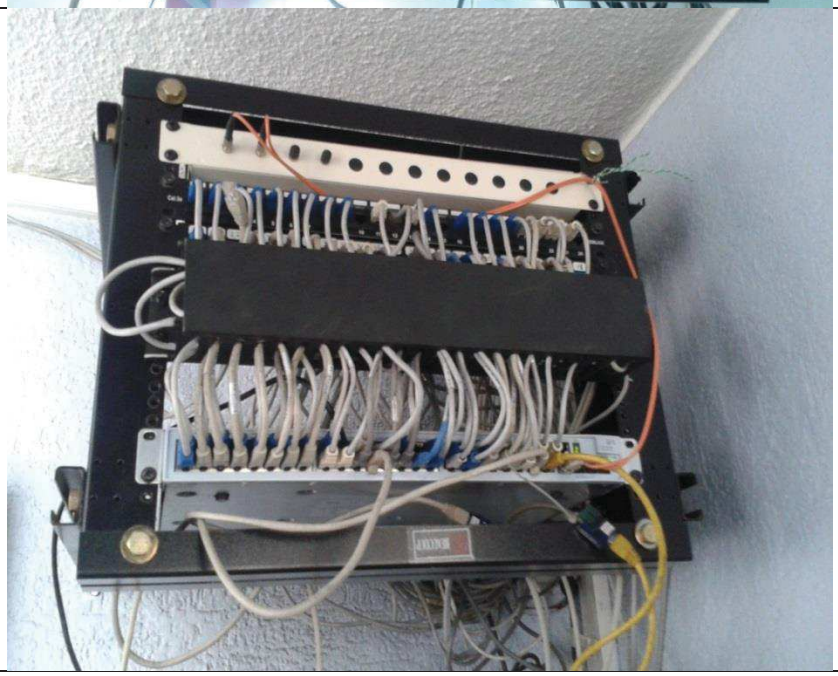
La siguiente tabla muestra los *switches* por piso, nombre, densidad de puertos y cantidad de puertos libres de cada uno.

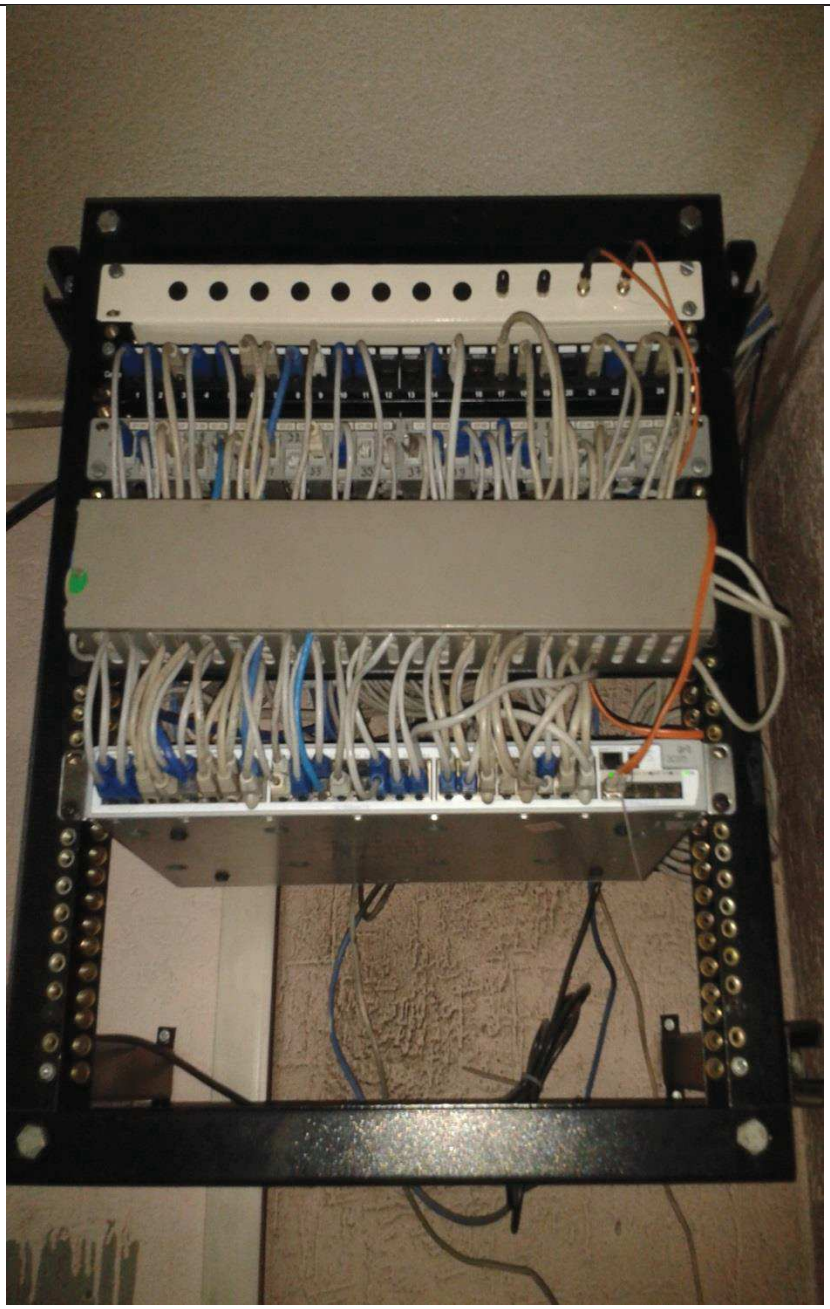
Tabla 3. Red conmutada 3COM – Densidad de puertos (2)

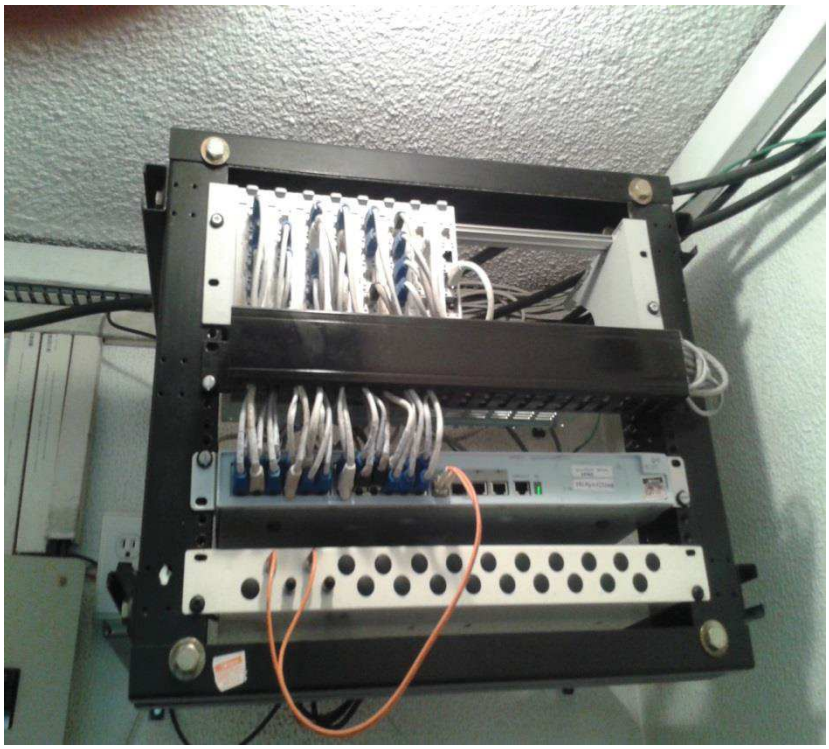
RED CONMUTADA 3Com (2) – DENSIDAD DE PUERTOS			
PISO	**NOMBRE**	**DENSIDAD DE PUERTOS DE DATOS**	**CANTIDAD DE PUERTOS DE DATOS LIBRES**
Piso 1	SW_CORE_MATRIZ	1 tarjeta de 20 puertos de fibra a 1 Gbps	9 de fibra
		1 tarjeta de 48 puertos de cobre a 100 Mbps	18 de cobre
		1 tarjeta de 20 puertos de fibra a 1 Gbps	8 de fibra
	SW_PISO_TI	48 puertos de cobre y 4 puertos de fibra	0 de cobre y 4 de fibra
	SW_PISO_1	24 puertos de cobre y 2 puertos de fibra	0 de cobre y 2 de fibra
Piso 2	SW_PISO_2	24 puertos de cobre y 2 de fibra	1 de fibra
	SW_PISO_2	24 puertos de cobre y 2 de fibra	7 de cobre y 2 de fibra
Piso 4	SW_PISO_3y4	48 puertos de cobre y 4 de fibra	3 de fibra
Piso 5	SW_PISO_5	48 puertos de cobre y 4 de fibra	3 de fibra
Piso 6	PISO6	24 puertos de cobre y 2 de fibra	1 de fibra
Piso 7	SW_PISO_7	48 puertos de cobre y 4 de fibra	3 de fibra
Piso 8	PISO8	48 puertos de cobre y 4 de fibra	17 de cobre y 3 de fibra
	PISO8_1	24 puertos de cobre	0 de cobre
Piso 9	PISO9	24 puertos de cobre y 2 de fibra	0 de cobre

Como se puede observar en la tabla 3 la densidad de puertos está prácticamente agotada por lo que la capacidad de crecimiento en prácticamente todos los pisos es imposible. La siguiente tabla 4 muestra las fotografías tomadas a los *racks* de comunicaciones de cada piso, la imagen de los *switches* del data center y del piso 9 no se incluyen por temas de seguridad.

Tabla 4. Red conmutada 3Com – Fotos (3)

RED CONMUTADA 3COM (3) – FOTOS		
PISO	**NOMBRE**	**FOTOGRAFÍAS**
Piso 1	SW_CORE_MATRIZ	No se incluye por temas de seguridad
	SW_PISO_TI	No se incluye por temas de seguridad
	SW_PISO_1	No se incluye por temas de seguridad
Piso 2	SW_PISO_2	
	SW_PISO_2	
Piso 4	SW_PISO_3y4	

Piso 5	SW_PISO_5	

Piso 6	PISO6	
Piso 7	SW_PISO_7	

<table>
<tr><td rowspan="2">Piso 8</td><td>PISO8</td><td rowspan="2">  </td></tr>
<tr><td>PISO8_1</td></tr>
<tr><td>Piso 9</td><td>PISO9</td><td>No se incluye por temas de seguridad</td></tr>
</table>

En lo referente a los modelos de los equipos implementados en la red conmutada 3Com se detallan en la siguiente tabla.

Tabla 5. Red conmutada 3Com - Modelos y características (4)

RED CONMUTADA 3COM (4) – MODELOS Y CARACTERÍSTICAS			
FUNCIONALIDAD	**MODELO**	**CARACTERÍSTICAS**	
Switch de núcleo	7750	Ancho de banda máximo del sistema: 120 Gbps Backplane: 48 Gbps Throughput máximo del sistema: 89 Mpps	
Switches de acceso	4500	24 puertos	Ancho de banda máximo del sistema: 32 Gbps Máxima capacidad de *switching*: 8.8 Gbps Máxima tasa de reenvío: 6.5 Mpps
		48 puertos	Ancho de banda máximo del sistema: 32 Gbps Máxima capacidad de *switching*: 13.6 Gbps Máxima tasa de reenvío: 10.1 Mpps

En cuanto a las configuraciones de los equipos, el *switch* de núcleo 3Com realiza funciones de *routing*, su ruta por defecto es la interfaz INSIDE del *firewall* UTM que es el equipo de frontera. Este equipo tiene configurado 29 interfaces VLAN que permiten manejar distintos segmentos de red en la LAN. Cada interfaz VLAN del *switch* de núcleo es el *default gateway* de las máquinas que estén en ese segmento de red (VLAN).

Los *switches* de acceso solo realizan funciones de conmutación y se comunican con el *switch* de núcleo mediante enlaces troncales, los demás puertos están configurados en modo acceso en su respectiva VLAN, ya sea VLAN de datos o de voz. A continuación se adjuntan las configuraciones genéricas y las explicaciones de los puertos de acceso y troncal de los *switches* 3Com. En el puerto de acceso se tienen las siguientes configuraciones:

stp edged-port enable
port link-type hybrid
port hybrid vlan 20 40 tagged
port hybrid vlan 6 untagged
port hybrid pvid vlan 6
broadcast-suppression pps 3000

Como se puede observar en la configuración anterior el puerto del *switch* está en modo acceso en la VLAN 6 (datos), las VLANs 20 y 40 son VLANs de voz que se tienen que etiquetar (*tagged*) manualmente. Además se encuentra configurado el equivalente al comando *spanning-tree portfast* en Cisco que le indica al puerto que no pase por los 4 estados del protocolo STP sino que directamente pase al estado de *forwarding* y un mecanismo de supresión de tormentas de *broadcast* que coloca el umbral en 3000 paquetes *broadcast* por segundo. En el puerto troncal se tienen las siguientes configuraciones:

port link-type trunk
port trunk permit vlan all
broadcast-suppression PPS 3000

Como se puede observar en la configuración anterior el puerto del *switch* está en modo troncal y permite que pasen todas las VLAN (las VLAN que están permitidas varían de un enlace troncal a otro) y un mecanismo de supresión de tormentas de *broadcast* que coloca el umbral en 3000 paquetes *broadcast* por segundo. En la siguiente imagen se muestra un esquema general de la red conmutada 3Com implementada en TAME EP en su edificio Matriz.

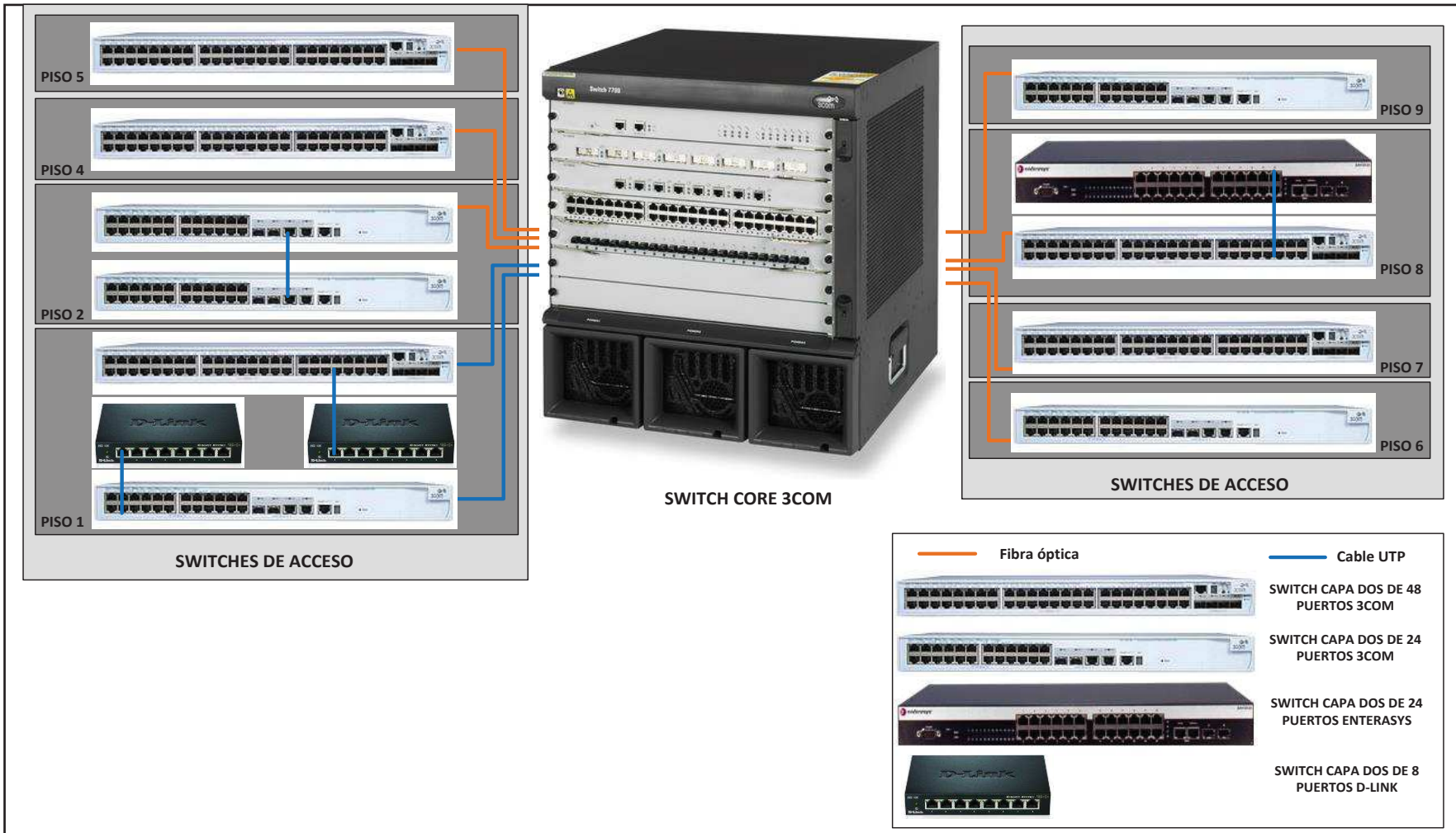


Figura 44. Topología red conmutada 3Com

2.2.2. Sistema de cableado estructurado

En cuanto al sistema de cableado estructurado del edificio Matriz no se tiene un estándar para el subsistema horizontal, subsistema vertical y mucho menos para el área de usuario. El subsistema vertical o *backbone* es de fibra óptica multimodo pero en ciertos pisos los *switches* se conectan en forma de cascada usando cable UTP (*Unshielded Twisted Pair*) ya que no existen suficientes hilos de la fibra óptica para todos los pisos.

En cuanto al subsistema horizontal no tiene una única marca de cables UTP y tampoco de categoría de los mismos implementados en todo el subsistema, los cables en cada *rack* de pared donde se ubica el *switch* de piso son de distinto color, marca, categoría y largo. Cabe recalcar que los *patch panels* de todos los pisos no son iguales y también difieren en tamaño y marca.

Los *patch cords* del área de usuario no están estandarizados, existen canaletas visibles a los largo del área de usuario e inclusive existen cables expuestos en algunas áreas.

El cableado horizontal, el cableado vertical y los cables de área de usuario no siguen ningún estándar de cableado estructurado, cabe recalcar que las instalaciones donde funciona TAME EP no fueron construidas contemplando la instalación de una red de información, es decir la red de información se instaló luego de que el edificio ya estaba funcionando.

2.2.3. Red inalámbrica

La red inalámbrica provee un servicio de conectividad inalámbrica a las instalaciones de TAME EP en su edifico Matriz, actualmente dispone de equipos inalámbricos en todos los pisos dentro del edificio (un *access point* por cada piso). TAME EP presenta una solución de redes inalámbricas unificadas bajo la plataforma FORTINET, usando una controladora inalámbrica FORTIGATE modelo 100D la cual permite una gestión unificada de toda la solución y equipos de acceso inalámbricos (*Access Point*) modelos 210B y 220B con estándares IEEE 802.11 a/b/g/n que permiten que los usuarios

accedan a los servicios de la LAN a través de la red inalámbrica. Los beneficios que se derivan de transportar comunicaciones por una infraestructura inalámbrica son:

i. Movilidad: Ya no se tiene que estar atado a su mesa de trabajo, tanto empleados y huéspedes pueden conectarse desde cualquier lugar dentro de la empresa, por ejemplo, desde una sala, un hall, etc.
ii. Soporte: La gran mayoría por no decir todas las funcionalidades y características de las redes cableadas tradicionales como VLANs, QoS (*Quality of Service*), etc. están presentes.
iii. Productividad: En el caso de sus empleados el acceso inalámbrico a Internet, a las aplicaciones y recursos ayudan al personal a hacer su trabajo y fomenta la colaboración.
iv. Capacidad de ampliación: Puede ampliar fácilmente las redes inalámbricas con el equipo existente, mientras que una red por cable requiere cableado adicional.

La siguiente imagen muestra un esquema general de la red inalámbrica implementada en TAME EP en su edificio Matriz.

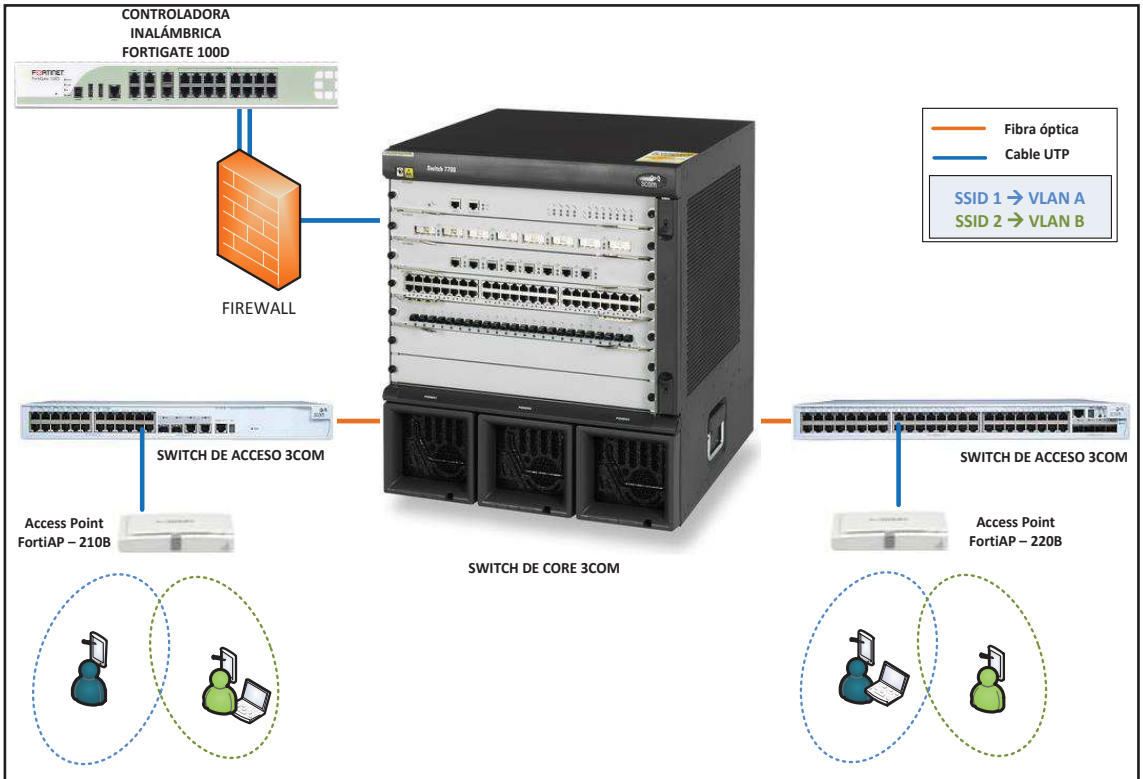


Figura 45. Topología Wireless

2.2.4. Red telefónica

TAME EP tiene una red telefónica de voz sobre IP (VoIP), es decir tanto la voz como los datos se transfieren por la misma red de información. Esta red está formada por una central telefónica de marca ELASTIX modelo ELX 5000B, además cuenta con aproximadamente 500 teléfonos IP de marca Yealink. Las sesiones multimedia entre los teléfonos IP son señalizadas y controladas por el protocolo estándar SIP (*Session Initiation Protocol*) creado por la IETF (*Internet Engineering Task Force).* La siguiente imagen muestra un esquema general de la red telefónica implementada en TAME EP en su edificio Matriz.

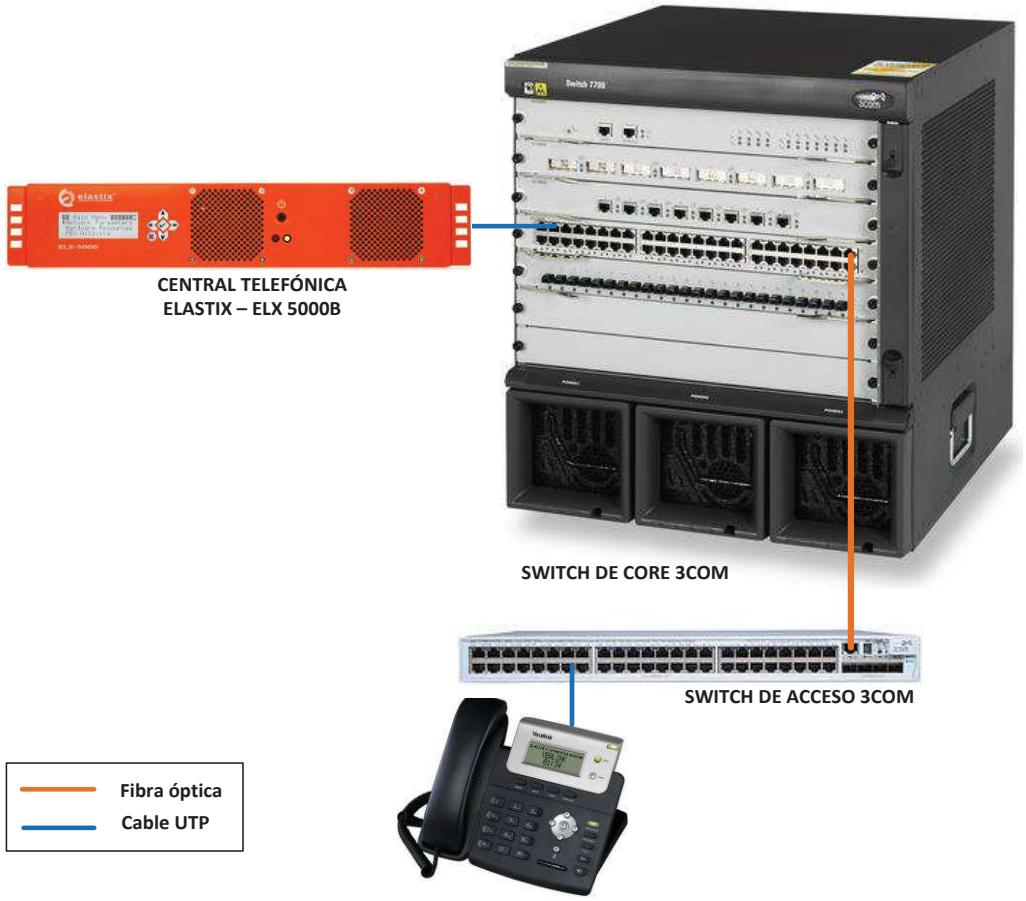


Figura 46. Topología red telefónica

2.2.5. Seguridad perimetral

La empresa TAME EP cuenta con un *firewall* de última generación con características UTM (*Unified Threat Management*), este equipo está ubicado entre la LAN del edificio Matriz, las oficinas ubicadas en las distintas provincias, las localidades en Tababela y la Internet. Este *firewall* de última generación de marca Check Point es el que da la cara al mundo y tiene las siguientes funciones:

i. *Firewall* (Contrafuegos)
ii. IPSec VPN (VPNs sitio a sitio, VPNs para trabajadores remotos)
iii. IPS (*Intrusion Prevention System* o Sistema de Prevención de Intrusos)
iv. Filtrado URL
v. Anti-Bot

vi. Antivirus
vii. Identity Awareness (Conciencia de identidad)
viii. DLP (*Data Loss Prevention* o Prevención de Pérdida de Información)
ix. Web Security (Seguridad Web)
x. Anti-Spam & Seguridad email.

Actualmente tiene configuradas y activas todas las funciones descritas anteriormente, excepto la de anti-spam. Soporta 66000 sesiones concurrentes, 2500 conexiones por segundo, hasta 10000 transacciones HTTP por segundo y soporta hasta 5000 usuarios. La topología UTM es la siguiente:

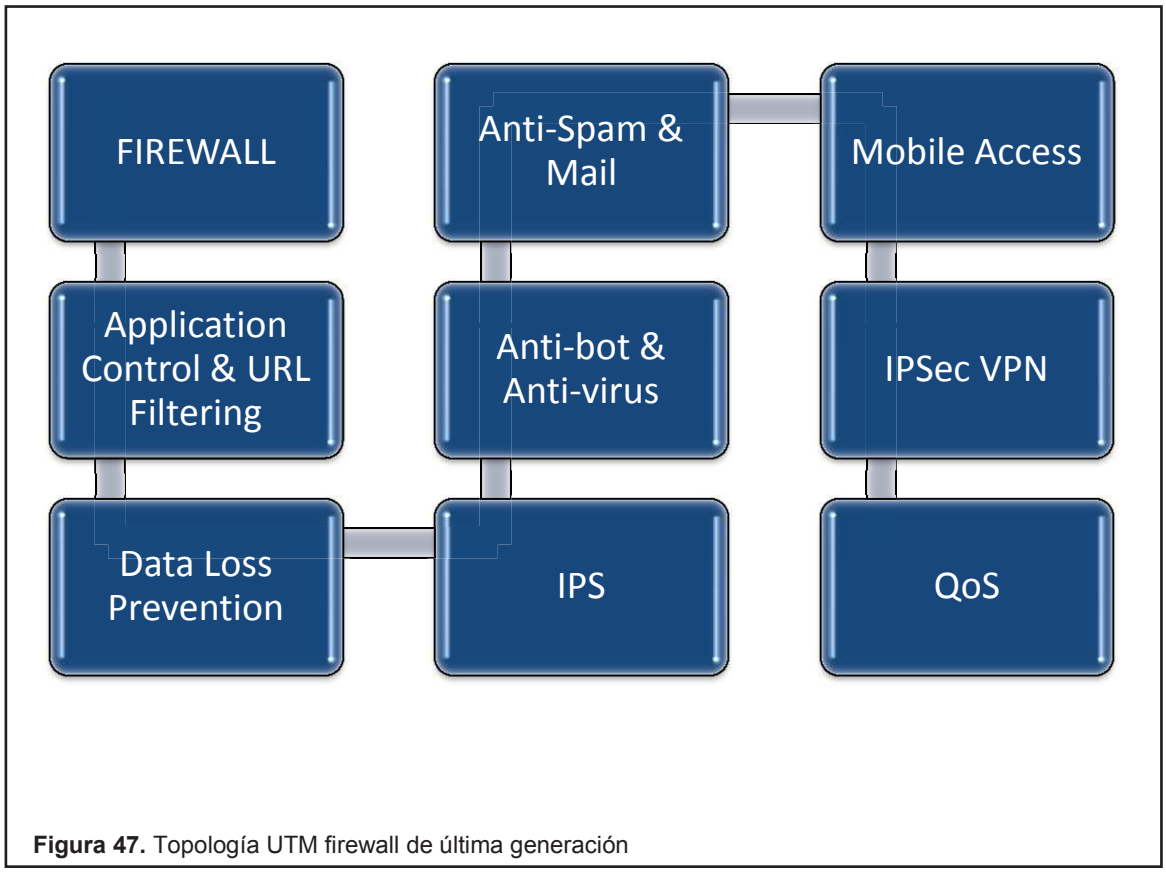


Figura 47. Topología UTM firewall de última generación

No se especificará modelo o versión ni direcciones IP por temas de seguridad. La siguiente imagen ilustra la seguridad perimetral de TAME EP de manera general.

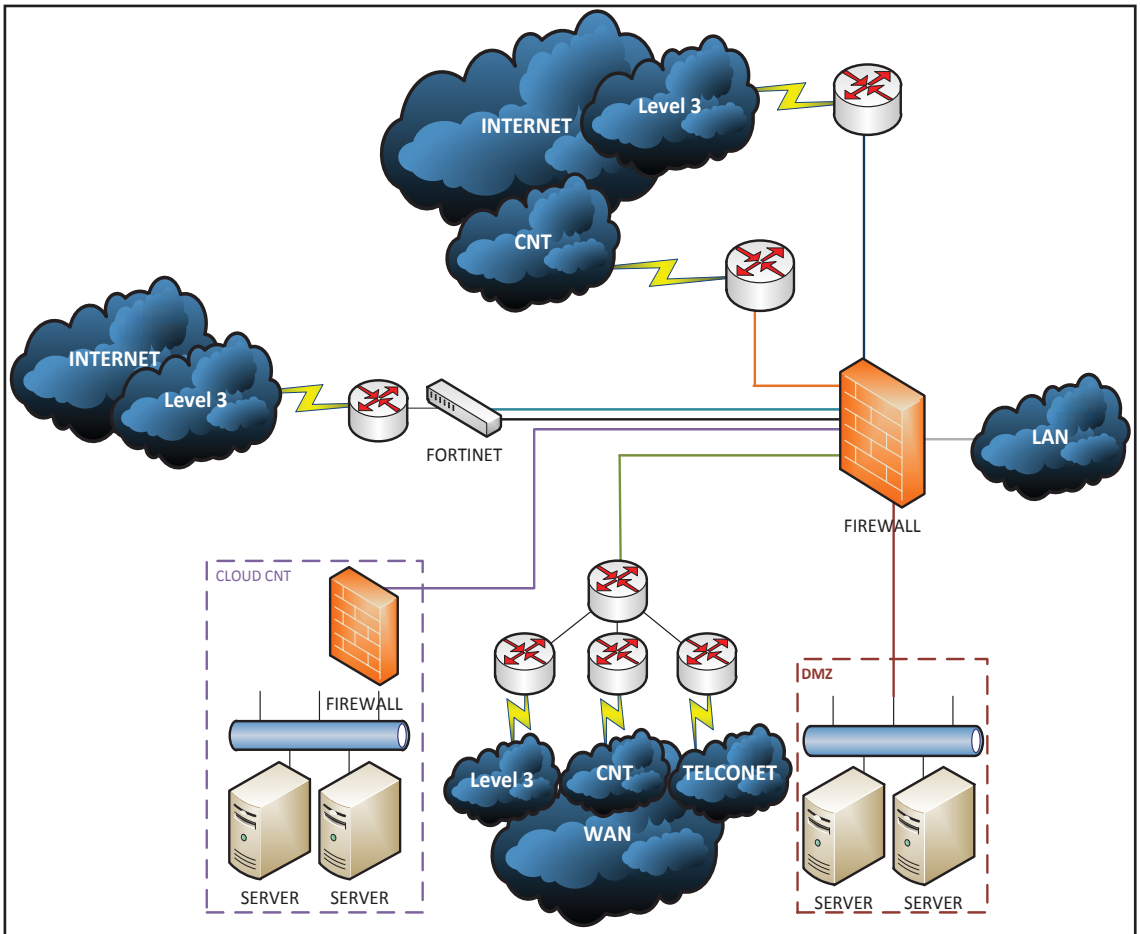


Figura 48. Seguridad perimetral red 3Com

2.2.6. Seguridad interna

Actualmente no existe ningún mecanismo que permita cierto nivel de seguridad a nivel de la red interna, a nivel de red cableada no hay ningún tipo de seguridad (IEEE 802.1X, MAB, etc.) la única prevención es en la red inalámbrica con SSID protegidos con WPA2 – Personal.

2.2.7. Servicios de *Networking*

Los servicios de *networking* se encuentran corriendo sobre sistemas operativos instalados en máquinas virtuales sobre la plataforma VMware ESX 5.0 la misma que está instalada en blades IBM. El directorio activo está levantado sobre una máquina virtual con el sistema operativo Windows Server 2008 R2,

esta misma máquina virtual realiza las funciones de DHCP Server, DNS Server y NTP Server.

El servicio de correo electrónico con dominio: tame.com.ec está levantado sobre un IBM Lotus 852. El servicio de correo electrónico tiene un nivel de seguridad adicional ya que todos los correos entrantes y salientes pasan por servidores antispam llamados Lycan y Nosferatus del *service provider* Level 3 (estos servidores tienen los registros MX del domino tame.com.ec). La siguiente imagen muestra un esquema general del servicio de correo electrónico.

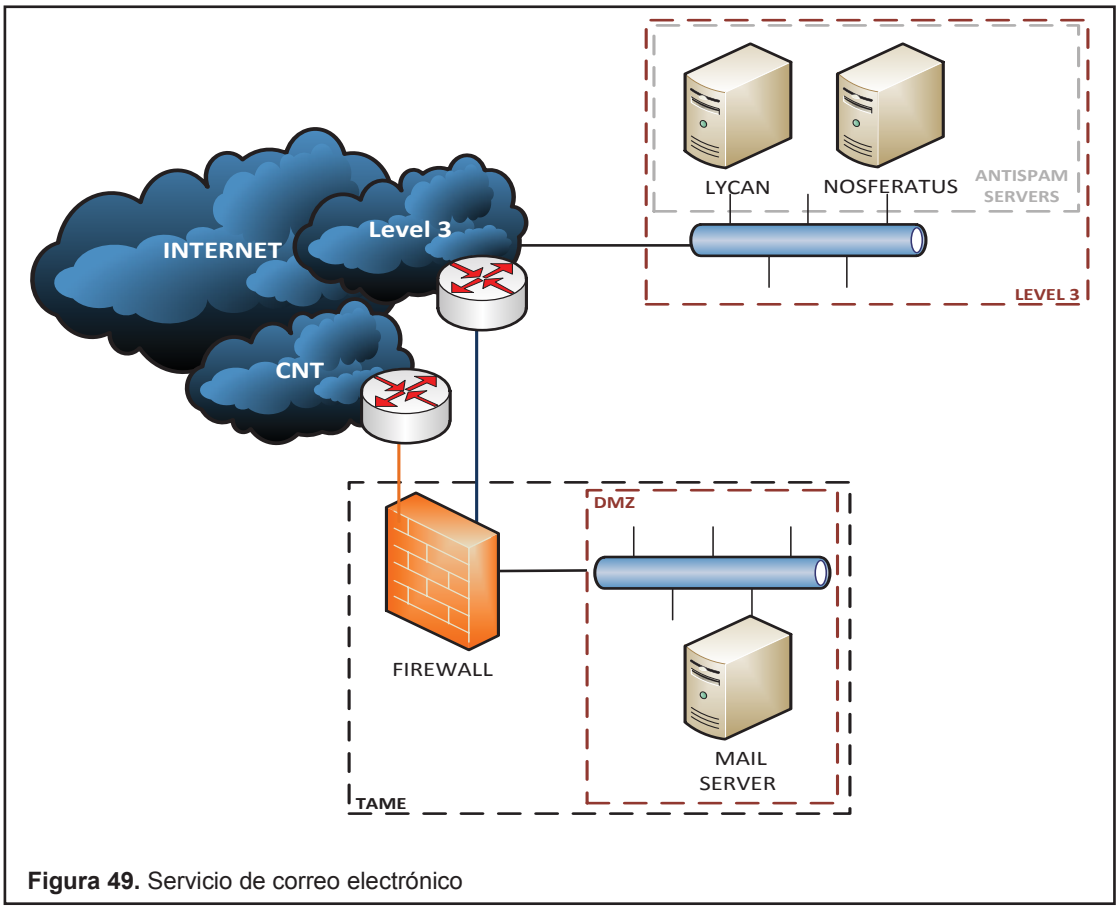


Figura 49. Servicio de correo electrónico

La página web de la empresa está almacenada (*hosting*) en La Nube, la misma que está diseñada con WordPress, cabe recalcar que las aplicaciones propias de la empresa en su mayoría están virtualizadas.

2.3. Topología completa de la actual LAN

La siguiente imagen muestra la topología completa de la actual red de información.

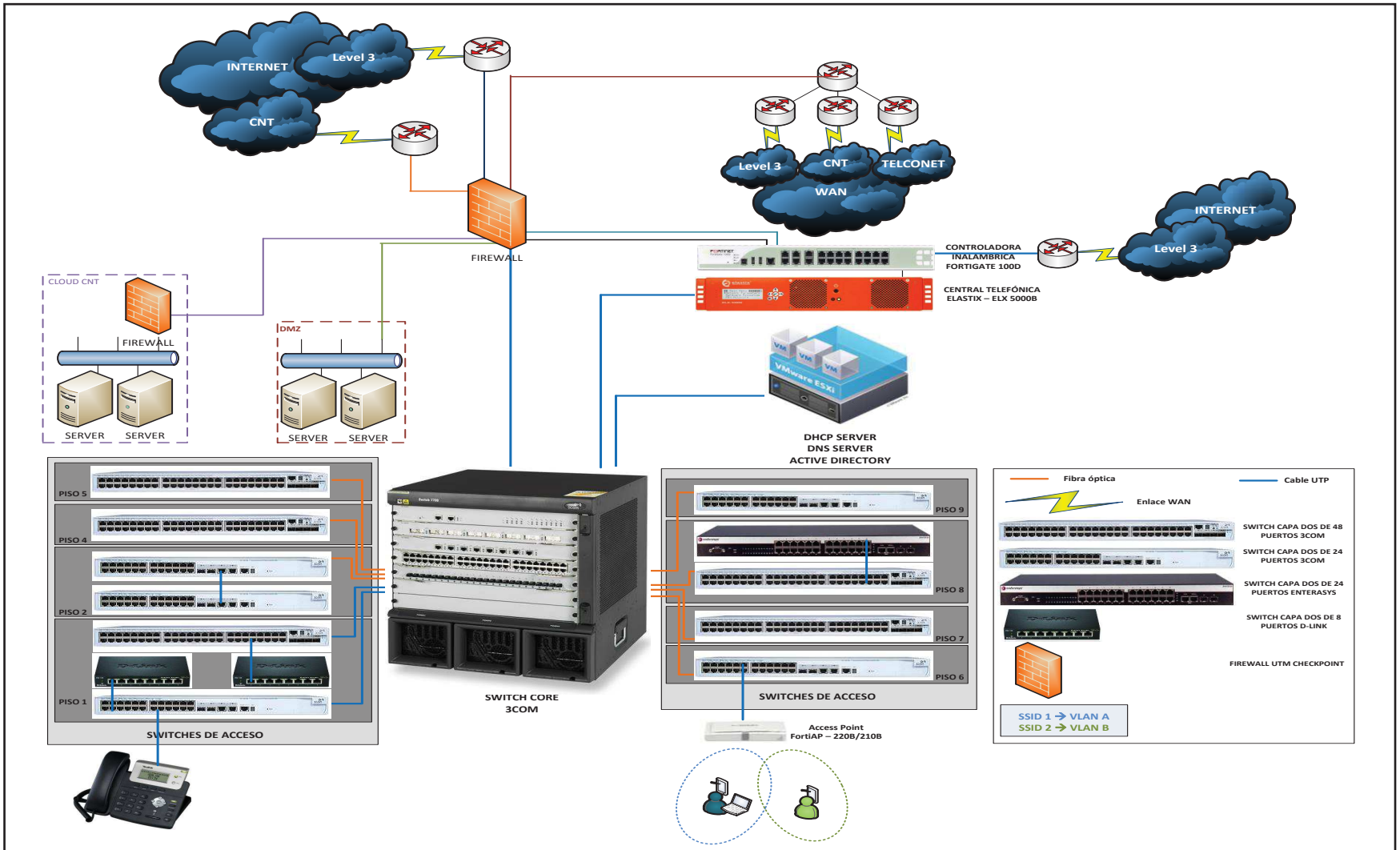


Figura 50. Topología completa actual 3Com

2.4. Falencias encontradas

Una vez levantada toda la información de la LAN y analizando cada área podemos describir las siguientes falencias encontradas:

i. La red actual cuenta con equipos de distintas marcas, lo que implica que se necesita especialistas en cada marca, más de un proveedor por cada marca e implica que el administrador de red debe conocer las configuraciones, los comandos para configurar y el funcionamiento específico de cada marca, además el stock de repuestos es demasiado grande por lo que no se puede dimensionar.

ii. La topología actual de la red conmutada no permite un correcto manejo de alta disponibilidad, redundancia, ni la posibilidad de crecimiento ya que la densidad de puertos en todos los *switches* está prácticamente agotada.

iii. La mayoría de computadoras personales de la empresa cuentan con el sistema operático Windows XP, este sistema operativo además de ya no tener soporte por parte de Microsoft tiene problemas al momento de integrarse con un sistema IBNS.

iv. La marca de prácticamente toda la red conmutada es 3Com y esta fue absorbida por la marca HP. Desde esta absorción ya no existe soporte técnico para todos los productos de la marca 3Com.

v. Los nombres de los *switches* no están estandarizados, como una buena práctica se debe indicar en el nombre del *switch* en que piso está y si es más de uno por piso indicar cuál es el principal y cuál el secundario, es una mala práctica tener distintos equipos con el mismo nombre.

vi. Todo el cableado estructurado de la red no está estandarizado, ni el cableado vertical ni el horizontal, además no existe conexiones físicas

desde el *data center* (donde se ubica el *switch* de núcleo) a cada piso del edificio lo que implica que no se puede configurar una topología en estrella completa.

vii. El hecho de que no exista ningún sistema de seguridad para la red interna implica un grave punto de falla ya que la LAN es mucho más vulnerable a ser comprometida, solo se necesita descifrar la clave de la red inalámbrica o encontrar un punto de red habilitado para tener acceso a todos los servicios de la misma.

viii. No existe un mecanismo que permita una auditoría correcta (*accounting*) de que persona ingresó, a qué hora del día y desde que equipo, a la red de información ya sea a los equipos de *networking* o como usuario final.

ix. El hecho de que exista *switches* no administrables conectados en puertos de acceso dificultarán el despliegue del sistema IBNS en esos puertos específicos, además los actuales *switches* 3Com no soportan una solución de servicios de red basados en identidad (IBNS).

3. Capítulo III. Diseño de la nueva red conmutada y del servicio de red basado en identidad (IBNS)

3.1. Introducción

La nueva red conmutada a implementarse en TAME EP en el edificio Matriz deberá mejorar las características y rendimiento de la actual red conmutada, además de eliminar las falencias encontradas en la misma. Es por eso que el diseño es una parte fundamental para que la nueva red conmutada cumpla con las expectativas de la empresa.

IBNS tiene como objetivo establecer un mecanismo de seguridad interna tanto a nivel LAN como WLAN que permita el acceso seguro a la red de TAME EP basados en la identidad y el estado de autenticación de todos los usuarios (usuarios corporativos, proveedores, visitantes, dispositivos periféricos, entre otros) que conforman la red.

Cabe recalcar que el diseño del presente proyecto tomará como referencia los pliegos presentados en el proyecto “ADQUISICIÓN E INSTALACIÓN DE EQUIPOS DE CONMUTACIÓN PARA OPERAR Y BRINDAR LA CONECTIVIDAD EN LA RED DEL NUEVO AEROPUERTO Y MATRIZ DE QUITO” por parte de la empresa pública TAME Línea Aérea del Ecuador "TAME EP".

3.2. Lineamientos principales para el diseño de redes conmutadas

En esta sección se tomará como base modelos de diseño y mejores prácticas referidas por el fabricante Cisco Systems para redes empresariales.

La complejidad de las redes de información actuales requiere un proceso de diseño capaz de separar las soluciones en elementos básicos, el modelo jerárquico de Cisco logra esto dividiendo la infraestructura de red en componentes modulares conocidos como capas.

3.2.1. Modelo jerárquico de Cisco

Las principales características asociadas con cada capa son el diseño jerárquico, la modularidad, y la división de funciones. Un diseño jerárquico evita la necesidad de una red con topología en malla en la que todos los nodos (equipos de *networking*) están interconectados. Este tipo de diseño facilita la solución de problemas (*troubleshooting*) al igual que el aislamiento de problemas y una gestión más eficiente de las redes de información. Además un diseño modular permite que un componente pueda ser reemplazado o puesto fuera de servicio con poco o ningún impacto en el resto de la red (redundancia). Las capas del modelo jerárquico de Cisco son la capa de acceso, distribución y núcleo, como se ilustra en la siguiente imagen:

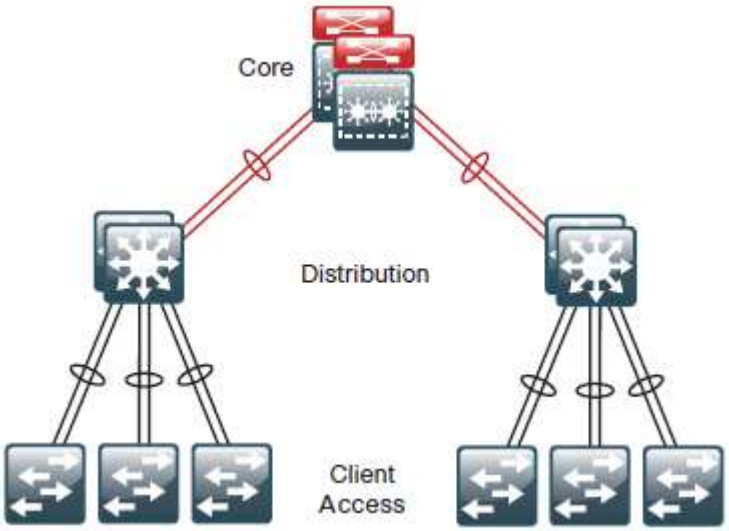


Figura 51. Modelo jerárquico de Cisco

Tomada de Cisco Campus Wired LAN, Technology Design Guide, Abril 2014

La capa de acceso es el punto de entrada a la red para los dispositivos finales, agrega a los dispositivos finales (computadoras, portátiles, teléfonos IP, dispositivos móviles) y proporciona enlaces a la capa de distribución. La capa de acceso puede soportar múltiples funciones como son: alta disponibilidad, convergencia, seguridad y calidad de servicio. La siguiente figura ilustra una imagen de la capa de acceso.

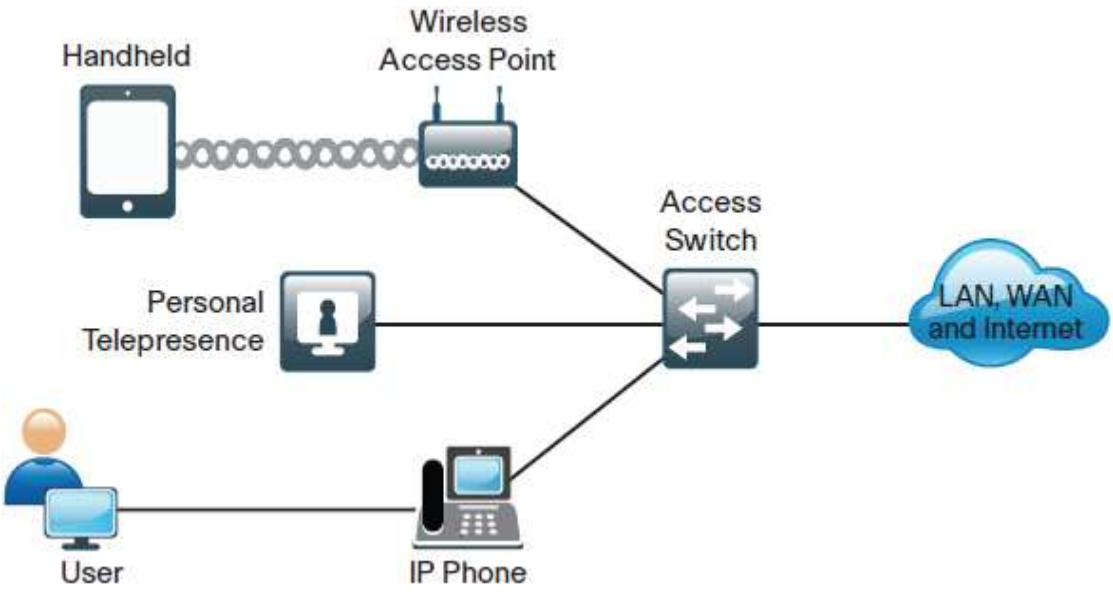


Figura 52. Capa de Acceso

Tomada de Cisco Campus Wired LAN, Technology Design Guide, Abril 2014

La capa de distribución proporciona conectividad basada en políticas y permite la comunicación entre la capa de acceso y la capa núcleo. Esta capa debe soportar características como: aprovisionamiento, alta disponibilidad, balanceo de carga y calidad de servicio. La alta disponibilidad se proporciona normalmente a través de caminos dobles (redundancia de enlaces) de la capa de distribución a la capa núcleo y de la capa de acceso a la capa de distribución. Existen mecanismos que trabajan a nivel de capa tres del modelo OSI que permiten que ambos enlaces de la capa de distribución a la capa núcleo se utilicen al mismo tiempo (balanceo de carga). La capa de distribución se encarga del *routing* y la manipulación de paquetes, además una de las funciones principales de la capa de distribución es aislar problemas de red evitando que afecten la capa núcleo y conecta servicios de red a la capa de acceso. Otra de las funciones principales de esta capa es la de proporcionar redundancia a nivel de puerta de enlace predeterminada utilizando protocolos de redundancia (HSRP o VRRP) para permitir la falla de uno de los *switches* de distribución sin afectar la conectividad hacia la puerta de enlace

predeterminada (*default gateway*) de los equipos finales. La siguiente figura ilustra una imagen de la capa de distribución.

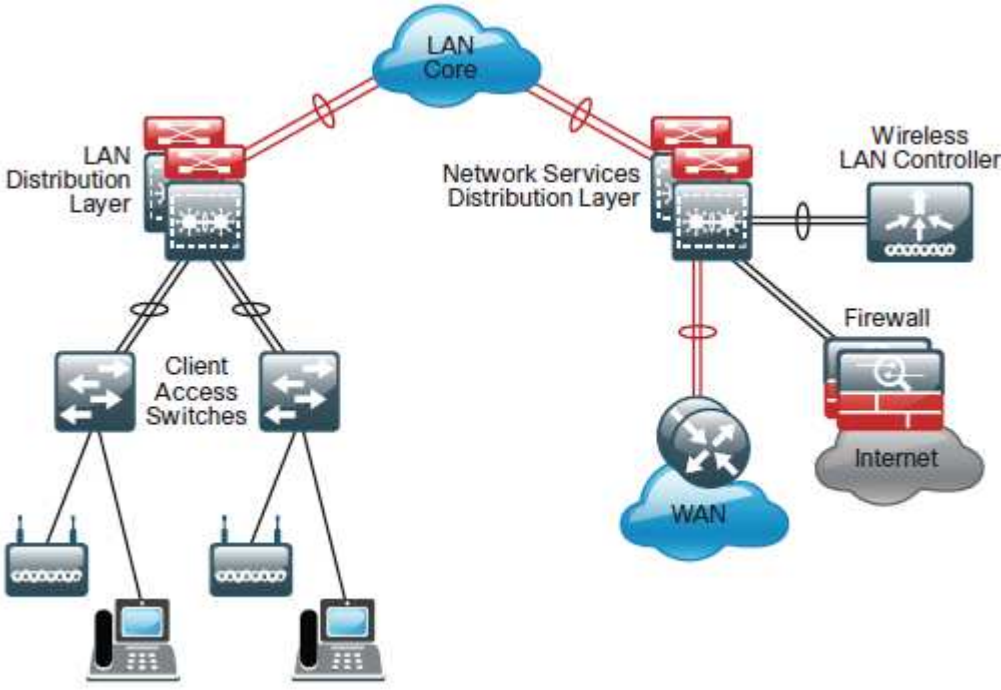


Figura 53. Capa de distribución

Tomada de Cisco Campus Wired LAN, Technology Design Guide, Abril 2014

La capa núcleo proporciona alta disponibilidad (redundancia), convergencia y escalabilidad. La capa núcleo es la estructura principal para la conectividad de toda la red de información. Los equipos que funcionen en esta capa deben ser confiables, capaces de redirigir el tráfico y converger rápidamente cuando existen cambios en la topología. Está diseñada para evitar cualquier manipulación de paquetes, como la comprobación de las listas de acceso y filtrado, que frenaría la conmutación de paquetes, que es su función principal. No todas las implementaciones requieren una capa de núcleo, las funciones básicas de la capa núcleo y la capa de distribución se pueden combinar en la capa de distribución para soluciones más pequeñas. La siguiente figura ilustra una imagen de la capa núcleo.

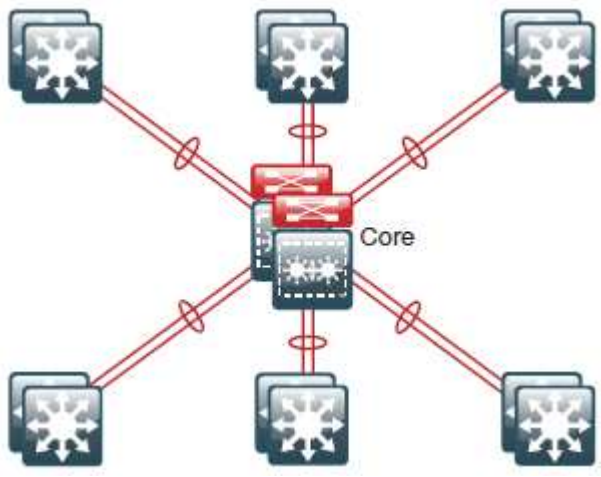


Figura 54. Capa núcleo

Tomada de Cisco Campus Wired LAN, Technology Design Guide, Abril 2014

En resumen cada capa del modelo jerárquico de Cisco debe cumplir con las siguientes funciones:

Tabla 6. Funciones y características de cada capa del modelo jerárquico de Cisco

FUNCIONES Y CARACTERÍSTICAS DEL MODELO JERÁRQUICO DE CISCO POR CAPA		
CAPA ACCESO	**CAPA DISTRIBUCIÓN**	**CAPA NÚCLEO**
Seguridad de puerto	Calidad de servicio (QoS)	Calidad de servicio (QoS)
VLANs	Soporte de capa 3 (Modelo OSI)	Soporte de capa 3 (Modelo OSI)
Fast Ethernet / Gigabit Ethernet	Tasa alta de reenvío de tráfico	Tasa muy alta de reenvío de tráfico
Power over Ethernet (PoE)	Gigabit Ethernet / 10 Gigabit Ethernet	Gigabit Ethernet / 10 Gigabit Ethernet
Agregación de enlaces	Componentes redundantes	Componentes redundantes
Calidad de servicio (QoS)	Políticas de seguridad / Listas de control de acceso y agregación de enlaces	Agregación de enlaces

3.2.2. Diseño a nivel de capa dos (modelo OSI)

Para diseñar una red confiable y robusta a nivel de capa dos nos centraremos en las siguientes tecnologías: STP (*Spanning Tree Protocol*), enlaces troncales (ISL/IEEE 802.1Q), DTP (*Dynamic Trunking Protocol*), VTP (*VLAN Trunking Protocol*) y EtherChannel.

3.2.2.1. STP (*Spanning Tree Protocol*)

Aunque algunas buenas prácticas de seguridad indican que se desactive el STP en el borde de la red, el riesgo de perder conectividad por no usar STP es mucho mayor que cualquier información de STP que pueda ser capturada por un atacante. Se necesita implementar STP por las siguientes razones:

i. Para soportar aplicaciones de centros de datos en una granja de servidores.
ii. Cuando una VLAN abarca *switches* de capa de acceso para soportar aplicaciones de negocio, en otras palabras cuando un servidor que contiene aplicaciones de negocio está conectado a un *switch* de capa de acceso.
iii. STP se requiere para proteger contra bucles del lado del usuario. Hay muchas maneras de que se cree un bucle en los puertos de capa de acceso, como por ejemplo: errores de cableado, estaciones finales mal configuradas o usuarios maliciosos. STP se requiere para asegurar una topología libre de bucles y para proteger el resto de la red de problemas creados en la capa de acceso.

STP permite a la red indicar qué interfaces van a estar bloqueadas, por ende permite ofrecer una topología libre de bucles (lazos) en una red con enlaces redundantes. Según las buenas prácticas de Cisco sugiere implementar RPVST+ (*Rapid Per-VLAN Spanning-Tree Plus*) debido a que RPVST+ proporciona una instancia independiente de IEEE 802.1w (menor tiempo de convergencia que IEEE 802.1D) por VLAN.

3.2.2.2. Enlaces troncales (ISL/IEEE 802.1Q)

El enlace troncal es un enlace punto a punto entre dos dispositivos de red que llevan el tráfico de múltiples VLANs. Cisco recomienda utilizar enlaces troncales IEEE 802.1Q. Las extensiones de Cisco al estándar IEEE 802.1Q evitan problemas de seguridad relacionados con tráfico no etiquetado (VLAN nativa), como el ataque de salto de VLAN.

Al ataque de salto de VLAN básico permite a un atacante recibir tráfico de todas las VLANs de una red haciendo pensar al *switch* que la máquina del atacante es otro *switch*, este ataque se lo puede realizar falsificando mensajes DTP o incorporando un *switch* ilegal y habilitando el enlace troncal. Existe otro tipo de ataque de salto de VLAN conocido como ataque de salto de VLAN con doble encapsulación, este ataque permite concentrarse en una VLAN específica y funciona incluso si los enlaces troncales se encuentran deshabilitados, pero solo funciona si el atacante y el puerto troncal están en la misma VLAN nativa.

Se recomienda filtrar manualmente las VLANs no utilizadas de las interfaces troncales para evitar la propagación de tramas *broadcast*, no se debe usar el filtrado de VLANs automático. Además no se debe habilitar enlaces troncales en los puertos de los usuarios, ya que los dispositivos de los usuarios no deben negociar un enlace troncal, mediante esta configuración se acelera el *Spanning Tree PortFast* (opción dentro del protocolo STP que le indica al puerto que no pase por los 4 estados del protocolo sino que directamente pase del estado "*blocking*" al estado de "*forwarding*") y es también una medida de seguridad contra el ataque de salto de VLAN.

3.2.2.3. DTP (*Dynamic Trunking Protocol*)

DTP es un protocolo propietario de Cisco que permite a los puertos negociar su método de troncalización y permite a un puerto convertirse automáticamente en troncal. La recomendación general para la configuración de DTP es configurar los extremos del enlace troncal como *desirable*, con esta configuración se tiene

la ventaja de proporcionar una indicación clara de una conexión de enlace troncal funcional con los comandos de monitoreo *show*. Como práctica recomendada (cuando se quiere usar DTP), al configurar enlaces troncales se debe definir el DTP como *desirable* - *desirable* y con encapsulación *Negotiate* para apoyar la negociación DTP.

Activando el enlace troncal en cada puerto (modo *trunk*) y con la opción *nonnegotiate* el enlace troncal se activa más rápido cuando exista una caída de servicio ya que no negocia DTP. Sin embargo, con esta configuración, DTP no supervisa activamente el estado del enlace troncal y se dificulta la identificación de un enlace troncal mal configurado. Una práctica alternativa es establecer un lado del enlace troncal (típicamente la capa de acceso) en modo *Auto* y el otro extremo (típicamente la capa de distribución) en modo *desirable*. Esta configuración permite la formación automática del enlace troncal, protege contra algunos errores de configuración y errores de *hardware*.

3.2.2.4. VTP (*VLAN Trunking Protocol*)

VTP es un protocolo propietario de Cisco que permite gestionar de forma centralizada la base de datos de las VLANs de todos los *switches* de la organización. Con VTP, al configurar una nueva VLAN en un *switch* en modo de servidor VTP, esta nueva VLAN se distribuye a través de todos los *switches* en el mismo dominio VTP, esta redistribución automática reduce la necesidad de configurar la misma VLAN en todos los *switches*. VTP sólo se ejecuta en los enlaces troncales y tiene 3 modos: servidor, cliente y transparente, como se describe en el capítulo 1.

Los *switches* de Cisco, por defecto, están configurados como servidor VTP con ningún nombre de dominio VTP ni *password* VTP especificado, debido a esto se recomienda al configurar *switches* nuevos, configurarles en modo Transparente y luego establecer el nombre del dominio VTP, con el fin de evitar sobrescribir la base de datos de VLANs de todos los *switches* de la organización. El hecho de que un *switch* Cisco sobrescriba su base de datos a

través de VTP depende totalmente del *configuration revision* y del nombre de dominio y *password* VTP como se describe a detalle en el capítulo 1.

Agregar o eliminar VLANs no es una práctica de gestión de red que se realice frecuentemente, por ende los beneficios de la propagación automática de la información de VLANs a través de la red no justifica el riesgo de un comportamiento inesperado, como una caída total de la red, debido a un error de funcionamiento. Por estas razones, el modo transparente de VTP es la opción de configuración recomendado.

3.2.2.5. EtherChannel

La tecnología *EtherChannel* permite unir enlaces *Ethernet* individuales en un único enlace lógico, de esta manera se suman los anchos de banda de cada enlace *Ethernet* (puede unir hasta ocho enlaces físicos).

EtherChannel también proporciona una optimización de STP al permitir que todos los puertos miembros del enlace *EtherChannel* se configuren en el modo de reenvío, esto se debe a que STP ve a un enlace *EtherChannel* como un único enlace lógico y su costo por defecto dentro de STP es 27. El protocolo STP utiliza el costo para elegir la mejor ruta, entre varias rutas posibles, desde los *switches* que no son *route bridge* hasta el *switch route bridge*, entre menor sea la suma de costos mejor será la ruta.

Existen dos variantes para el mecanismo de control de *EtherChannel* (no interactúan entre ellos): la norma previa de Cisco que utiliza *Port Aggregation Protocol* (PAgP) y la basada en el estándar IEEE 802.3ad que utiliza Link *Aggregation Control Protocol* (LACP).

Existen tres modos diferentes de configuración para PAgP: *auto* (negociación pasiva en el enlace *EtherChannel*), *desirable* (negociación activa en el enlace *EtherChannel*) y *on* (ningún protocolo es usado, el *switch* asume que el otro lado está habilitado para agregación de enlaces). Para *EtherChannels* de capa 2, se recomienda una configuración PAgP *desirable* - *desirable*, de esta manera el protocolo PAgP se ejecuta a través de todos los miembros del

enlace *EtherChannel*, lo que garantiza que si un miembro falla no provoque una falla a nivel de STP.

Existen dos modos de configurar para LACP: *active* (habilita el protocolo LACP incondicionalmente) y *passive* (habilita LACP solo si detecta LACP en el dispositivo). La práctica recomendada para *EtherChannel* usando LACP es establecer un lado del enlace *EtherChannel* en *active* y la otra en *passive*, o ambos lados del enlace *EtherChannel* en *active*.

3.2.3. Diseño a nivel de capa tres (modelo OSI)

Un buen diseño de red siempre debe contemplar alta disponibilidad y una convergencia rápida. Para lograr estos dos objetivos se deben analizar las siguientes áreas: gestión de *oversubscription* y ancho de banda, balanceo de carga y redundancia a nivel de puerta de enlace predeterminada.

3.2.3.1. Gestión de *oversubscription* y ancho de banda

Las redes de campus típicamente están implementadas con exceso de suscripción (*oversubscription*). *Oversubscription* es el hecho de asumir que todos los dispositivos de la red no van a transmitir a su máxima velocidad al mismo tiempo, por ende la infraestructura de red no tiene la capacidad de manejar todo este tráfico. Con exceso de suscripción se ahorra dinero pero se tiene el riesgo de congestión, cuellos de botella y deficiencia en la transmisión de información si se tiene picos de uso. Se debe considerar dónde y en qué relación hacer un exceso de suscripción dentro de la red ya que un mal diseño de esta práctica conlleva a los problemas descritos anteriormente.

La recomendación empírica para exceso de suscripción de transmisión de datos es de 20:1 para los enlaces desde la capa de acceso a la capa de distribución. La recomendación es de 4:1 para los enlaces de la capa de distribución hasta la capa núcleo. La siguiente figura ilustra una imagen del típico exceso de subscripción.

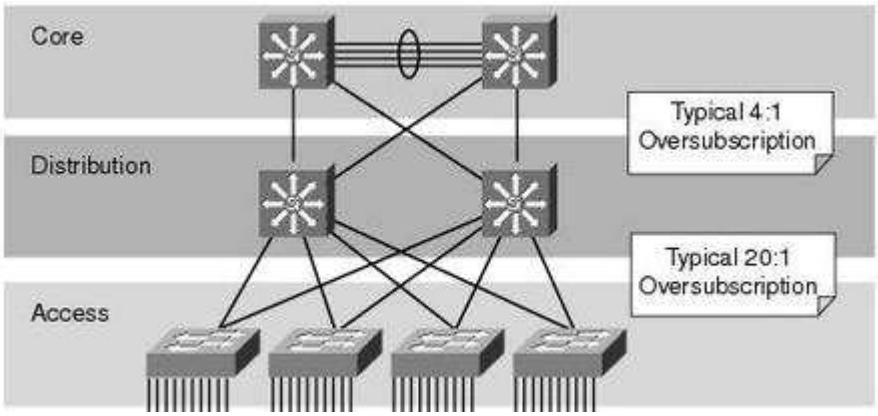


Figura 55. "Oversubscription" típica recomendada

Tomada de http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSDesign.html#wp998242

Como las nuevas aplicaciones y servicios requieren más ancho de banda y para que la sensación de que existe un buen servicio para el usuario final, se necesita manejar mayor ancho de banda entre las distintas capas. Una solución es aumentar el ancho de banda de los enlaces troncales, es decir aumentando la capacidad del medio de transmisión, esto implica costos, ya que se necesita cambiar el *backbone* (cableado vertical).

Si tenemos más enlaces disponibles en nuestro *backbone* y los conectamos, por el protocolo STP solo un enlace troncal entre esos dos *switches* estará activo, por lo que el hecho de conectar más enlaces troncales entre dos *switches* solo sirve para redundancia y no para aumentar ancho de banda entre las capas.

La tecnología *EtherChannel* permite agregar ancho de banda entre las capas mediante la creación de una sola interfaz lógica que agrupa a varios enlaces, por lo que el uso de esta tecnología es recomendado dentro del diseño para gestionar ancho de banda entre las distintas capas y nos permite modificar la relación de exceso de suscripción en nuestra red.

3.2.3.2. Balanceo de carga

En redes redundantes cuando existen caminos del mismo costo entre *switches* de acceso, debe existir una forma de balancear la carga entre estos caminos

del mismo costo. Cisco tiene un algoritmo determinístico llamado CEF (*Cisco Express Forwarding*).

La decisión de enviar tráfico por un enlace u otro depende del valor de ingreso para el cálculo de CEF, cuando todos los *switches* usan el valor de ingreso por defecto (direcciones destino y origen a nivel de capa 3) algunos enlaces redundantes no son usados (polarización CEF). Para evitar este inconveniente se modifica el valor de ingreso para el cálculo de CEF en las capas del modelo jerárquico. Se recomienda en la capa núcleo usar el valor por defecto (basado en información a nivel de capa 3) y a nivel de la capa de distribución usar la información a nivel de capa 3 y la información de capa 4. Con esto se logra que no existan enlaces redundantes sin uso.

La tecnología *EtherChannel* permite balanceo de carga entre los enlaces que conforman el *EtherChannel* en caso de que un enlace falle. Se puede modificar el algoritmo que se usa para seleccionar el enlace que conforma el *EtherChannel* por el cual el paquete se va a transmitir. Por defecto se usa información a nivel de capa 3 para el balanceo de carga dentro de un *EtherChannel* pero se puede usar información a nivel de capa 4 también como información de ingreso para el algoritmo.

La siguiente figura muestra los resultados de experimentos en los laboratorios de Cisco usando un esquema de una red por VLAN, dos VLANs por *switch* y usando direccionamiento privado (RFC 1918). Por defecto, usando información de capa 3, el algoritmo da una relación de un tercio a dos tercios de utilización por enlace, cuando se usa información a nivel de capa 4 la utilización por enlace es casi la misma en cada enlace con la misma topología y patrón de tráfico.

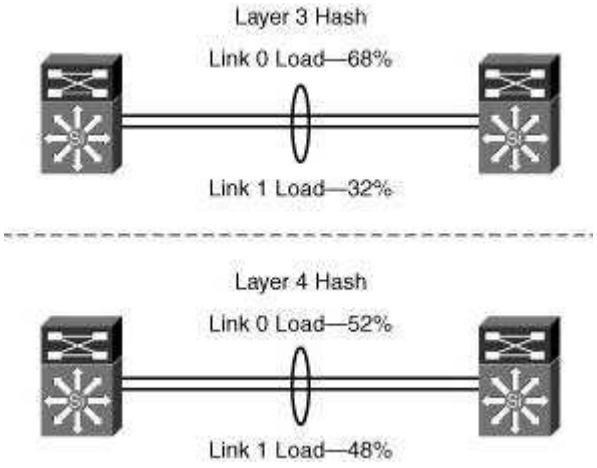


Figura 56. Balanceo de carga en un enlace EtherChannel

Tomada de http://www.ciscopress.com/articles/article.asp?p=1315434&seqNum=3

Se recomienda usar información a nivel de capa 3 y capa 4 para que el algoritmo de *EtherChannel* logre una utilización uniforme de los miembros del *EtherChannel*. Además se recomienda usar dos, cuatro u ocho puertos en cada enlace *EtherChannel* para alcanzar el mejor balanceo de carga.

3.2.3.3. Redundancia a nivel de puerta de enlace predeterminada

Es importante dentro del diseño de redes empresariales incluir redundancia a nivel de puerta de enlace predeterminada. Como lo indica su nombre la redundancia a nivel de puerta de enlace predeterminada permite mantener conectividad desde los usuarios finales hasta el equipo que maneje el *default gateway* en caso de una falla de este equipo. Existen algunos protocolos creados para permitir redundancia a nivel de puerta de enlace predeterminada como: HSRP (*Hot Stanby Routing Protocol*), VRRP (*Virtual Router Redundancy Protocol*) y otros que permiten además de redundancia balanceo de carga como GLBP (*Gateway Load Balancing Protocol*).

Dentro de infraestructuras de red implementadas con equipos Cisco se usa HSRP (*desarrollado por Cisco Systems*) y no VRRP (desarrollado por la Internet *Engineering Task Force)* debido a que HSRP, además se der un

protocolo propietario de Cisco, permite un despliegue rápido de nuevas características y funcionalidades con respecto a VRRP, aunque cabe recalcar que ambos protocolos proveen un método robusto de redundancia a nivel de *default gateway*. Por lo general se usa VRRP cuando se necesita redundancia con equipos de otros fabricantes.

Cabe recalcar que HSRP y VRRP son protocolos que se despliegan en un modelo activo-pasivo es decir, un miembro dentro del despliegue no trabaja y solo espera a que el equipo principal falle. Esta solución implica pérdida de dinero y eficiencia ya que un equipo que funciona perfectamente la mayor parte del tiempo no está en funcionamiento.

GLBP es un protocolo diseñado por Cisco que permite balancear el tráfico entre grupos de equipos, que trabajen a nivel de capa 3, redundantes. Este protocolo permite redundancia a nivel de *default gateway*, balanceo de carga y permite que los dos equipos que realizan *routing* trabajen al mismo tiempo.

Existe una tecnología de virtualización de sistemas de red, propietaria de Cisco, que permite combinar varios *switches* Cisco (de gama alta) en un único *switch* virtual, conocida como VSS (*Virtual Switching System*). Usando esta tecnología se tienen grandes ventajas respecto a usar protocolos de redundancia a nivel de puerta de enlace predeterminada, a continuación se mencionan algunas.

i. Incrementa la eficiencia operacional simplificando la infraestructura de red reduciendo la carga de administración. Podemos afirmar que reduce la carga de administración ya que ahora existe una única IP de administración y un solo archivo de configuración en lugar de configurar todos los equipos redundantes con las mismas políticas.
ii. Reduce a una sola dirección IP como *default gateway* por VLAN en lugar de 3 como se usan con los protocolos de redundancia a nivel de puerta de enlace predeterminada y ya no se necesita usar HSRP, VRRP o GLBP.

iii. Mediante la tecnología MEC (*Multichassis EtherChannel*) se logra configurar topologías redundantes sin las limitaciones de diseño del protocolo STP, además logra flexibilidad en el despliegue ya que permite una distancia de hasta 40 km entre cada *switch* que conforma el VSS.

iv. Los dos *switches* miembros del VSS tienen activo al mismo tiempo el plano de datos, es decir los dos conmutan y realizan *routing* al mismo tiempo.

La siguiente imagen ilustra el despliegue con protocolos de redundancia a nivel de puerta de enlace predeterminada y otra con VSS, en la figura con tecnologías tradicionales se puede apreciar como uno de los dos enlaces redundantes están bloqueados hacia los *switches* de núcleo/distribución mientras que con VSS los dos están activos al mismo tiempo.

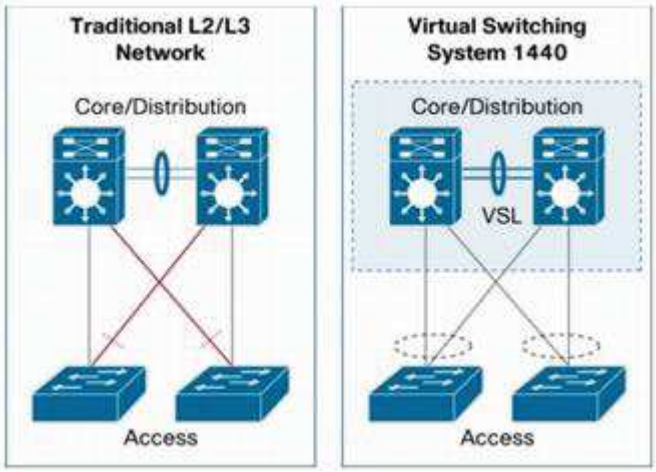


Figura 57. VSS vs. Redes tradicionales

Tomado de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-virtual-switching-system-1440/prod_qas0900aecd806ed74b.html

3.3. Diseño de la nueva red conmutada

El diseño que se presentará a continuación es el teórico ideal que permite escalabilidad y alta disponibilidad (redundancia) y se implementará en dos fases, la primera fase no involucra redundancia (por temas de presupuesto) y

es la que se implementa en este proyecto, la fase dos involucra redundancia y ésta se realizará en un futuro proyecto.

Basados en los lineamientos principales de la sección anterior y tomando como referencia los pliegos presentados en el proyecto “ADQUISICIÓN E INSTALACIÓN DE EQUIPOS DE CONMUTACIÓN PARA OPERAR Y BRINDAR LA CONECTIVIDAD EN LA RED DEL NUEVO AEROPUERTO Y MATRIZ DE QUITO” por parte de la empresa pública TAME Línea Aérea del Ecuador "TAME EP", se diseñará (para la fase uno y dos) una red conmutada con topología en estrella con redundancia a nivel de *switch* de núcleo y enlaces de *backbone*, donde el centro de esta topología será un *switch* que permita *routing* (capa 3 del modelo OSI) que se ubicará en el cuarto de telecomunicaciones y los distintos nodos serán *switches* de capa dos que se ubicarán en los *racks* de pared de cada piso.

Ya que la empresa se puede considerar como un módulo de campus pequeño (dentro de la clasificación Cisco), se fusionará la capa núcleo con la capa distribución, esta fusión se conoce como *collapsed core* o núcleo colapsado, además por la distribución física y el espacio de los *racks* de piso no se podría colocar *switches* extras dentro de los mismos que cumplan con funciones de la capa de distribución. Por estas razones el *switch* de núcleo colapsado será el encargado de cumplir con las funciones de las dos capas (núcleo y distribución). Mientras que los *switches* ubicados en los *racks* de piso cumplirán únicamente las funciones de la capa de acceso.

Como ya se describió en el capítulo dos existen en algunos pisos conexiones en cascada (conexión directa entre un *switch* de acceso y el siguiente) lo que implica un grave punto de falla, además de un menor rendimiento en la tasa de transferencia. Con el diseño de topología en estrella se elimina este punto de falla.

También del levantamiento de información cuyas observaciones se describen en el capítulo dos, la densidad de puertos está prácticamente agotada en todos los pisos, especialmente en los pisos (4, 5, 6 y 7) por lo que se agregará un

switch de 24 puertos en estos pisos para solventar esta falencia, además al estar la densidad de puertos prácticamente agotada no existía capacidad de crecimiento, este punto también se solventa con la agregación de *switches* de acceso en estos pisos.

La empresa pública TAME en su edificio Matriz tiene 9 pisos, en base al levantamiento de información se colocarán *switches* de 24 y 48 puertos por cada piso de acuerdo a la siguiente tabla.

Tabla 7. *Switche*s por piso edificio Matriz (Diseño fase uno y fase dos)

***SWITCHES* POR PISO EDIFICIO MATRIZ (Diseño fase uno y dos)**		
PISO	**DESCRIPCIÓN (CAPA DEL MODELO OSI Y CANTIDAD DE PUERTOS)**	**CAPA MODELO JERÁRQUICO CISCO**
Piso 1	*Switch* de núcleo principal con funciones de capa 3 del modelo OSI (L3) de más de 48 puertos	Núcleo y Distribución
	Switch de núcleo principal con funciones de capa 3 del modelo OSI (L3) de más de 48 puertos	Núcleo y Distribución
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 2	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 4	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 5	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
Piso 6	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 7	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
Piso 8	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 9	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso

La siguiente imagen muestra el diseño completo (fase uno y dos) simulado en el *software* Cisco *Packet Tracer*, recalcando que no se puede simular la tecnología VSS en este *software*.

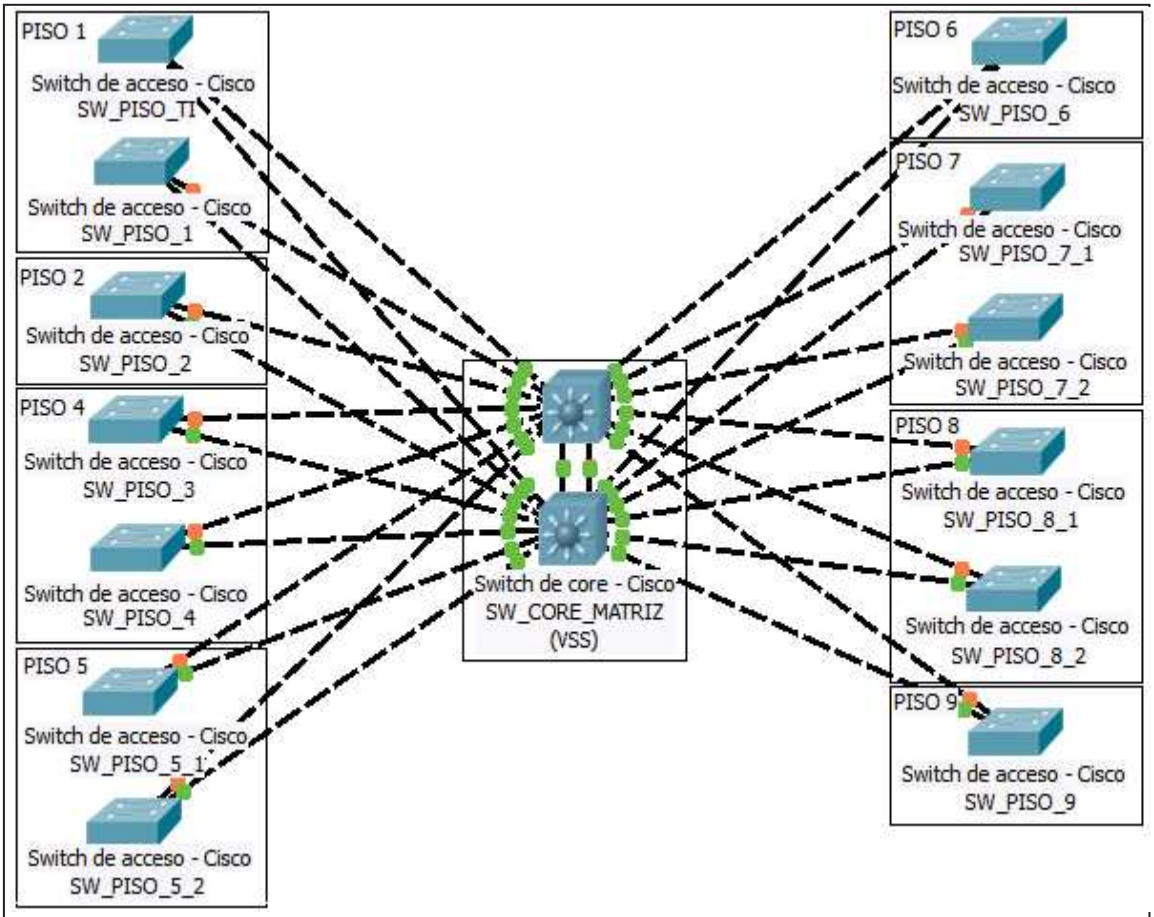


Figura 58. Diseño completo (fase uno y fase dos) simulado en Cisco *Packet Tracer*

La siguiente figura ilustra el diseño completo (fase uno y dos) de la nueva red conmutada a nivel del modelo jerárquico de Cisco y la ubicación de cada *switch* dentro del edificio Matriz (por piso).

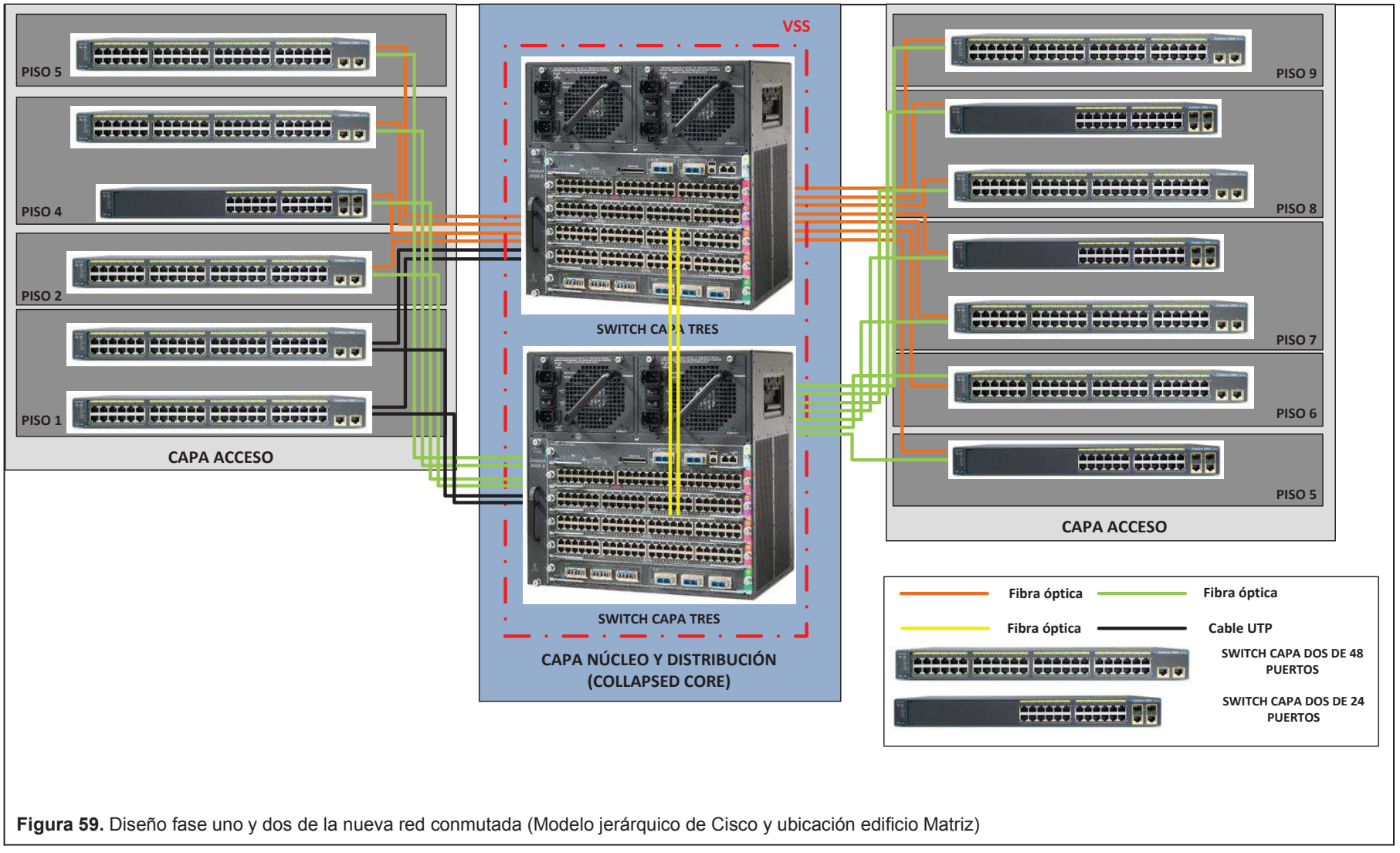


Figura 59. Diseño fase uno y dos de la nueva red conmutada (Modelo jerárquico de Cisco y ubicación edificio Matriz)

Mediante este diseño se cumplen con algunos de los lineamientos principales para el diseño de las redes conmutadas descritos en la sección anterior, además se toma en cuenta el factor capacidad de crecimiento al proveer una holgura en la densidad de puertos usados.

Se diseñó una topología con alta disponibilidad (redundancia) con dos *switches* de núcleo colapsado en VSS (*Virtual Switching System*) con enlaces redundantes *EtherChannels* (usando dos enlaces de fibra óptica) contra cada *switch* de acceso. La tecnología MEC permite establecer una interfaz *EtherChannel* usando puertos de ambos *switches* miembros del VSS, de esta manera se puede establecer una topología con redundancia sin tener varios caminos que puedan causar un lazo a nivel de capa dos.

Cabe recalcar que debido a que los dos *switches* de acceso que brindarán conectividad para el piso 1 se ubicarán en el mismo *rack* que el *switch* de núcleo colapsado, el medio de trasmisión a usarse será cable UTP.

A nivel de capa dos, a pesar que en la topología no existen enlaces redundantes que puedan causar lazos, el protocolo STP va a estar activo, usando el protocolo PVST+ que viene activo por defecto en los *switches* Cisco. Los enlaces troncales serán desplegados con el estándar IEEE 802.1Q y el protocolo DTP va a estar desactivado ya que se configurará manualmente cada puerto en troncal tanto en el *switch* de núcleo colapsado como en los *switches* de acceso. Se configurará el *switch* de núcleo colapsado como servidor VTP y los *switches* de acceso en modo cliente, obviamente tanto los *switches* de acceso como el núcleo colapsado tendrán el mismo *password* y dominio VTP.

A nivel de capa tres en cuanto a exceso de suscripción se tendrá una relación de 2,4:1 entre la capa de acceso y la capa de núcleo colapsado. No se tendrá redundancia a nivel de puerta de enlace predeterminada ni tampoco balanceo de carga con protocolos como HSRP o VRRP, estas características se solventan con la tecnología VSS. Como ya se mencionó anteriormente este diseño no se implementará en este proyecto pero servirá como alistamiento para el diseño e implementación de la fase dos.

En cuanto al diseño para la fase uno no se tomará en cuenta el parámetro de redundancia, pero se mantendrá absolutamente todo el resto del diseño, tanto a nivel de capa dos como de capa tres. Ya que no existirán enlaces redundantes desde los *switches* de acceso hasta el *switch* de núcleo colapsado el exceso de suscripción tendrá una relación de 4,8:1.

Para el diseño de la fase uno, en base al levantamiento de información se colocarán *switches* de 24 y 48 puertos por cada piso de acuerdo a la siguiente tabla 8.

Tabla 8. *Switches* por piso edificio Matriz (Diseño fase uno)

***SWITCHES* POR PISO EDIFICIO MATRIZ (Diseño fase uno)**		
PISO	**DESCRIPCIÓN (CAPA DEL MODELO OSI Y CANTIDAD DE PUERTOS)**	**CAPA MODELO JERÁRQUICO CISCO**
Piso 1	*Switch* de core principal con funciones de capa 3 del modelo OSI (L3) de más de 48 puertos	Núcleo y Distribución
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 2	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 4	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 5	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
Piso 6	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 7	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
Piso 8	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 24 puertos	Acceso
	Switch de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso
Piso 9	*Switch* de acceso con funciones de capa 2 del modelo OSI (L2) de 48 puertos	Acceso

La siguiente imagen muestra el diseño de la fase uno simulado en el *software* Cisco *Packet Tracer*.

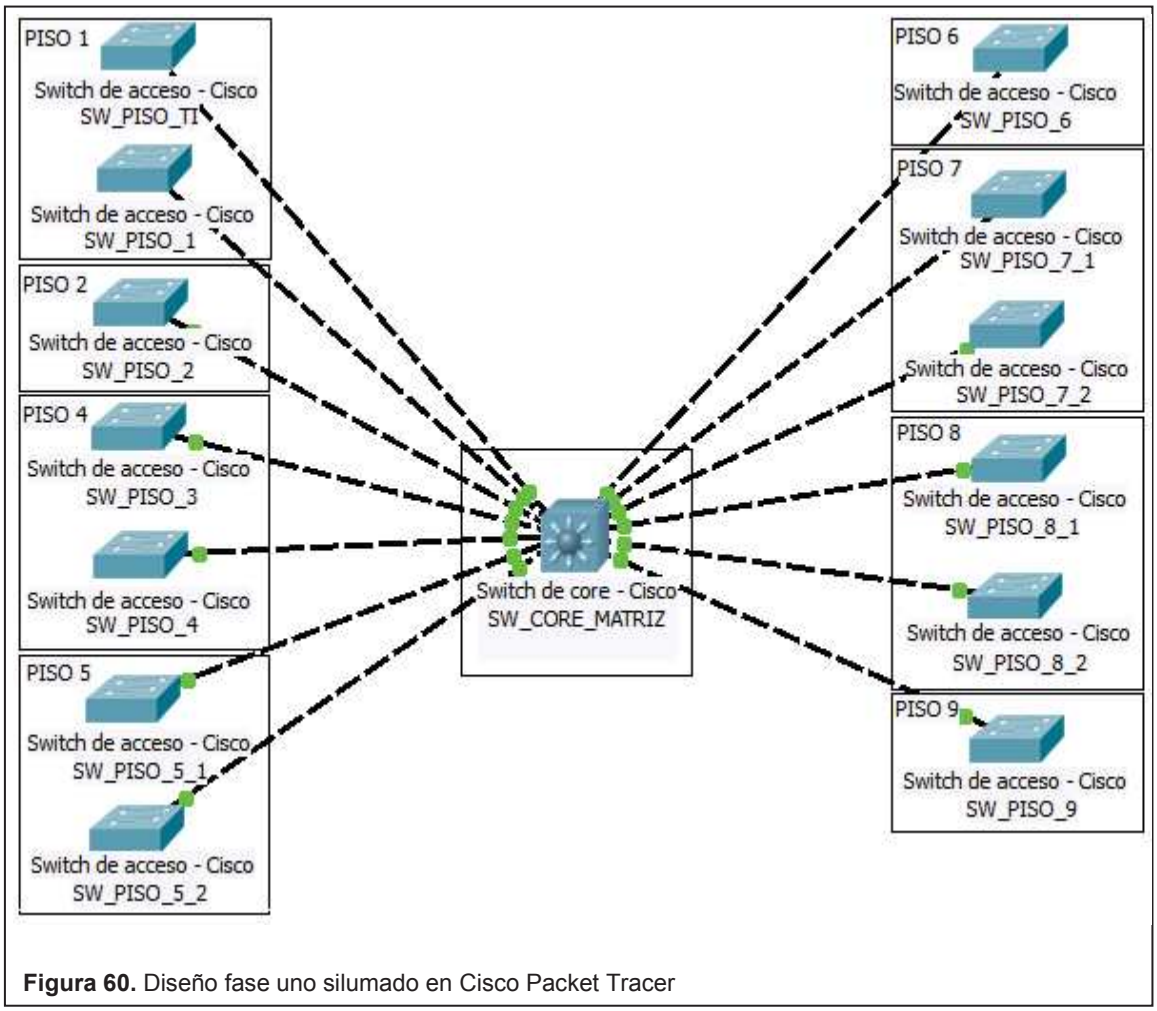


Figura 60. Diseño fase uno silumado en Cisco Packet Tracer

La siguiente figura ilustra el diseño de la fase uno de la nueva red conmutada a nivel del modelo jerárquico de Cisco y la ubicación de cada *switch* dentro del edificio Matriz (por piso).

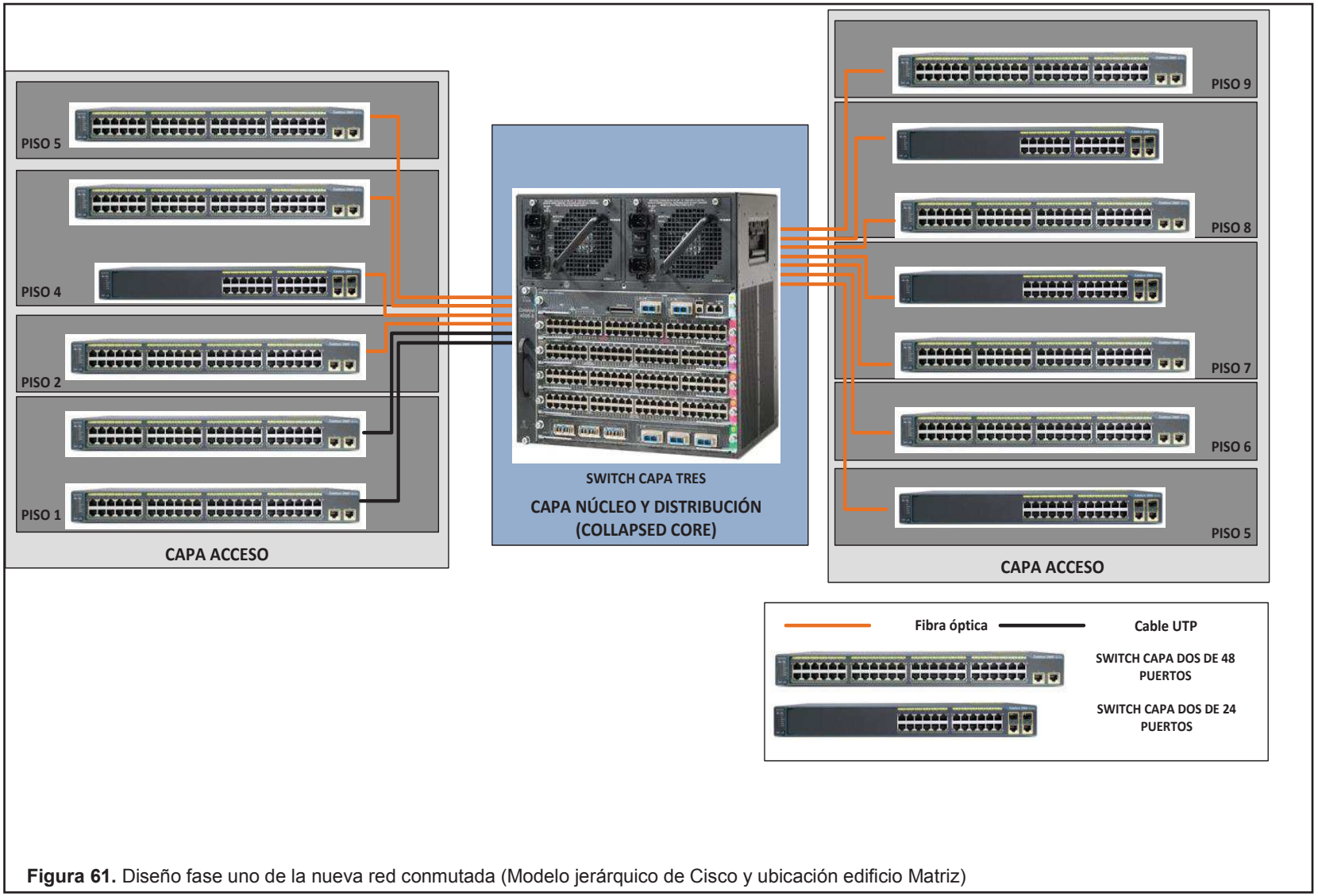


Figura 61. Diseño fase uno de la nueva red conmutada (Modelo jerárquico de Cisco y ubicación edificio Matriz)

3.4. Elementos necesarios para la nueva red conmutada

Los elementos necesarios para el diseño de la nueva red conmutada se pueden clasificar en medios de transmisión y equipos de *networking*.

3.4.1. Medios de transmisión

En esta área se definirá los distintos medios de transmisión que se necesitan para el diseño propuesto y se especificará cuáles serán implementados y cuáles no.

3.4.1.1. Subsistema vertical

Como ya se describió en el anterior capítulo la red cuenta con un *backbone* de fibra óptica obsoleto, el cual no llega a todos los pisos donde se encuentran *racks* de piso y no tiene hilos libres para la conexión de nuevos *switches*, por lo que en la nueva red de información es imprescindible cambiar de *backbone*.

El cambio de este *backbone* responde principalmente al diseño de una topología en estrella donde cada *switch* de acceso se conecta directamente al *switch* de núcleo colapsado y se elimina la mala práctica de conectar *switches* en cascada.

El nuevo *backbone* tendrá 22 hilos, será de fibra óptica multimodo a 1 Gbps, y conectará el *switch* de núcleo colapsado con cada *switch* de acceso en cada *rack* de piso para que se pueda configurar la topología en estrella, además con 22 hilos se configura el alistamiento para completar la fase 2 del proyecto en un futuro.

La conexión entre el *switch* de núcleo colapsado y los *switches* de acceso del piso 1 será a través de *patch cords* UTP.

3.4.1.2. Subsistema horizontal y Área de usuario

Estas dos áreas salen del alcance del presente proyecto por lo cual no habrá ningún cambio en estas áreas.

3.4.2. Equipos de *networking*

Los nuevos equipos de *networking* de capa dos y capa tres que se dimensionarán serán equipos de última generación, deberán asegurar capacidad de crecimiento, además deben tener las interfaces necesarias para configurar la topología en estrella antes diseñada usando como medio de transmisión para el *backbone* fibra óptica y que sean de la marca Cisco Systems. Los equipos de *networking* deben ser de esta marca por las siguientes razones:

- La tecnología VSS que nos permitirá configurar redundancia a nivel de *switches* de núcleo colapsado presenta grandes ventajas respecto a protocolos de redundancia como HSRP o GLBP, esta tecnología es propietaria de Cisco.
- Para un despliegue IBNS los equipos autenticadores deben soportar los VSA (*Vendor Specific Attribute*) de Cisco. Mediante los VSA un vendedor (fabricante) puede configurar sus propios atributos RADIUS que no están incluidos en las RFC 2865 y 2866. Uno de estos atributos propios de Cisco es el CoA (*Change of Authorization*) que permite cambiar el perfil de autorización que se le asigna a un usuario final, gracias a este atributo se puede configurar una de las grandes características de IBNS como es la movilidad. El VSA CoA no es soportado por otras marcas que también proveen soluciones de control de acceso a la red.

Tomando en cuenta el diseño antes descrito el *switch* de núcleo colapsado deberá trabajar tanto en la capa dos como en la capa tres del modelo OSI, mientras que los *switches* de acceso solo en la capa dos. Estos equipos de *networking* deben presentar mayores características que los equipos que van a reemplazar. La siguiente tabla muestra los equipos que se dimensionarán de acuerdo a la capa del modelo jerárquico de Cisco.

Tabla 9. Dimensionamiento de los equipos de *networking* de acuerdo al modelo jerárquico de Cisco

DIMENSIONAMIENTO DE LOS EQUIPOS DE *NETWORKING* DE ACUERDO AL MODELO JERÁRQUICO DE CISCO			
CAPA DEL MODELO JERÁRQUICO DE CISCO	**MODELO DEL EQUIPO**	**CARACTERÍSTICAS MÍNIMAS**	**CARACTERÍSTICAS DE CADA EQUIPO**
Núcleo colapsado	WS-C4506-E	Debe soportar VSS: Supervisor Engine 7-E o 7L-E Mínimo Cisco IOS XE 3.4.0SG Mínimo ROMMON IOS 15.0 (1r) SG7 Licencia IPBase	Soporta VSS: Supervisor Engine 7L-E Software tanto IOS como ROMMON son actualizables Licencia IPBase
		Debe soportar: VTP, PVST+, EtherChannel y que trabaje a nivel de la capa 3 del modelo OSI	Soporta: VTP, PVST+, EtherChannel y trabaja a nivel de la capa 3 del modelo OSI
		Mínima capacidad de *switch*ing centralizada: 520Gbps Mínima capacidad de *switching* (backplane) por slot: 48Gbps Mínimo throughtput: 225 Mpps IPv4 / 110 Mpps IPv6	Capacidad de *switching* centralizada: 520Gbps Capacidad de *switching* (backplane) por slot: 48Gbps Throughtput: 225 Mpps (IPv4) / 110 Mpps (IPv6)
Acceso	WS-C2960S-48FPD-L	Mínimo ancho de banda del sistema: 176 Gbps Mínimo ancho de banda de reenvío (*switching*): 88 Gbps Mínima tasa de reenvío: 101.2 Mpps Mínima potencia PoE disponible: 740W Debe soportar IEEE 802.3at (Mínimo 24 puertos) Debe soportar: VTP, PVST+ y EtherChannel	Ancho de banda del sistema: 176 Gbps Ancho de banda de reenvío (*switching*): 88 Gbps Tasa de reenvío: 101.2 Mpps Potencia PoE disponible: 740W Soportar 24 puertos con el estándar IEEE 802.3at Soporta: VTP, PVST+ y EtherChannel
	WS-C2960S-48FPS-L	Mínimo ancho de banda del sistema: 176 Gbps Mínimo ancho de banda de reenvío	Ancho de banda del sistema: 176 Gbps Ancho de banda de reenvío (*switching*): 88 Gbps

		(*switching*): 88 Gbps Mínima tasa de reenvío: 77.4 Mpps Mínima potencia PoE disponible: 740W Debe soportar IEEE 802.3at (Mínimo 24 puertos) Debe soportar: VTP, PVST+ y EtherChannel	Tasa de reenvío: 77.4 Mpps Potencia PoE disponible: 740W Soporta 24 puertos con el estándar IEEE 802.3at Soporta: VTP, PVST+ y EtherChannel
	WS-C2960S-24PD-L	Mínimo ancho de banda del sistema: 176 Gbps Mínimo ancho de banda de reenvío (*switching*): 88 Gbps Mínima tasa de reenvío: 65.5 Mpps Mínima potencia PoE disponible: 370W Debe soportar IEEE 802.3at (Mínimo 12 puertos) Debe soportar: VTP, PVST+ y EtherChannel	Ancho de banda del sistema: 176 Gbps Ancho de banda de reenvío (*switching*): 88 Gbps Tasa de reenvío: 65.5 Mpps Potencia PoE disponible: 370W Soporta 12 puertos con el estándar IEEE 802.3at Soporta: VTP, PVST+ y EtherChannel
	WS-C2960S-24PS-L	Mínimo ancho de banda del sistema: 176 Gbps Mínimo ancho de banda de reenvío (*switching*): 88 Gbps Mínima tasa de reenvío: 41.7 Mpps Mínima potencia PoE disponible: 370W Debe soportar IEEE 802.3at (Mínimo 12 puertos) Debe soportar: VTP, PVST+ y EtherChannel	Ancho de banda del sistema: 176 Gbps Ancho de banda de reenvío (*switching*): 88 Gbps Tasa de reenvío: 41.7 Mpps Potencia PoE disponible: 370W Soporta 12 puertos con el estándar IEEE 802.3at Soporta: VTP, PVST+ y EtherChannel

La siguiente figura muestra una comparación en cuanto a las características de los *switches* dimensionados comparados contra los *switches* que se van a reemplazar en la capa de núcleo colapsado.

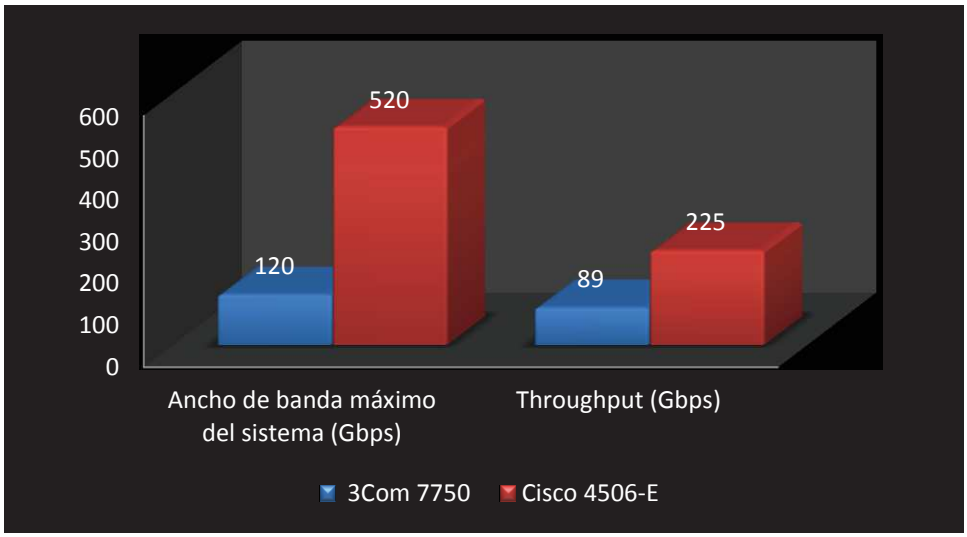


Figura 62. Ancho de banda y throughput *switches* actuales vs *switches* dimensionados (capa de núcleo colapsado)

La siguiente figura muestra una comparación en cuanto a las características de los *switches* dimensionados comparados contra los *switches* que se van a reemplazar en la capa de acceso.

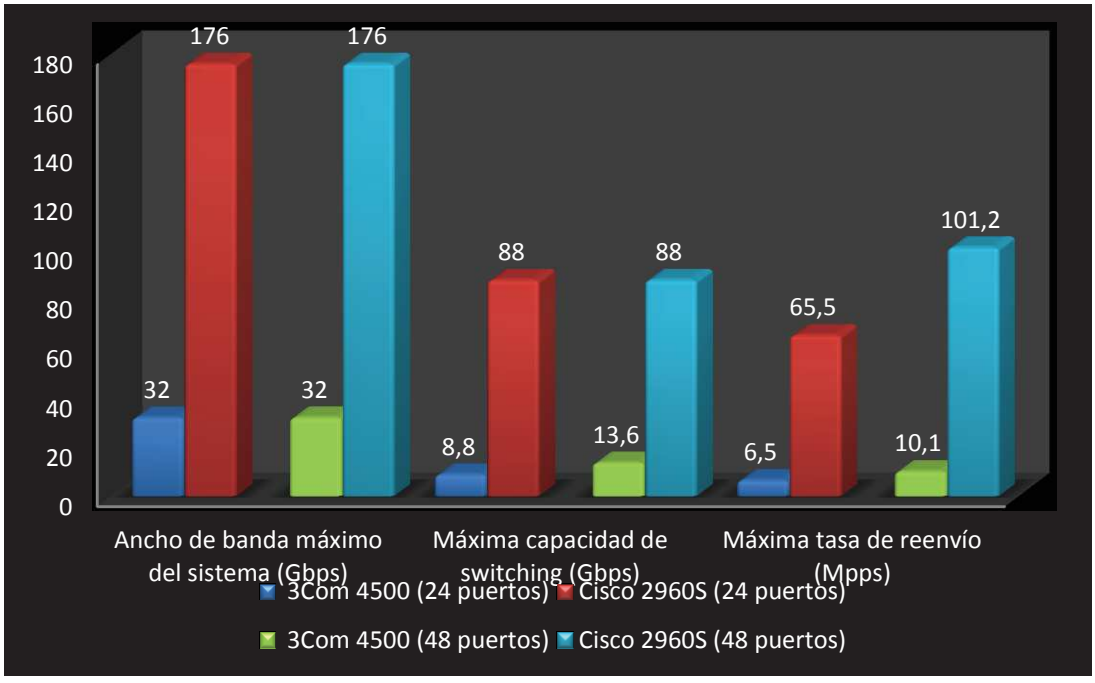


Figura 63. Características *switches* actuales vs *switches* dimensionados (capa de acceso)

Como se puede observar en las figuras 62 y 63 las características de los equipos dimensionados son mucho mayores que los actuales equipos por lo que la nueva red conmutada tendrá un mayor rendimiento que la actual red.

3.5. Antecedentes del control de acceso a la red

Los contratistas, clientes potenciales, invitados y consultores necesitan tener acceso a los recursos, servicios y aplicaciones de la infraestructura de red a través de las mismas conexiones que los empleados; es por eso que la posibilidad de que personas no autorizadas (atacantes y/o usuarios maliciosos) tengan acceso a información crítica de la empresa aumenta. Uno de los puntos más vulnerables de la infraestructura de red es el acceso en donde los usuarios finales se conectan a la red. Antes se usaba otros tipo de seguridad como la seguridad física para proteger las áreas donde se podía tener acceso a la red o simplemente no se daba acceso a ninguna persona ajena a la empresa a la red, pero en la actualidad las salas de conferencias, recepción, aulas de capacitación ofrecen acceso a la red a través de puntos de red en la pared (red cableada) y en todo el edificio a través de la red inalámbrica.

Una vez conectado a la red, los empleados, contratistas, consultores, clientes, invitados, atacantes y usuarios maliciosos tienen acceso a todos los recursos de la red (servicios, aplicaciones) y lo más crítico a la información confidencial de la empresa.

Para proteger la posible pérdida de información sensible de la organización se necesita implementar control de acceso a la red dentro de la infraestructura de red. Los nuevos diseños de red deben incluir control de acceso a la red desde su inicio, ya que la implementación de controles de acceso basados en roles (identidad) para los usuarios y/o dispositivos ayudan a reducir la pérdida potencial de información sensible permitiendo a las organizaciones verificar la identidad de un usuario o dispositivos, el nivel de privilegio y el cumplimiento de políticas de seguridad antes de conceder el acceso a la red.

El cumplimiento de las políticas de seguridad consiste en exigir antivirus, actualizaciones del sistema operativo o parches en los dispositivos que se quieran conectar a la infraestructura de red. Los dispositivos no autorizados o que no cumplan con las políticas de seguridad de la empresa serán colocados en un área de cuarentena donde se hará la remediación antes de tener acceso a la red o simplemente estos dispositivos no podrán ingresar a la red. Cisco utiliza las siguientes soluciones para el control de acceso a la red:

i. Servicio de red basado en identidad (IBNS)
ii. Servicio de control de acceso a la red (NAC)
iii. Motor de servicio de identidad (ISE)

IBNS es una solución creada para permitir al usuario final y a los dispositivos finales acceso seguro a la infraestructura de red tanto para la red cableada como para la red inalámbrica. Proporciona control de acceso a la red basado en estándares como por ejemplo el protocolo IEEE 802.1X, usando autenticación específica mediante direcciones MAC y mediante verificación de credenciales.

NAC es un servicio que utiliza la infraestructura de red existente para hacer cumplir la política de seguridad de la organización en todos los dispositivos que tratan de acceder a la red, tanto en la red cableada como la inalámbrica.

Existe una plataforma que permite combinar las principales características de ambas soluciones descritas anteriormente en una sola implementación, es decir permite control de acceso a la red basado en identidad (IBNS) usando IEEE 802.1X, *MAC-Authentication Bypass* (MAB) y *Web-Authentication*, y además permite autenticar, autorizar y remediar usuarios (cableados, inalámbricos, remotos) y sus dispositivos antes de que puedan acceder a la red (NAC) para cumplir con la política de seguridad de la organización (en cuanto a la red interna se refiere). Esta plataforma se conoce como *Cisco Identity Service Engine* (ISE).

3.6. Lineamientos principales para el diseño del servicio de red basado en identidad (IBNS)

IBNS es una plataforma que permite acceso seguro a la red basados en la identidad y el estado de autenticación de todos los usuarios (usuarios corporativos, proveedores, visitantes, dispositivos periféricos, entre otros) que conforman la red.

IBNS utiliza el estándar IEEE 802.1X, este protocolo tiene la capacidad de permitir o denegar la conectividad de red, a nivel de capa dos, en función de la identidad del usuario o el dispositivo. Cabe recalcar que la solución IBNS permite un control de acceso a la red para los dispositivos que no soportan IEEE 802.1X, a través de *MAC-Authentication Bypass* (MAB) y acceso basado en las credenciales del usuario a través de *Web-Authentication*. Esta solución comprende varios productos de Cisco que ofrecen control de acceso basado en identidad para garantizar la conectividad y el acceso seguro a los recursos de red, además IBNS ayuda a las empresas a gestionar mejor la movilidad de los empleados y a reducir los gastos que abarcan la seguridad del acceso a la red, mediante una solución global de acceso seguro a la red.

3.6.1. Consideraciones de diseño

IBNS proporciona acceso personalizado a la red basado en la identidad del usuario o del dispositivo. Las siguientes secciones señalan algunas consideraciones que se deben tener en cuenta para la implementación de una solución IBNS que se adapte a la infraestructura de red existente.

3.6.1.1. Categorías de usuario y dispositivos

El primer paso del diseño IBNS es identificar quién tendrá acceso a la red, es decir definir las categorías de usuarios y dispositivos que se conectarán a la red y qué tipo de acceso obtendrá (nivel de acceso). Para las implementaciones iniciales, se sugiere utilizar categorías amplias para los usuarios y dispositivos, cuanto más simple sea la política, más fácil y efectiva será la implementación inicial.

Cuando el control de acceso básico a la red se ha desplegado con éxito, se pueden implementar grupos y políticas más granulares. Una vez que se definan las categorías de usuarios y dispositivos de la red se debe asignar cada categoría a un nivel de acceso a la red. Cisco sugiere referirse a la siguiente tabla para despliegues iniciales.

Tabla 10. Niveles de acceso de acuerdo a la categoría del usuario y dispositivo para despliegues iniciales según Cisco

NIVELES DE ACCESO DE ACUERDO A LA CATEGORÍA DEL USUARIO Y DISPOSITIVO PARA DESPLIEGUES INICIALES	
CATEGORÍA	**NIVEL DE ACCESO A LA RED**
Empleado	Acceso completo (Intranet e Internet)
Dispositivos conocidos	Acceso completo (Intranet e Internet)
Dispositivos desconocidos	Solo servicios de conectividad (DHCP, DNS, TFTP)
Pre-autenticación	Solo servicios de conectividad (DHCP, DNS, TFTP)
Autenticación fallida	Solo servicios de conectividad (DHCP, DNS, TFTP)

La categoría de pre-autenticación se refiere al nivel de acceso que un usuario o dispositivo recibirá antes de que su identidad sea determinada. En algunos despliegues este nivel de autenticación no existe y simplemente se deniega el acceso a la red a estos dispositivos. Pre-autenticación se usa con dispositivos que dependen de acceso inmediato a la red, para funcionar normalmente incluso antes de que se haya establecido su identidad, por ejemplo un dispositivo que necesita descargar su sistema operativo (teléfonos IP, *access points*) o un dispositivo que necesita suficiente conectividad para realizar otro tipo de autenticación como por ejemplo *Web-Authentication*.

La categoría de falla de autenticación, como dice su nombre, sucede cuando un usuario o dispositivo no logra proporcionar las credenciales válidas. En algunos despliegues este nivel de autenticación no existe y simplemente se deniega el acceso a la red a estos dispositivos (este es el valor predeterminado). Usando la política de “no acceso”, un proceso manual debe

ser considerado para que los usuarios legítimos puedan remediar sus credenciales, este proceso puede consumir muchos recursos, tanto en términos de educación del usuario final como de soporte de *help desk*, por lo que se sugiere usar otro tipo de política.

3.6.1.2. Autenticación del usuario y dispositivo

La autenticación es el proceso mediante el cual la red verifica la identidad del dispositivo y/o usuario que intenta conectarse. Para que la red sea capaz de autenticar a los usuarios y dispositivos, primero debe decidir qué tipo de credenciales son aceptables para una identificación válida. Lo recomendado es utilizar formas confiables y robustas de identificación, como certificados digitales o los nombres y contraseñas encriptados. Para determinar si las credenciales son aceptables o no depende del método de autenticación que se utiliza para validar estas credenciales, el método de autenticación determina cómo un dispositivo presenta sus credenciales a la red.

IEEE 802.1X es un estándar que define un proceso por el cual el dispositivo que quiere conectarse a la red (llamado suplicante) puede presentar credenciales robustas como certificados digitales y/o contraseñas. IEEE 802.1X es un método de autenticación robusto y es el método que se usa por defecto cuando el suplicante soporta este estándar. El método de EAP (*Extensible Authentication Protocol*) especifica cómo las credenciales se validan y cómo son presentadas, algunos ejemplos de métodos EAP incluyen PEAP-MSCHAPv2 *(Protected Extensible Authentication Protocol – Microsoft Challenge-Handshake Authentication Protocol*) para credenciales basadas en usuario y contraseña y EAP-TLS (*Extensible Authentication Protocol - Transport Layer Security*), para credenciales basadas en certificados digitales. Para los dispositivos que no son compatibles con el estándar IEEE 802.1X existe el método conocido como *MAC-Authentication Bypass* (MAB). MAB es un método de autenticación secundaria en la que el *switch* de acceso detecta la dirección MAC del dispositivo y lo presenta como una forma de identificación.

Una vez elegido el tipo de credencial, ya sea usando IEEE 802.1X con usuario y contraseña o con certificados digitales, o usando la dirección MAC con el método MAB, estas credenciales se deben validar, para esto se requiere una base de datos de dispositivos permitidos y sus credenciales. En la mayoría de los despliegues no hay necesidad de construir una base de datos de credenciales de usuarios ya que con el directorio activo de Microsoft se tiene una base de datos de los usuarios válidos y los equipos corporativos, también se puedes usar LDAP. LDAP (*Lightweight Directory Access Protocol*) es un protocolo abierto, documentado por la IETF, de capa aplicación usado para acceder a servicios de directorio distribuido a través de la red de información que actúan en concordancia con el estándar X.500. Si se utiliza la autenticación basada en direcciones MAC, entonces se necesita una base de datos de direcciones MAC válidas.

3.6.1.3. Niveles de autorización

La autorización es el proceso mediante el cual se otorga a un dispositivo final un nivel de acceso a la red específico. En una red con IBNS el acceso a la red depende de la identidad del dispositivo final, pero también depende de en qué parte del proceso de autenticación se encuentra el dispositivo final. Al diseñar un despliegue de IBNS se debe considerar el tipo de autorización que tiene el dispositivo final en cada una de estas etapas de autenticación: pre-autenticación, autenticación exitosa y falla de autenticación.

En la etapa de pre-autenticación los dispositivos finales no están autorizados para acceder a la red antes de la autenticación. Antes de que el dispositivo final se autentique correctamente a través de 802.1X o MAB, el puerto no permite ningún tipo de tráfico excepto el que es requerido para la autenticación. La siguiente imagen ilustra el funcionamiento de un puerto habilitado con IEEE 802.1X.

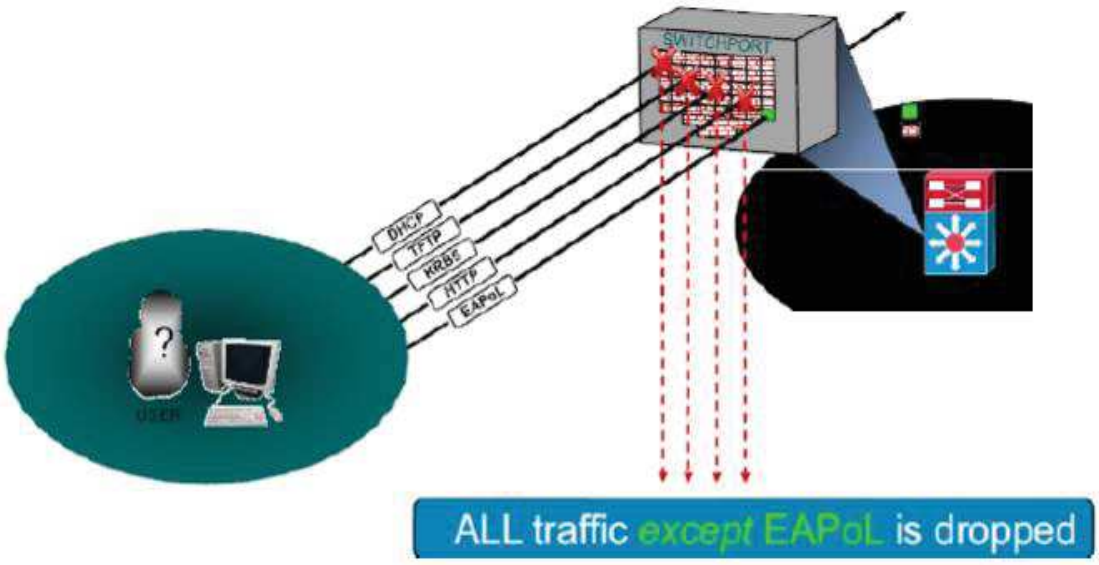


Figura 64. Funcionamiento de un puerto habilitado con IEEE 802.1X

Tomada de: http://www.cisco.com/go/ibns

Este método de control de acceso puede causar problemas para los dispositivos que necesitan acceso a la red antes de la autenticación o dispositivos que son sensibles a los retrasos en el acceso de red. Como alternativa, es posible configurar los *switches* Cisco para dos niveles de autorización conocidos como: acceso abierto y acceso abierto selectivo.

El acceso abierto es lo contrario de la autorización previa de autenticación predeterminado. El modo acceso abierto permite todo el tráfico a través del puerto antes de la autenticación, este modo es importante para el despliegue en las etapas iniciales de la implementación. Acceso abierto selectivo representa un término medio entre el modo por defecto (acceso cerrado) y el acceso abierto. Con acceso abierto selectivo se utiliza listas de acceso (ACL) para permitir o denegar tráfico específico, por ejemplo se puede permitir únicamente tráfico DHCP y TFTP.

En la etapa de autenticación exitosa, es decir una vez que el usuario o dispositivo final presenta sus credenciales y están son validadas y aceptadas por la red, se permite todo el tráfico por ese puerto (acceso total). Para lograr el

acceso basado en la identidad del usuario o dispositivo autenticado se utiliza el control de acceso dinámico con VLANs y/o listas de acceso (ACL). Cuando el acceso posterior a la autenticación exitosa se implementa con VLANs, el *switch* asigna dinámicamente una VLAN a un puerto basado en la identidad del dispositivo que autentifica. Una VLAN aísla tráfico en la capa 2 del modelo OSI pero no puede restringir el acceso a subredes específicas (Capa 3) o aplicaciones (Capa 4 y superiores). En cambio cuando la autorización de autenticación exitosa se implementa con listas de acceso, el *switch* asigna dinámicamente ACLs a un puerto basado en la identidad del dispositivo que autentica, aunque las ACLs no alcanzan el mismo nivel de aislamiento lógico que las VLAN proporcionan, las ACL dinámicas se pueden implementar sin cambiar los esquemas de direccionamiento existentes. Se debe tener cuidado que las listas de acceso dinámicas no sobrepasen la capacidad TCAM del *switch* de acceso.

TCAM (*Ternary Content Addressable Memory*) es una memoria CAM (*Content Addressable Memory)* especializada, diseñada para búsquedas rápidas. La memoria CAM compara exactamente bit por bit y tiene dos posibles resultados: 0 (*true*) o 1 (*false*) y es más usada para armar tablas que buscan coincidencias exactas como las tablas de direcciones MAC. La memoria TCAM tienes tres posibles resultados: 0, 1 y “no importa”. El tercer resultado admite realizar búsquedas amplias basadas en coincidencias de patrones (no exactas como en la memoria CAM) y permite que un paquete sea examinado contra una lista de acceso completa en una sola búsqueda.

Otro factor a considerar al decidir entre VLANs dinámicas y ACLs dinámicas, es la forma de autenticación usada en el despliegue, las ACLs dinámicas funcionan bien con cualquier tipo de autenticación, mientras que la asignación de VLANs dinámicas no suelen trabajar bien con el modo de autenticación acceso abierto. Cuando la autenticación está en modo de acceso abierto, los dispositivos finales pueden recibir direcciones IP en una subred específica (VLAN) pero si una VLAN diferente es asignada como el resultado de una autenticación, la dirección antigua no será válida en la nueva VLAN.

Dispositivos finales compatibles con IEEE 802.1X con suplicantes modernos pueden detectar el cambio de VLAN y solicitar una nueva dirección IP en la nueva VLAN pero los dispositivos sin clientes 802.1X (tales como las impresoras, teléfonos, *access points*) no serán capaces de hacerlo. Los diferentes tipos de autorizaciones disponibles tras la autenticación exitosa y las consideraciones de implementación para cada método se resumen en la siguiente tabla.

Tabla 11. Tipos de autorización con autenticación exitosa

TIPOS DE AUTORIZACIÓN CON AUTENTICACIÓN EXITOSA				
MÉTODO DE AUTORIZACIÓN	**IMPACTO EN LA RED**	**IMPACTO TCAM**	**MÉTODOS DE AUTENTICACIÓN COMPATIBLES**	**NOTAS**
Abierto (por defecto)	Mínimo	Ninguno	Acceso cerrado	Para etapas iniciales en despliegues complejos o para despliegues simples
VLAN dinámica	Significativo	Ninguno	Acceso cerrado	Permite aislamiento lógico a nivel de capa dos del modelos OSI
ACL dinámica	Mínimo	Significativo	Todos	Permite control de acceso a nivel de capa 3 y capa 4

En la etapa de falla de autenticación, después de un fallo de autenticación el puerto se quedará en el mismo estado en el que estaba antes de la autenticación (comportamiento por defecto). Ya que una falla de autenticación revierte el proceso a una etapa de pre-autenticación es necesario verificar si esta etapa (pre-autenticación) es adecuada para los dispositivos que fallaron la

autenticación, se puede modificar el comportamiento por defecto de una falla de autenticación.

3.6.1.4. Modo de conexión del usuario y dispositivo final

La conexión más sencilla es una conexión directa de un único host (dispositivo final) a un puerto del *switch*, esto se conoce como *single host*. El modo *single host* es la forma más segura y el modo por defecto en los *switches* Cisco habilitados para IEEE 802.1X y MAB. Un puerto configurado con IEEE 802.1X en modo *single host* sólo permitirá un dispositivo a la vez en ese puerto (un dominio de datos), si otro dispositivo se conecta a ese puerto el *switch* apaga (*shutdown*) el puerto.

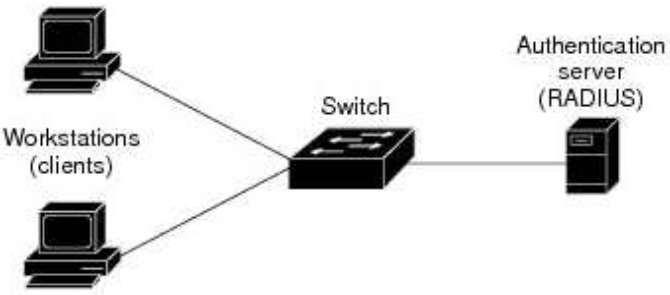
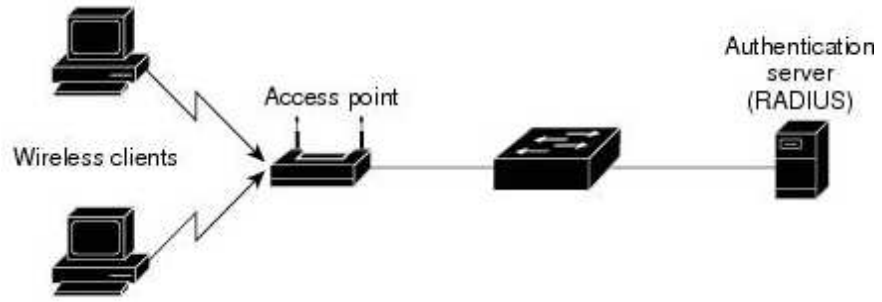
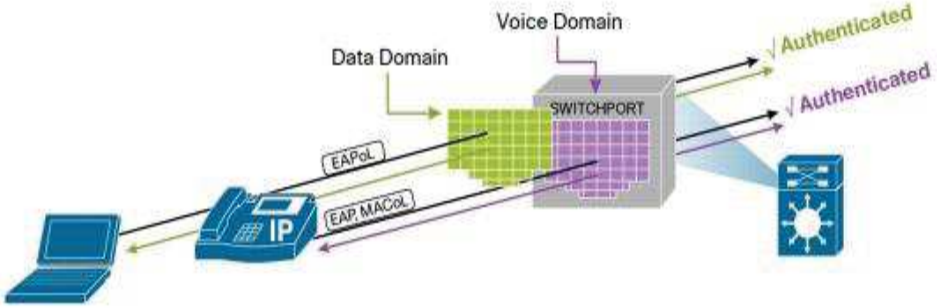
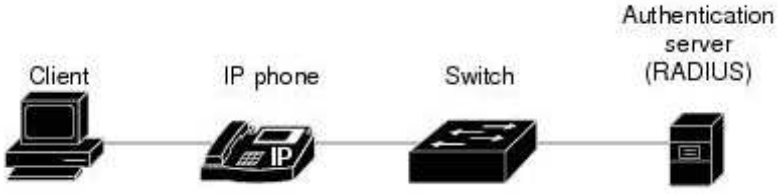
El modo *multi-host* permite autenticar múltiples *hosts* en un puerto configurado para IEEE 802.1X después de que un solo *host* ha sido autenticado de manera exitosa, este modo no es recomendado.

Un despliegue común en infraestructuras de red IP es el uso de telefonía IP, en estas implementaciones dos dispositivos se conectan a un mismo puerto del *switch*: el teléfono IP y un PC detrás del teléfono IP. Para este tipo de despliegues se necesita el modo *multi-domain*. Con este modo el *switch* permite que dos dispositivos se autentiquen en un mismo puerto; un dispositivo de voz (dominio de voz) y un dispositivo de datos (dominio de datos).

En la actualidad muchas computadoras soportan máquinas virtuales, para este tipo de escenarios se utiliza el modo *multi-auth*, que permite a cada máquina virtual acceder al puerto después de ser autenticada. Este modo permite la autenticación de solo un dispositivo de voz (dominio de voz) y varios dispositivos de datos (dominio de datos). El modo más adecuado para configurar en el *switch* está determinado por cómo los dispositivos finales se conecten a la red.

La siguiente tabla ilustra los distintos modos de conexión que existen para los usuarios finales.

Tabla 12. Modos de conexión usuarios finales

MODOS DE CONEXIÓN USUARIO FINAL	
MODO	**ILUSTRACIÓN**
Single host	 Tomada de: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#wp1132802
Multi-host	 Tomada de: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#wp1132802
Multi-Domain	 Tomada de: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-605524.html
Multi-auth	 Tomada de: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dot1x.html#wp1132802

3.6.2. Mejores prácticas para la implementación

Una vez que se ha determinado cómo se van a autenticar los usuarios y dispositivos, qué segmento de red se les concederá antes y después de la autenticación y cómo se les permitirá a los dispositivos conectarse a la red, el siguiente paso es implementar la solución. El despliegue IBNS es más exitoso cuando se implementa en fases, añadiendo paulatinamente las restricciones de acceso de red para minimizar el impacto a los usuarios finales. Las tres fases sugeridas por Cisco son: modo monitor, modo de bajo impacto y modo de alta seguridad, la siguiente tabla muestra las principales características de cada fase.

Tabla 13. Fases mejores prácticas para la implementación IBNS

FASES MEJORES PRÁCTICAS IMPLEMENTACIÓN IBNS	
FASES	**PRINCIPALES CARACTERÍSTICAS**
Modo monitor	• En esta fase no se impide el acceso a ningún usuario pero se obtiene visibilidad sobre quién se está conectando a la red, quién obtuvo acceso a la red, qué dispositivo tiene un cliente 802.1X operativo y quién presenta credenciales válidas. • En modo monitor la autenticación (IEEE 802.1X y MAB) está activada pero no ejecuta ningún tipo de autorización, es decir no hay impacto en los usuarios o puntos finales, los usuarios siguen con el mismo tipo de acceso a la red que antes de la implementación de IBNS, en otras palabras el nivel de autorización siempre es *open*, independiente de si la autenticación es exitosa o no. • Permite recolectar información muy detallada de cada extremo que se conecta a la red, incluyendo: nombre de usuario, dirección IP, dirección MAC, el puerto y el *switch* donde se conectó y el tiempo de conexión. • Permite afrontar de manera proactiva los problemas que podrían afectar a los usuarios finales una vez que el control de acceso a la red basado en identidad (IBNS) esté activado.
Modo de bajo impacto	• En modo de bajo impacto, el nivel de pre-autenticación está en acceso abierto selectivo en lugar de acceso abierto. La diferencia es que este modo se añade una ACL en el puerto del *switch* que especifica exactamente qué tráfico se permitirá antes de la autenticación, los dispositivos que fallen el proceso de autenticación (mediante 802.1X o MAB) seguirán teniendo acceso limitado definido por la ACL configurada en ese puerto de entrada. • Dado que el modo de bajo impacto puede desplegarse con poco o ningún cambio en el diseño de la red existente, es ideal para implementar control de acceso a la red sin alterar la infraestructura de VLANs existentes o el esquema de direccionamiento IP.

	• Estas listas de acceso dinámicas amplían el protocolo RADIUS para optimizar el proceso de descarga y soportar ACLs de tamaño arbitrario.
Modo de alta seguridad	• Si el modo de bajo impacto no cumple con los requisitos de seguridad de la red este modo puede ser omitido por completo y la implementación puede pasar directamente a la fase de modo de alta seguridad en modo monitoreo. • El modo de alta seguridad es un modelo de implementación tradicional de IEEE 802.1X. En una red bien diseñada, este modo proporciona un control total sobre el acceso a la red a nivel de capa 2. • En este modo el puerto se mantiene cerrado hasta que exista una autenticación exitosa, no existe el concepto de pre-autenticación. • Para los dispositivos que no pueden realizar 802.1X puede existir un retraso significativo al acceder a la red. Para evitar los retrasos asociados con 802.1X en el modo de alta seguridad, el *switch* se debe configurar para realizar primero MAB y luego 802.1X. Esto permitirá a los dispositivos que no tienen un cliente IEEE 802.1X obtener acceso inmediato a través de MAB. • Este modo utiliza asignación dinámica de VLAN para aislar las diferentes clases de usuarios en diferentes dominios de difusión (*broadcast*). Los dispositivos que no pueden autenticar o fallan en la autenticación conservan el mismo nivel de acceso que tenían antes de la autenticación.

La siguiente tabla muestra un resumen de los distintos escenarios IBNS descritos anteriormente y parámetros importantes de cada escenario.

Tabla 14. Resumen escenarios IBNS

RESUMEN ESCENARIOS IBNS					
ESCENARIO	**TIPOS DE AUTENTICACIÓN**	**MODO DE CONEXIÓN**	**PRE-AUTENTICACIÓN**	**AUTENTICACIÓN EXITOSA**	**FALLA DE AUTENTICACIÓN**
Modo monitor	IEEE 802.1X y MAB	Multi-*authentication*	Acceso abierto	Abierto	Acceso abierto
Modo de bajo impacto	IEEE 802.1X y MAB	Single-*authentication* y Multi-domain	Acceso abierto selectivo	ACL Dinámica	Acceso abierto selectivo
Modo de alta seguridad	IEEE 802.1X y MAB	Single-*authentication* y Multi-domain	Cerrado	VLAN Dinámica	Cerrado

3.7. Diseño del servicio de red basado en identidad (IBNS)

IBNS será desplegado en el edificio Matriz de TAME EP siguiendo las buenas prácticas y sugerencias del fabricante Cisco descritas en la sección anterior. Como se detalla a profundidad en el capítulo uno, la solución IBNS necesita para su despliegue de 3 elementos; un servidor de autenticación, un autenticador y un suplicante.

El servidor de autenticación debe cumplir las funciones de autenticación, autorización y contabilidad (*accounting*) y operar tanto con el protocolo RADIUS como con el protocolo TACACS+. Los nuevos *switches* Cisco funcionarán como autenticador para todos los usuarios tanto del edificio Matriz como de Tababela y los dispositivos finales como suplicantes.

La solución IBNS para TAME EP será para ambientes virtuales, se creará una máquina virtual dentro del *blade center* que alojará todo el sistema operativo del servidor AAA.

Ya que el servicio IBNS es crítico se considerará alta disponibilidad a nivel del servidor AAA, por lo que se instalará una máquina virtual con el sistema operativo del servidor AAA en el *blade center* del *data center* de la Matriz ubicado en Quito (servidor AAA primario) y se instalará otra máquina virtual en el *blade center* del *data center* del nuevo aeropuerto de TAME EP ubicado en Tababela (servidor AAA secundario).

Ya que la empresa TAME EP cuenta con un *firewall* de última generación donde llegan todos sus enlaces WAN (incluido el del nuevo aeropuerto) se debe configurar reglas que permitan al servidor AAA primario comunicarse con el AAA secundario sin ningún tipo de filtro para que exista una réplica de la base de datos, sincronización y comunicación exitosa, y que permitan también a todos los *switches* de Matriz comunicarse con el AAA secundario usando los protocolos RADIUS (puertos UDP 1645, 1646, 1812 y 1813) y TACACS+ (puerto TCP 49).

En cuanto a la categoría de usuarios y dispositivos se integrará el servidor AAA con el directorio activo de Microsoft, de esta manera se podrá gestionar el acceso a la red de cada usuario o grupo de usuarios (grupo de seguridad).

Generalmente dentro del directorio activo se trabaja con unidades organizacionales, pero el servidor AAA de Cisco (CSACS) no trabaja con unidades organizacionales solo con grupos de seguridad. Por lo que los usarios pertenecientes a unidades organizacionales específicas deben pertenecer a un grupo de seguridad para el despliegue IBNS.

Para la autenticación de los empleados (dispositivos que estén dentro del dominio tame-ep.net.ec) se usará un despliegue SSO (*Single Sing On*) usando IEEE 802.1X como método y como credenciales las almacenadas en el directorio activo de Microsoft, para los dispositivos que no tienen un cliente IEEE 802.1X por ejemplo teléfonos IP e impresoras se utilizará el método MAB. En cuanto a personas ajenas a la organización (dispositivos fuera del dominio) se usará el método *web authentication*.

Lo que se refiere a niveles de autorización se usará un despliegue de VLAN dinámicas, es decir dependiendo de las credenciales que ingrese el usuario el servidor AAA le dirá al autenticador (*switch* de acceso) que coloque a ese puerto en una VLAN específica. La siguiente imagen muestra el funcionamiento esperado en el diseño IBNS propuesto.

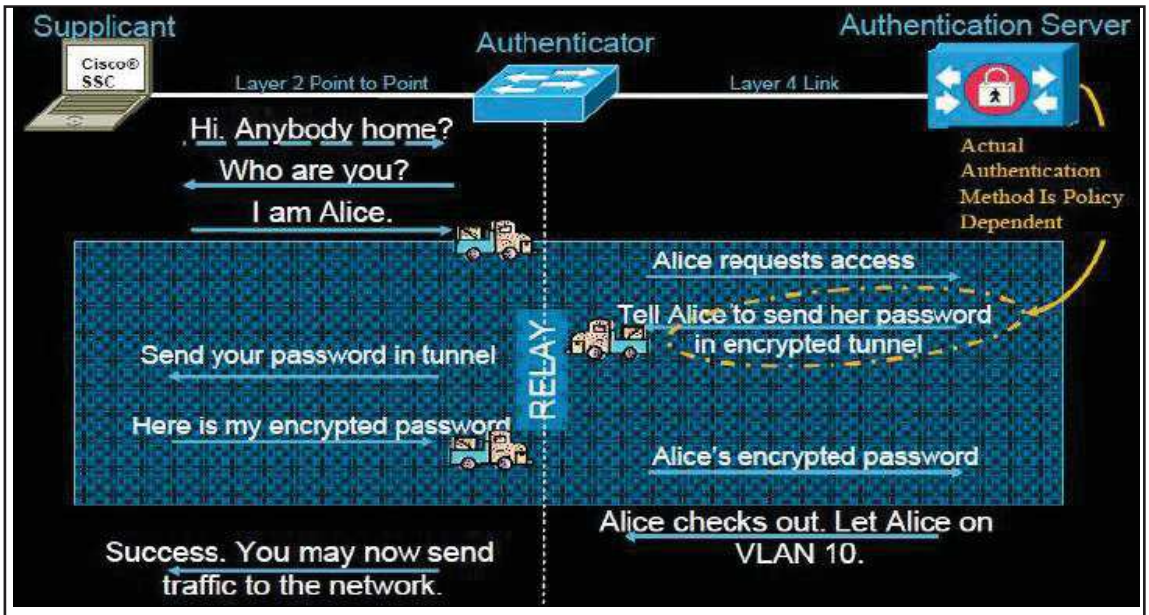


Figura 65. Funcionamiento IBNS

Tomada de: http://www.cisco.com/go/ibns

Se crearán nuevos segmentos de red asociados con cada grupo de seguridad en el directorio activo, de esta manera se podrá asignar una VLAN específica (segmento de red) dependiendo de a qué grupo de seguridad pertenece ese usuario, con esta configuración se puede asignar privilegios y restricciones por cada grupo de seguridad. El nuevo direccionamiento IP se detalla en la siguiente sección.

Para la implementación del sistema IBNS como fase inicial se usará el modo de alta seguridad pero en modo monitoreo, en este escenario se configurará toda la solución, los niveles de autenticación y autorización definitivos, pero con la salvedad de que no se bloquea los puertos del *switch* por una autenticación fallida.

Con este tipo de despliegues se tiene dos grandes ventajas: la primera es que el usuario final no tiene ningún tipo de afectación, es decir el despliegue de IBNS es transparente para los empleados. La segunda ventaja es que permite acciones proactivas al personal de infraestructura de red para lograr remediar

errores antes del despliegue definitivo y de esta manera se reduce la afectación al usuario final al mínimo.

Una vez solucionados todos los problemas que se puedan encontrar en la fase inicial se modificará la opción para que el modo de alta seguridad no siga en modo monitoreo y la solución IBNS empiece a trabajar en todo el edificio Matriz.

3.8. Elementos necesarios para el servicio de red basado en identidad (IBNS)

Para el despliegue de IBNS se necesita un servidor AAA (Autenticación, Autorización y Contabilidad/*Accounting*), un equipo de *networking* que actúe como autenticador y un equipo final que actúe como suplicante (computadoras de escritorio, portátiles, dispositivos inalámbricos), como se describe más a profundidad en el capítulo uno.

3.8.1. Servidor AAA

Existen muchos servidores de autenticación en el mercado: el servidor Steel-Belted RADIUS de Funk, el RADIUS *Authentication* Billing Manager de Livingston Enterprises entre otros. Aunque son productos muy conocidos carecen de la habilidad de combinar los protocolos TACACS+ y RADIUS en una sola solución.

El Cisco Secure Access Control Server (CSACS) es una sola solución que ofrece AAA tanto para TACACS+ como para RADIUS, además es un servidor de control de acceso a la red altamente escalable y de alto rendimiento que puede ser usado para controlar el acceso y la configuración para todos los dispositivos de red usando tanto RADIUS como TACACS+.

3.8.2. Autenticador

Los equipos de *networking* a nivel de capa de acceso, seleccionados en la sección anterior dentro del esquema IBNS tomarán el papel de autenticador. Estos *switches* controlan el acceso físico a la red basado en el estado de

autenticación del suplicante, estos dispositivos actúan como un intermediador entre el cliente y el servidor de autenticación (CSACS). La siguiente tabla indica qué *switches* asumirán este papel, cabe recalcar que el *switch* de núcleo colapsado no fungirá de autenticador ya que ningún dispositivo final se conectará a este equipo, pero si se configurará TACACS+ para la administración del equipo.

Tabla 15. Equipos autenticadores

EQUIPOS AUTENTICADORES	
CAPA DEL MODELO JERÁRQUICO DE CISCO	**MODELO DEL EQUIPO**
Acceso	WS-C2960S-48FPD-L
	WS-C2960S-48FPS-L
	WS-C2960S-24PD-L
	WS-C2960S-24PS-L

3.8.3. Suplicante

Todos los dispositivos de los usuarios finales tomarán el papel de suplicantes es decir, computadoras, portátiles, teléfonos IP, dispositivos inalámbricos y todo dispositivo que desee conectarse a la infraestructura de red.

3.9. Diseño del nuevo direccionamiento IP

El nuevo direccionamiento IP para TAME EP en el edificio Matriz y en Tababela tiene el objetivo de tener una red de información escalable y que permita sumarizar redes. El hecho de poder sumarizar redes implica un menor procesamiento en los *router*s, disminuyendo el *delay* por procesamiento.

Además al tener un direccionamiento IP ordenado y con redes contiguas permite un *troubleshooting* más eficiente. Tomando en cuenta las ventajas de tener un direccionamiento IP escalable, la siguiente tabla indica las redes que se usarán en Matriz y Tababela.

Tabla 16. Nuevo direccionamiento IP Matriz y Tababela.

NUEVO DIRECCIONAMIENTO IP MATRIZ Y TABABELA		
LOCALIDAD	**DIRECCIONAMIENTO**	**RANGO**
Edificio Matriz	10.1.0.0/17	10.1.0.1 – 10.1.127.254
Localidades en Tababela	10.1.128.0/17	10.1.128.1 – 10.1.255.254

La siguiente tabla 17 muestra el direccionamiento IP para el edifico Matriz de las nuevas VLANs y su asociación con los grupos de seguridad en el directorio activo, de acuerdo al diseño IBNS.

Tabla 17. Direccionamiento IP edificio Matriz para las nuevas VLANs.

DIRECCIONAMIENTO IP MATRIZ – NUEVAS VLAN		
NOMBRE DEL GRUPO DE SEGURIDAD	**DESCRIPCIÓN**	**SEGMENTO DE RED**
EQ-ADQAER	VLAN100-Departamento de Adquisiciones Aeronáuticas	10.1.100.0/24
EQ-ADQLOC	VLAN101-Departamento de Adquisiciones Locales	10.1.101.0/24
EQ-DIRAUD	VLAN102-Dirección de Auditoría	10.1.102.0/24
EQ-DPTOCAP	VLAN103-Departamento de Capacitación	10.1.103.0/24
EQ-DPTOCON	VLAN104-Departamento de Contabilidad	10.1.104.0/24
EQ-INGSW	VLAN105-Departamento de Ingeniería de Software	10.1.105.0/24
EQ-DPTOHD	VLAN106-Departamento de Help Desk	10.1.106.0/24
EQ-DPTOINFR	VLAN107-Departamento de Infraestructura	10.1.107.0/24
EQ-DPTOINGR	VLAN108-Departamento de Ingresos	10.1.108.0/24
EQ-DPTOINV	VLAN109-Departamento de Inventarios	10.1.109.0/24
EQ-DIRJUR	VLAN110-Dirección Jurídica	10.1.110.0/24
EQ-DPTOMKTG	VLAN111-Departamento de Marketing	10.1.111.0/24
EQ-DIRPALNIF	VLAN112-Dirección de Planificación	10.1.112.0/24
EQ-DPTOPPTO	VLAN113-Departamento de Presupuesto	10.1.113.0/24
EQ-DPTORRHH	VLAN114-Departamento de Recursos Humanos	10.1.114.0/24
EQ-DPTOPT	VLAN115-Departamento de Plataformas Tecnológicas	10.1.115.0/24
EQ-	VLAN116-Departamento de Relaciones Públicas	10.1.116.0/24

DPTORRPP		
EQ-RENOFTA	VLAN117-Departamento de Renovación de Flota	10.1.117.0/24
EQ-DPTORSVA	VLAN118-Departamento de Reservaciones	10.1.118.0/24
EQ-DPTORM	VLAN119-Departamento de Revenue Management	10.1.119.0/24
EQ-DPTOSEG	VLAN120-Departamento de Seguros	10.1.120.0/24
EQ-DPTOTES	VLAN121-Departamento de Tesorería	10.1.121.0/24
EQ-DPTOVEN	VLAN122-Departamento de Ventas	10.1.122.0/24
EQ-GERENTES	VLAN123-Gerentes EQ	10.1.123.0/24
EQ-INVITADOS	VLAN124-Invitados	10.1.124.0/24
EQ-CESADOS	VLAN125-Usuarios Deshabilitados	10.1.125.0/24

4. Capítulo IV. Análisis técnico económico

4.1. Introducción

Para la ejecución del presente proyecto se debe realizar una gran inversión de tiempo, esfuerzo y dinero, con el interés de mejorar el rendimiento de la red, de convertirla en una red más robusta y de gran confiabilidad.

Luego de identificar el estado de la red actual, las causas de su degradación, sus puntos de falla, entre otros factores tomados de la información recabada en los capítulos anteriores, se expone una nueva solución con la que se espera superar los inconvenientes actuales para convertirla en una red resistente y de mayor rendimiento.

En el presente capítulo se presentará un análisis de las fortalezas y beneficios que se espera obtener luego del nuevo diseño presentado en el capítulo 3 y de la implementación que se documentará en el capítulo 5, se tomará en cuenta y se detallará los valores económicos de la solución que se brindará. Los detalles se exhibirán más adelante en el desarrollo de este capítulo.

4.2. Análisis técnico

En cuanto a las mejoras que se aspira lograr, tenemos en primera instancia que al usar una misma marca de los equipos de la red, se espera lograr una mejor administración, además de un mejor control y un ahorro significativo de recursos ya que no se requerirá especialistas en cada marca como en la actualidad para brindar soporte.

Se disminuirá la degradación al reemplazar las actuales interconexiones entre los *switches* mediante cableado UTP por la utilización de fibra óptica, adicional mejorará la velocidad de transmisión y se evitará inconvenientes por las características y ventajas que presenta la fibra óptica frente al cableado tradicional de cobre.

Los *switches* D-LINK no administrables instalados en el piso 1 son un grave punto de falla en cuanto a seguridad, permite que un usuario con tan solo

conectarse tenga acceso a la red sin tener que superar ningún nivel de seguridad. Al reemplazar estos *switches* por equipos más robustos, que permitan monitoreo, y sean gestionables permitirá aumentar la seguridad, ya que cada puerto estará configurado para permitir o no la conexión a estos equipos y dependiendo de las credenciales se permitirá acceso únicamente a los recursos a los que tenga autorización, aumentando el nivel de dificultad de acceder a la red y minimizando uno de los principales ataques en seguridad como es un ataque interno por permitir accesos a recursos por personas no autorizadas. Además se prevé un crecimiento a futuro tomando en cuenta la demanda actual de puertos y se tendrá un margen de disponibilidad de ellos.

Al realizar un direccionamiento de red basados en segmentación, se manejará un mejor esquema aplicando por ejemplo calidad de servicio para la voz, teniendo un mayor cuidado sobre el tráfico sensible, ya que al dividir la red por VLANs una de las principales características es que permite separar el tráfico de acuerdo a nuestros requerimientos y además permite aplicar prioridad sobre el tráfico de mayor importancia en la red.

Otro gran beneficio que se espera obtener con la división de tráfico en diferentes VLANs es mejorar el rendimiento y disminuir las tormentas de *broadcast*, ya que el tráfico de una VLAN pasará únicamente por donde sea necesario, evitando saturar la red al permitir que todo el tráfico se transporte por toda la red.

Se disminuirán puntos de falla al implementar una topología en estrella, ya que todos los *switches* tendrán una conexión directa con el *switch* de *core* colapsado y contarán con todas las seguridades necesarias para evitar que personas que no estén autorizadas tengan acceso a los recursos.

Una de las mejores prácticas para manejar una mejor administración es estandarizar los nombres de los equipos, identificándolos a todos y cada uno de ellos, además de respaldar regularmente la información, llevando así un control centralizado de la información relevante y permitiendo el acceso solo a quienes llevan el control de la red.

Mediante el IBNS se tendrá un control de los usuarios que acceden a la red y las acciones que realizan mientras están conectados, luego de haber sido autenticados y autorizados según sus respectivas credenciales. Se va a asociar cada nuevo segmento de red a un grupo de seguridad dentro del directorio activo logrando visibilidad, movilidad y permitiendo dar permisos o restricciones ya sea por grupo de seguridad (áreas de trabajo) o por usuario, es decir por identidad.

4.3. Análisis económico

En cuanto a temas de costos, para detallar el análisis económico se dividirá primordialmente en dos grupos, en el primero se evaluará los costos de los equipos de la solución y en el segundo grupo se evaluará los costos de los servicios necesarios para lograr la implementación. En la siguiente gráfica se muestra brevemente la división de los costos de los dos grupos mencionados:

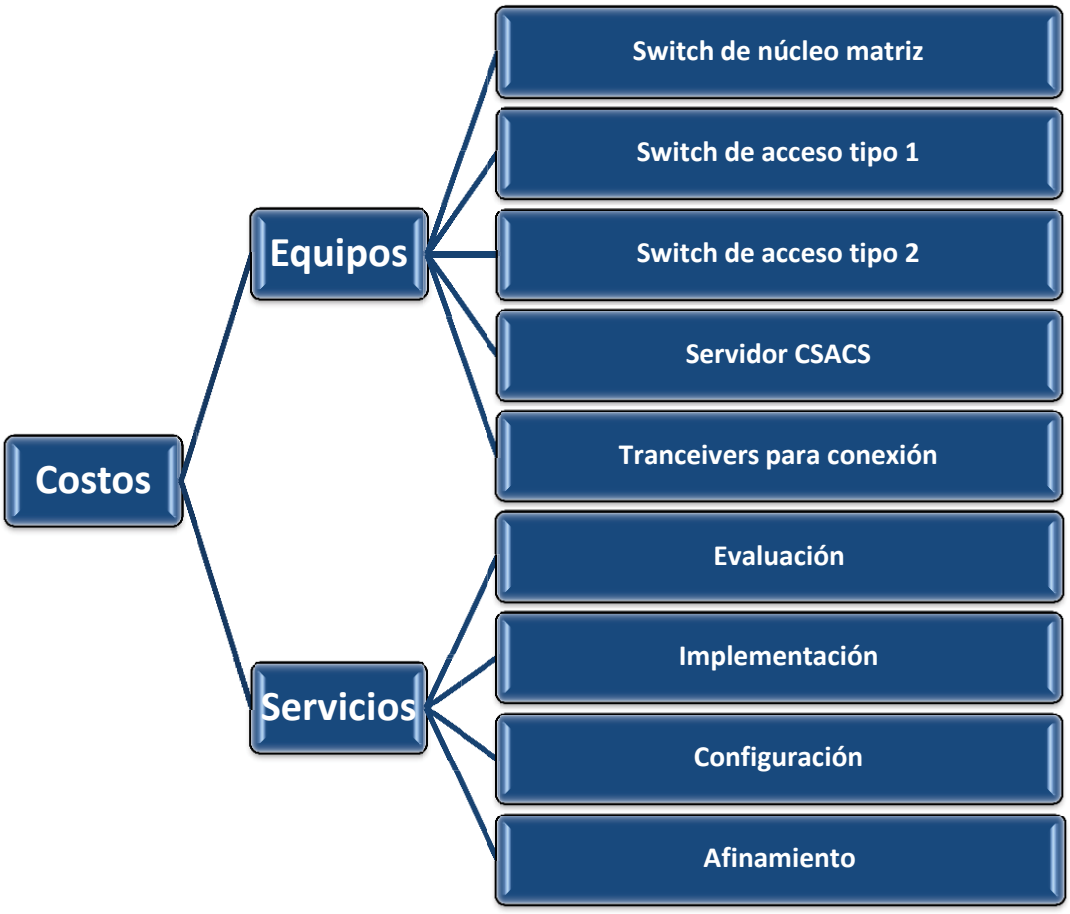


Figura 66. División de costos

A continuación se presenta una tabla sintetizada en la que se puede observar los equipos necesarios para la reingeniería, luego de las respectivas evaluaciones, tomadas a partir del diseño mostrado en el capítulo 3, la cantidad requerida de cada uno, su respectiva descripción y su correspondiente valor económico en el mercado.

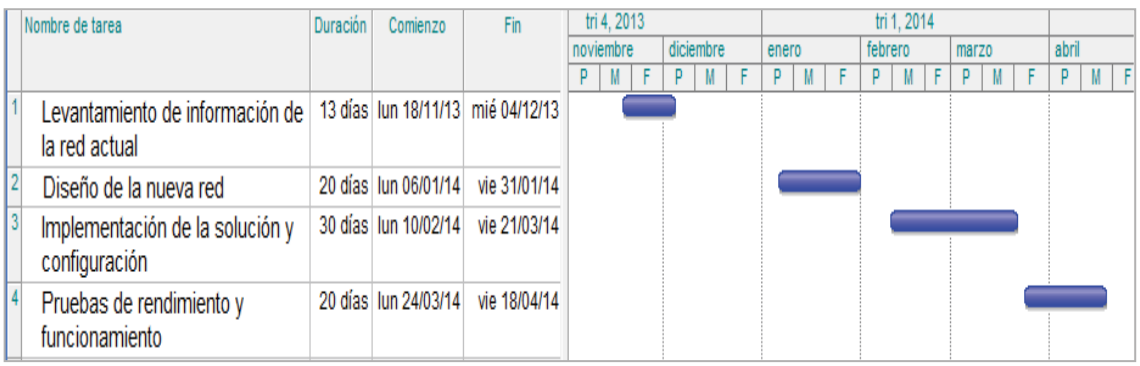
Tabla 18. Detalle de equipos

DETALLE DE EQUIPOS					
ÍTEM	**NOMBRE**	**DESCRIPCIÓN**	**CANTIDAD**	**PRECIO USD**	**PRECIO TOTAL**
1.0	WS-C4506-E	Catalyst 4500 E-Series *Switch* de Núcleo	1	31470,00	31470,00
2.0	WS-C2960S-24PS-L	Catalyst 2960S 24 GigE PoE 370W 4 x SFP LAN Base	1	3195,00	3195,00
3.0	WS-C2960S-48FPS-L	Catalyst 2960S 48 GigE PoE 740W 4 x SFP LAN Base	4	6595,00	26380,00
4.0	L-CSACS-54VM-K9	ACS 5.4 VMware Software + Base License	1	14395,00	14395,00
5.0	WS-C2960S-24PD-L	Catalyst 2960S 24 GigE PoE 370W 2 x 10G SFP+ LAN Base	3	4595,00	13785,00
6.0	WS-C2960S-48FPD-L	Catalyst 2960S 48 GigE PoE 740W 2 x 10G SFP+ LAN Base	5	7995,00	39975,00
7.0	GLC-SX-MMD	1000BASE-SX SFP transceiver module MMF 850nm DOM	22	500,00	11000,00
			Subtotal 1		140200,00

Con la solución planteada se busca mejorar la seguridad de la información, optimizar el *performance* de la red, llevar un control de las personas que ingresan a la red y las acciones que realizan dentro de ella, todas estas gestiones en busca de precautelar la correcta operación de la red.

En cuanto al costo de los servicios, se debe considerar el tiempo de la solución desde un inicio, que va desde el levantamiento de la información actual, continuando con una investigación de los diferentes equipos en el mercado, su funcionamiento y operación, la selección de los equipos, la implementación y finalmente las pruebas del rendimiento, todas éstas etapas son primordiales para determinar el costo total y real de los servicios requeridos para culminar con el proyecto.

Para tener una idea más clara a continuación se presenta un cronograma con el detalle de las diferentes y principales etapas para llevar a cabo con el presente proyecto.



	Nombre de tarea	Duración	Comienzo	Fin
1	Levantamiento de información de la red actual	13 días	lun 18/11/13	mié 04/12/13
2	Diseño de la nueva red	20 días	lun 06/01/14	vie 31/01/14
3	Implementación de la solución y configuración	30 días	lun 10/02/14	vie 21/03/14
4	Pruebas de rendimiento y funcionamiento	20 días	lun 24/03/14	vie 18/04/14

Figura 67. Cronograma de Implementación

Para el levantamiento de información de la red actual se establece que son necesarios 13 días laborables, para lo cual se asigna a 2 ingenieros para que se realice visitas en sitio validando la información con la cual trabajan en la actualidad, entre lo relevante está el tipo de equipos instalados, la configuración en cada uno de ellos, las interconexiones, topologías, etc., luego de haber validado la información de la red actual se podrá realizar en base a ello un breve esquema definiendo los puntos claves de la red.

Para realizar el nuevo diseño, 20 días laborables son necesarios debido a múltiples subtareas requeridas para poder plasmar el diseño; previo a ello es necesario realizar una investigación y análisis de los equipos en el mercado indagando su funcionamiento y alcance, para poder luego de ello seleccionar los que cumplan con los nuevos requerimientos de la red. Dos ingenieros en base a la información recaudada presentan el nuevo diseño de la red, ilustrado en el capítulo 3 del presente proyecto.

Para la implementación y configuración de los equipos se establece que será necesario 30 días luego de cumplir con las fases anteriores, en esta tarea se contempla la instalación física de los equipos en los diferentes pisos y áreas de acuerdo al diseño realizado y la configuración en cada equipo para que cumpla con las metas propuestas en el proyecto, principalmente optimizar el

rendimiento de la red, limitar el acceso a la red mediante políticas de seguridad y mitigar amenazas.

Finalmente para realizar pruebas de la solución se asigna 20 días, tiempo en el cual se pondrá a prueba la correcta operación de la red y se realizarán afinamientos en la configuración para cumplir con los objetivos de mejoras en la red luego de implementar el presente proyecto.

En la siguiente tabla se consolida el costo de los servicios Smartnet ofertado por Cisco por el tiempo de cobertura de un año y con un soporte 8x5x4.

Tabla 19. Costos de Servicios Smartnet

COSTOS DE SERVICIOS SMARTNET					
ÍTEM	**NOMBRE**	**DESCRIPCIÓN**	**CANTIDAD**	**PRECIO USD**	**PRECIO TOTAL**
1.0	CON-SCP-C4506E	Catalyst 4500 E-Series *Switch* de Núcleo	1	4.065,88	4.065,88
2.0	CON-SCN-2960S2PS	SC CORE 8X5XNBD Catalyst 2960S Stack	1	264,00	264,00
3.0	CON-SCN-2960S4FS	SC CORE 8X5XNBD Cat 2960S Stk48 GigE PoE 740W4xSFP Base	4	544,50	2.178,00
4.0	CON-SCN-2960S2PD	SC CORE 8X5XNBD Cat2960S Stk24 GigE PoE370W2x10G LANBas	3	379,50	1.138,50
5.0	CON-SCN-2960S4FD	SC CORE 8X5XNBD Cat 2960S Stk48 GigE PoE 740W2x10G LANB	5	660,00	3.300,00
			Subtotal 2		10.946,38

Cisco *SMARTnet* es una solución orientada para pequeñas y medianas empresas que contemplan dos temas principales, primero acceso en línea a herramientas para instalación, configuración, *troubleshooting* y segundo provee reemplazo de *hardware*.

Diseñados para permitirle ampliar y potenciar la vida operativa de sus equipos de red de Cisco, este servicio ofrece acceso permanente al Centro de Asistencia Técnica de Cisco, actualizaciones y mejoras del software operativo

de Cisco, reemplazo de hardware y mucho más (Tomado de http://www.cisco.com/web/LA/productos/servicios/smbsupport.html).

Los valores asignados para las tareas levantamiento de información y diseño de la nueva solución se determinaron tomando como base el sueldo de un ingeniero en redes y teniendo en cuenta el número de días necesarios para la realización de cada tarea. A continuación se presenta los costos restantes de la solución, tomando en cuenta la capacitación del personal para llevar a cabo la instalación y las configuraciones en los equipos.

Tabla 20. Costos Servicios

COSTOS SERVICIOS		
ÍTEM	**DESCRIPCIÓN**	**PRECIO USD**
1.0	Levantamiento de información	1600,00
2.0	Diseño de la nueva solución	3000,00
3.0	Instalación y configuración de la solución ofertada	10500,00
4.0	Curso de 50 horas de CSACS para 2 personas	2500,00
5.0	Transferencia general de conocimientos (8 horas)	400,00
6.0	Paquete de 36 horas de soporte especializado con respuesta 8x5x4	2520,00
7.0	Capacitación en academia CCNA para 2 personas (280 horas)	2000,00
8.0	Capacitación en academia CCNP para 2 personas (270 horas)	2100,00
9.0	Cableado vertical (Fibra Óptica)	6000,00
	Subtotal 3	30620,00

El costo total de la solución tomando en cuenta todos los valores mencionados es de $ 181766,38. En este valor se contempla lo necesario para culminar con éxito el proyecto.

5. Capítulo V. Implementación y pruebas de la nueva red conmutada y del servicio de red basado en identidad

5.1. Implementación red conmutada

5.1.1. Antecedentes

La red conmutada en el edificio matriz estaba conformada con equipos de distintas marcas como 3Com, D-LINK, ENTERASYS. El *backbone* es de fibra óptica pero en ciertos pisos los *switches* se conectaban en forma de cascada usando cable UTP, lo que implica una degradación en el rendimiento de la red y un grave punto de falla. La topología de la red conmutada no permitía un correcto manejo de alta disponibilidad, redundancia, ni la posibilidad de crecimiento ya que la densidad de puertos en todos los *switches* estaba prácticamente agotada.

5.1.2. Desarrollo

Se definió un esquema de direccionamiento IP basado en segmentación de red por servicios (datos y voz). La segmentación para el tráfico de voz ayuda a asegurar la calidad de servicio del mismo y al tener una red de información segmentada en VLANs se tienen las siguientes ventajas:

i. Seguridad: Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.
ii. Reducción de costo: El ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y más usos eficientes de enlaces y ancho de banda existente.
iii. Mejor rendimiento: La división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de *broadcast*) reduce el tráfico innecesario en la red y potencia el rendimiento.

iv. Mitigación de la tormenta de *broadcast*: La división de una red en las VLAN reduce la cantidad de dispositivos que pueden participar en una tormenta de *broadcast*.
v. Mayor eficiencia del personal de TI: Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.

La implementación, que se basa en el diseño para la fase uno descrito en el capítulo III, se desarrolló en dos etapas: la primera etapa se centró en la instalación, configuración, implementación y afinamiento de los equipos de *networking* (*switches*) y sus respectivas pruebas de funcionamiento, en esta etapa se mantuvo el direccionamiento IP de la red de información anterior.

La segunda etapa se centró en el despliegue IBNS, es decir en la instalación, configuración y afinamiento del CSACS, además de la configuración de los equipos autenticadores y pruebas de funcionamiento. En esta etapa se cambia el direccionamiento IP de los empleados al detallado en el capítulo III.

5.1.3. Cambio de *backbone* edificio matriz

El antiguo *backbone* de TAME EP en el edifico Matriz consistía en un hilo de fibra óptica fusionado por piso que permitía la conectividad desde el *switch* de núcleo ubicado en el primer piso hasta cada *switch* de acceso ubicado en los distintos pisos.

Esta topología física tenía el grave problema que en los pisos donde, por la cantidad de usuarios, se necesita más de un *switch* estos debían conectarse en forma de cascada usando cable UTP, lo que implica una degradación en el rendimiento de la red y un grave punto de falla.

Esto se puede explicar indicando que si el enlace que une el *switch* de acceso con el *switch* de núcleo falla, todo ese piso quedaría sin servicios, mientras que en una red sin conexiones en cascada solo los usuarios conectados al *switch* afectado quedarían sin servicio, mientras que el resto de usuarios de ese piso no tendrían problemas.

El nuevo *backbone* permite la conexión en forma directa de cada *switch* de acceso al *switch* de núcleo colapsado, es decir permite una topología en estrella. Lo que representa grandes ventajas con la topología anterior como la mejora del rendimiento (*throughput*) y la eliminación de puntos de falla en cada piso por la conexión en forma de cascada.

5.1.4. Equipos de la red conmutada

A nivel de *networking* se maneja el módulo de campus que será dividido mediante el modelo jerárquico de Cisco, que comprende tres capas: núcleo, distribución y acceso.

TAME EP manejará este esquema, donde las capas de núcleo y distribución (*collapsed core*), serán manejadas por el mismo equipo conocido como *switch* de núcleo ubicado en el *data center* en el edificio Matriz y la capa de acceso será manejada por un equipo ubicado en cada uno de los pisos.

La siguiente tabla presenta los *switches* instalados por piso en el edifico matriz, su descripción, nombre (*hostname*) y en qué capa del modelo jerárquico de Cisco están operando.

Tabla 21. *Switches* instalados por piso edificio Matriz

***SWITCHES* INSTALADOS EDIFICIO MATRIZ**			
PISO	**DESCRIPCIÓN**	**NOMBRE**	**CAPA MODELO JERÁRQUICO CISCO**
Piso 1	*Switch* de núcleo principal de Cisco con funciones de capa 3 del modelo OSI (L3)	SW_CORE_MATRIZ	Núcleo colapsado
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_TI	Acceso
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_1	Acceso
Piso 2	*Switch* de acceso de Cisco con funciones de	SW_PISO_2	Acceso

	capa 2 del modelo OSI (L2)		
Piso 4	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_3	Acceso
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_4	Acceso
Piso 5	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_5_1	Acceso
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_5_2	Acceso
Piso 6	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_6	Acceso
Piso 7	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_7_1	Acceso
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_7_2	Acceso
Piso 8	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_8_1	Acceso
	Switch de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_8_2	Acceso
Piso 9	*Switch* de acceso de Cisco con funciones de capa 2 del modelo OSI (L2)	SW_PISO_9	Acceso

5.1.5. Configuración de *routing* inter VLAN

En lo que se refiere al edificio Matriz para el *routing* inter VLAN se configuró el equipo “SW_CORE_MATRIZ” ubicado en el *data center*, este es un *switch* Cisco 4506-E con capacidades de capa 3 del modelo OSI. En este proyecto, se

crearon las interfaces VLAN que se muestran a continuación en la tabla para la conectividad entre VLANs. No se muestra exactamente la dirección IP de cada interfaz VLAN por temas de seguridad.

Tabla 22. Conectividad entre VLANs edificio Matriz

INTERFACES VLAN MATRIZ		
INTERFAZ	**DIRECCIÓN**	**DESCRIPCIÓN**
Vlan 1	10.1.X.X/24	SERVIDORES
Vlan 2	10.1.X.X/29	VLAN SITA
Vlan 4	10.1.X.X/26	ADMINISTRACION
Vlan 5	10.1.X.X/24	VLAN_INFORMATICA
Vlan 6	10.1.X.X/24	VLAN_VENTAS
Vlan 7	10.1.X.X/24	VLAN_RECURSOS_HUMANOS
Vlan 8	10.1.X.X/24	VLAN_LOGISTICA
Vlan 9	10.1.X.X/24	VLAN_FINANZAS
Vlan 10	10.1.X.X/24	VLAN_COMERCIAL
Vlan 11	10.1.X.X/24	VLAN_PRESIDENCIA_ASESORIAS
Vlan 12	10.1.X.X/24	VLAN_AUDITORIA
Vlan 13	10.1.X.X/24	MANTENIMIENTO INFORMATICA
Vlan 17	10.1.X.X/24	Reservaciones
Vlan 18	10.1.X.X/24	Call_Center
Vlan 19	10.1.X.X/24	Datos_Reservas
Vlan 20	10.1.X.X/24	ADM_NETworking
Vlan 21	10.1.X.X/24	VLAN_CAPACITACION
Vlan 23	10.1.X.X/24	DataFast
Vlan 27	10.1.X.X/24	--
Vlan 40	10.1.X.X/24	--
Vlan 220	10.220.X.X/24	VLAN_VIA_XXI
Vlan 225	10.1.X.X/24	--

5.1.6. Segmentación de VLANs

Para el edificio Matriz se estableció el “SW_CORE_MATRIZ” como el servidor del dominio VTP de la red, el cual es “tXXe” con contraseña “tXXXX3”. Los demás *switches* Cisco de la red se encuentran funcionando en modo cliente y están todos bajo la versión 2 de VTP. La siguiente tabla indica las distintas VLANs creadas en el *switch*.

Tabla 23. VLANs edificio Matriz

VLANS EDIFICIO MATRIZ		
VID	**NOMBRE**	**DESCRIPCIÓN**
1	Default	VLAN por defecto
2	SITA	VLAN para SITA
3	VPN_Cisco_Client	VLAN para la VPN de Cisco
4	ADMINISTRACION	VLAN para administración
5	VLAN-INFORMATICA	VLAN para el departamento de informática
6	VENTA_BOLETOS	VLAN para la venta de boletos
7	RECURSOS_HUMANOS	VLAN para el departamento de recursos humanos
8	VLAN_LOGISTICA	VLAN para el departamento de logística
9	VLAN_FINANZAS	VLAN para el departamento de finanzas
10	VLAN_COMERCIAL	VLAN para el departamento comercial
11	PRESI_ASESORIAS	VLAN para asesorías
12	VLAN_AUDITORIA	VLAN para el departamento de auditorías
13	MANTEN_INFORMATICA	VLAN de mantenimiento
17	RESERVACIONES	VLAN para reservaciones
18	CALL_CENTER	VLAN para el departamento de call center
19	DATOS_RESERVAS	VLAN para los datos de las reservas
20	ADM_NETWORKING	VLAN para la administración de los equipos de networking
21	VLAN_CAPACITACIÓN	VLAN para capacitaciones
23	DATAFAST	VLAN para Datafast
27	DEMO_FORTINET	VLAN para demo de Fortinet
33	PRUEBA	VLAN de prueba
40	ELASTIX	VLAN de voz con ELASTIX
220	VLAN_VIA_XXI	VLAN para VIA_XXI
221	VLAN0221	VLAN 221
225	Core<->Checkpoint	VLAN para la comunicación entre el *switch* de núcleo colapsado y el Firewall Checkpoint
250	PRUEBAS_VIA_XXI	VLAN de prueba para VIA_XXI
873	METRO	VLAN para METRO

5.1.7. Configuración de puertos

Cada uno de los puertos designados como troncales tiene la capacidad de pasar todas las VLAN del dominio VTP. Los puertos en modo de acceso pertenecen a una VLAN de datos específica y a una VLAN de voz, sin

embargo, con el despliegue del sistema IBNS estas VLANs se asignarán dinámicamente dependiendo del nivel de autorización e identidad que tenga el usuario. La siguiente tabla indica la configuración de los puertos en el *switch* de núcleo colapsado del edificio Matriz.

Tabla 24. Configuración de puertos en el *switch* de núcleo colapsado "SW_CORE_MATRIZ" edificio Matriz

PUERTOS *SWITCH* DE NÚCLEO COLAPSADO "SW_CORE_MATRIZ"				
PUERTOS	**PORTCHANNEL**	**TRONCAL**	**ACCESO**	**DESCRIPCIÓN**
GigabitEthernet 2/1	-	-	VLAN 1	10.1.X.X
GigabitEthernet 2/2	-	-	VLAN 1	Server MAIL 10.1.X.X
GigabitEthernet 2/3	-	X	-	Hacia *switch* "SW_PISO_1"
GigabitEthernet 2/4	-	-	VLAN 1	EQMAIL
GigabitEthernet 2/5	-	-	VLAN 1	INETSERVER MATRIZ 10.1.X.X
GigabitEthernet 2/6	-	-	VLAN 2	SITA 159
GigabitEthernet 2/7	-	X	-	-
GigabitEthernet 2/8	-	-	VLAN 2	SITA 160
GigabitEthernet 2/9	-	-	VLAN 18	CM_S8300
GigabitEthernet 2/10	-	-	VLAN 40	NBX MÓDULOS ANALÓGICOS
GigabitEthernet 2/11	-	-	VLAN 18	CM_SMART
GigabitEthernet 2/12	-	-	VLAN 20	NBX MÓDULOS E1
GigabitEthernet 2/13	-	-	VLAN 18	CM_AES 10.1.X.X
GigabitEthernet 2/14	-	-	VLAN 18	CM_BCMRD 10.1.X.X
GigabitEthernet 2/15	-	X	-	--
GigabitEthernet 2/16	10	X	-	Hacia *switch* MAIPU
GigabitEthernet 2/17	-	-	VLAN 1	--
GigabitEthernet 2/18	-	-	VLAN 18	CM_VOICE_PORTAL 10.1.X.X
GigabitEthernet 2/19	-	-	VLAN 1	--

GigabitEthernet 2/20	-	-	VLAN 1	SW-Blade-21
GigabitEthernet 2/21 – 2/23	-	-	VLAN 4	--
GigabitEthernet 2/24	-	-	VLAN 4	Console_blade
GigabitEthernet 2/25	-	X	-	POWER6 1
GigabitEthernet 2/26	-	-	VLAN 1	POWER6 2
GigabitEthernet 2/27	10	X	-	Hacia *switch* MAIPU
GigabitEthernet 2/28	-	-	VLAN 873	DMZ
GigabitEthernet 2/29	-	-	VLAN 873	DMZ
GigabitEthernet 2/30 – 2/34	-	-	VLAN 1	--
GigabitEthernet 2/35	-	X	-	--
GigabitEthernet 2/36 – 2/47	-	-	VLAN 1	--
GigabitEthernet 2/48	-	X	-	Hacia *switch* SW_PISO_TI
GigabitEthernet 3/1	-	X	-	Hacia SW_PISO_7_2
GigabitEthernet 3/2	-	X	-	PISO2_RRHH
GigabitEthernet 3/3	-	X	-	Hacia SW_PISO_5_2
GigabitEthernet 3/4	-	X	-	PISO4_LOGISTICA
GigabitEthernet 3/5	-	X	-	PISO5_FINANZAS
GigabitEthernet 3/6	-	X	-	PISO6_PRESIDENCIA
GigabitEthernet 3/7	-	X	-	PISO7_COMERCIAL
GigabitEthernet 3/8	-	X	-	PISO8_RESERVAS
GigabitEthernet 3/9	-	X	-	PISO9_AULA
GigabitEthernet 3/10	-	X	-	Hacia SW_PISO_3
GigabitEthernet 3/11	-	X	-	POWER6 1
GigabitEthernet 3/12	-	X	-	Hacia SW_PISO_8_2

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 1 del edificio Matriz.

Tabla 25. Configuración de puertos en el *switch* "SW_PISO_1" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_1"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/2, 1/0/19, 1/0/36, 1/0/37, 1/0/38, 1/0/40, 1/0/47	-	-	VLAN 1 VLAN 40 (Voz)	-
GigabitEthernet 1/0/25 – 1/0/29, 1/0/32 – 1/0/35, 1/0/39, 1/0/41, 1/0/43 – 1/0/46	-	-	VLAN 5 VLAN 40 (Voz)	-
GigabitEthernet 1/0/3 – 1/0/18, 1/0/20, 1/0/22	-	-	VLAN 6 VLAN 40 (Voz)	-
GigabitEthernet 1/0/21	-	-	VLAN 8 VLAN 40 (Voz)	-
GigabitEthernet 1/0/24	-	-	VLAN 8 VLAN 27	-
GigabitEthernet 1/0/30, 1/0/31, 1/0/42	-	-	VLAN 13 VLAN 40 (Voz)	-
GigabitEthernet 1/0/1	-	-	VLAN 20 VLAN 40 (Voz)	-
GigabitEthernet 1/0/23	-	-	VLAN 220 VLAN 40 (Voz)	-
GigabitEthernet 1/0/48	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso de TI del edificio Matriz.

Tabla 26. Configuración de puertos en el *switch* "SW_PISO_TI" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_TI"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/5 - 1/0/7, 1/0/9, 1/0/10,	-	-	VLAN 1 VLAN 40	-

1/0/23, 1/0/38, 1/0/40			(Voz)	
GigabitEthernet 1/0/2 – 1/0/4, 1/0/8, 1/0/12 – 1/0/14, 1/0/16 - 1/0/22, 1/0/25 – 1/0/29, 1/0/32 – 1/0/34, 1/0/37, 1/0/39, 1/0/41, 1/0/43 – 1/0/46	-	-	VLAN 5 VLAN 40 (Voz)	-
GigabitEthernet 1/0/11	-	-	VLAN 11 VLAN 40 (Voz)	-
GigabitEthernet 1/0/1, 1/0/15, 1/0/24, 1/0/30, 1/0/31, 1/0/42, 1/0/48	-	-	VLAN 13 VLAN 40 (Voz)	-
GigabitEthernet 1/0/24, 1/0/36	-	-	VLAN 27	-
GigabitEthernet 1/0/47	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 2 del edificio Matriz.

Tabla 27. Configuración de puertos en el *switch* "SW_PISO_2" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_2"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 – 1/0/24, 1/0/26 – 1/0/36, 1/0/38 – 1/0/48	-	-	VLAN 7 VLAN 40 (Voz)	-
GigabitEthernet 1/0/25	-	-	VLAN 11 VLAN 40 (Voz)	-
GigabitEthernet 1/0/37	-	-	VLAN 27	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 3 del edificio Matriz.

Tabla 28. Configuración de puertos en el *switch* "SW_PISO_3" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_3"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 – 1/0/23	-	-	VLAN 11 VLAN 40 (Voz)	-
GigabitEthernet 1/0/25	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 4 del edificio Matriz.

Tabla 29. Configuración de puertos en el *switch* "SW_PISO_4" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_4"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/45	-	-	VLAN 1 VLAN 40 (Voz)	-
GigabitEthernet 1/0/1 – 1/0/38, 1/0/40 – 1/0/44	-	-	VLAN 8 VLAN 40 (Voz)	-
GigabitEthernet 1/0/46, 1/0/48	-	-	VLAN 27	_
GigabitEthernet 1/0/47	-	-	VLAN 27 VLAN 40 (Voz)	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 5_1 del edificio Matriz.

Tabla 30. Configuración de puertos en el *switch* "SW_PISO_5_1" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_5_1"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet	-	-	VLAN 1	-

1/0/12, 1/0/13, 1/0/15, 1/0/20, 1/0/32			VLAN 40 (Voz)	
GigabitEthernet 1/0/1 – 1/0/11, 1/0/14, 1/0/16 – 1/0/19, 1/0/21 – 1/0/31, 1/0/33 – 1/0/47	-	-	VLAN 9 VLAN 40 (Voz)	-
GigabitEthernet 1/0/48	-	-	VLAN 27	
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 5_2 del edificio Matriz.

Tabla 31. Configuración de puertos en el *switch* "SW_PISO_5_2" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_5_2"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/26 - 1/0/28	-	-	VLAN 1 VLAN 40 (Voz)	-
GigabitEthernet 1/0/1 –1/0/24	-	-	VLAN 9 VLAN 40 (Voz)	-
GigabitEthernet 1/0/25	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 6 del edificio Matriz.

Tabla 32. Configuración de puertos en el *switch* "SW_PISO_6" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_6"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 - 1/0/7, 1/0/9 – 1/0/48	-	-	VLAN 11 VLAN 40 (Voz)	-
GigabitEthernet 1/0/8	-	-	VLAN 27	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 7_1 del edificio Matriz.

Tabla 33. Configuración de puertos en el *switch* "SW_PISO_7_1" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_7_1"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/3, 1/0/7, 1/0/9, 1/0/10, 1/0/13 - 1/0/24, 1/0/26 – 1/0/35, 1/0/37 – 1/0/40. 1/0/42 – 1/0/44	-	-	VLAN 10 VLAN 40 (Voz)	-
GigabitEthernet 1/0/1, 1/0/2, 1/0/4 – 1/0/6, 1/0/8, 1/0/11, 1/0/36, 1/0/41, 1/0/45 – 1/0/48	-	-	VLAN 12 VLAN 40 (Voz)	-
GigabitEthernet 1/0/12, 1/0/24, 1/0/25	-	-	VLAN 27	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 7_2 del edificio Matriz.

Tabla 34. Configuración de puertos en el *switch* "SW_PISO_7_2" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_7_2"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 – 1/0/23	-	-	VLAN 10 VLAN 40 (Voz)	-
GigabitEthernet 1/0/24	-	-	VLAN 12 VLAN 40 (Voz)	-
GigabitEthernet 1/0/25	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 8_1 del edificio Matriz.

Tabla 35. Configuración de puertos en el *switch* "SW_PISO_8_1" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_8_1"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 – 1/0/37, 1/0/39 – 1/0/48	-	-	VLAN 9 VLAN 40 (Voz)	-
GigabitEthernet 1/0/38	-	-	VLAN 27	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 8_2 del edificio Matriz.

Tabla 36. Configuración de puertos en el *switch* "SW_PISO_8_2" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_8_2"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/1 – 1/0/24	-	-	VLAN 17	-
GigabitEthernet 1/0/1 – 1/0/24	-	-	VLAN 19	-
GigabitEthernet 1/0/25	-	X	-	Hacia *switch* de core

La siguiente tabla indica la configuración de los puertos en el *switch* del piso 9 del edificio Matriz.

Tabla 37. Configuración de puertos en el *switch* "SW_PISO_9" edificio Matriz

PUERTOS *SWITCH* "SW_PISO_9"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
GigabitEthernet 1/0/25 – 1/0/47, 1/0/50 – 1/0/52	-	-	VLAN 1	-
GigabitEthernet 1/0/48	-	-	VLAN 9	-
GigabitEthernet 1/0/8,	-	-	VLAN 10	-

PUERTOS *SWITCH* "SW_PISO_9"				
Puertos	**Port-channel**	**Troncal**	**Acceso**	**Descripción**
1/0/15 - 1/0/22, 1/0/24				
GigabitEthernet 1/0/1 – 1/0/12, 1/0/14 – 1/0/24, 1/0/48	-	-	VLAN 21	-
GigabitEthernet 1/0/13	-	-	VLAN 27	-
GigabitEthernet 1/0/49	-	X	-	Hacia *switch* de core

5.1.8. Direccionamiento IP

El direccionamiento IP considera requerimientos de una VLAN de telefonía, VLAN de datos, VLAN para los access point y VLAN de servidores entre otras. La siguiente tabla indica las VLAN y su ámbito en el edificio Matriz

Tabla 38. Direccionamiento IP edificio Matriz

DIRECCIONAMIENTO IP EDIFICIO MATRIZ			
ÁMBITO	**VLAN**	**RANGO**	**DESCRIPCIÓN**
10.1.X.X/24	VLAN 1	10.1.X.X – 10.1.X.X	SERVIDORES
10.1.X.X/29	VLAN 2	10.1.X.X – 10.1.X.X	VLAN SITA
10.1.X.X/26	VLAN 4	10.1.X.X – 10.1.X.X	ADMINISTRACION
10.1.X.X/24	VLAN 5	10.1.X.X – 10.1.X.X	VLAN_INFORMATICA
10.1.X.X/24	VLAN 6	10.1.X.X – 10.1.X.X	VLAN_VENTAS
10.1.X.X/24	VLAN 7	10.1.X.X – 10.1.X.X	VLAN_RECURSOS_HUMANOS
10.1.X.X/24	VLAN 8	10.1.X.X – 10.1.X.X	VLAN_LOGISTICA
10.1.X.X/24	VLAN 9	10.1.X.X – 10.1.X.X	VLAN_FINANZAS
10.1.X.X/24	VLAN 10	10.1.X.X – 10.1.X.X	VLAN_COMERCIAL
10.1.X.X/24	VLAN 11	10.1.X.X – 10.1.X.X	VLAN_PRESIDENCIA_ASESORIAS
10.1.X.X/24	VLAN 12	10.1.X.X – 10.1.X.X	VLAN_AUDITORIA
10.1.X.X/24	VLAN 13	10.1.X.X – 10.1.X.X	MANTENIMIENTO INFORMATICA
10.1.X.X/24	VLAN 17	10.1.X.X – 10.1.X.X	Reservaciones
10.1.X.X/24	VLAN 18	10.1.X.X – 10.1.X.X	Call_Center
10.1.X.X/24	VLAN 19	10.1.X.X – 10.1.X.X	Datos_Reservas
10.1.X.X/24	VLAN 20	10.1.X.X – 10.1.X.X	ADM_NETworking
10.1.X.X/24	VLAN 21	10.1.X.X – 10.1.X.X	VLAN_CAPACITACION
10.1.X.X/24	VLAN 23	10.1.X.X – 10.1.X.X	DataFast
10.1.X.X/24	VLAN 27	10.1.X.X – 10.1.X.X	--

10.1.X.X/24	VLAN 40	10.1.X.X – 10.1.X.X	--
10.220.X.X/ 24	VLAN 220	10.220.X.X – 10.220.X.X	VLAN_VIA_XXI
10.1.X.X/24	VLAN 225	10.1.X.X – 10.1.X.X	Core – Check Point

5.1.9. Equipamiento

A continuación en la tabla se presenta el direccionamiento y contraseñas para la administración de los equipos de red de TAME EP en el edificio Matriz.

Tabla 39. Direccionamiento y contraseñas para la administración de los equipos de red edificio Matriz.

EQUIPAMIENTO EDIFICO MATRIZ					
EQUIPO	**DIRECCIÓN**	**SERVICIO**	**USERNAME**	**PASSWORD**	**ENABLE**
CH-HA	10.1.X.X	telnet/ssh	tXXe	tXXe	cXXXXXXXe
SW_CORE_MATRIZ	10.1.X.X	telnet/ssh	tXXe	tXXe	cXXXXXXXe
SW_PISO_1	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_TI	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_2	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_3	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_4	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_5_1	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_5_2	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_6	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_7_1	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_7_2	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_8_1	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_8_2	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe
SW_PISO_9	10.1.X.X	telnet/ssh	tXXe	cXXXXXXXe	cXXXXXXXe

En la tabla siguiente se muestran los modelos, imagen y versión de sistema operativo de los equipos configurados en el edificio Matriz.

Tabla 40. Modelo, imagen y versión de los equipos de red configurados en el edificio Matriz.

MODELO, IMAGEN Y VERSIÓN DE LOS EQUIPOS DE RED EDIFICIO MATRIZ			
EQUIPO	**MODELO**	**IMAGEN**	**VERSIÓN**
Edge	S4152F	MyPower S4152F_5.4.15.0	R03
SW_CORE_MATRIZ	WS-C4506-E	cat4500e-UNIVERSALK9-M	15.0(1r)SG10
SW_PISO_1	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_TI	WS-C2960S-48FPS-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_2	WS-C2960S-48FPS-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_3	WS-C2960S-24PD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_4	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_5_1	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_5_2	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_6	WS-C2960S-48FPS-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_7_1	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_7_2	WS-C2960S-24PD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_8_1	WS-C2960S-48FPD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_8_2	WS-C2960S-24PD-L	C2960S-UNIVERSALK9-M	12.2(55)SE7
SW_PISO_9	WS-C2960S-48FPS-L	C2960S-UNIVERSALK9-M	12.2(55)SE7

La siguiente imagen muestra la topología de la red conmutada implementada en el edificio Matriz.

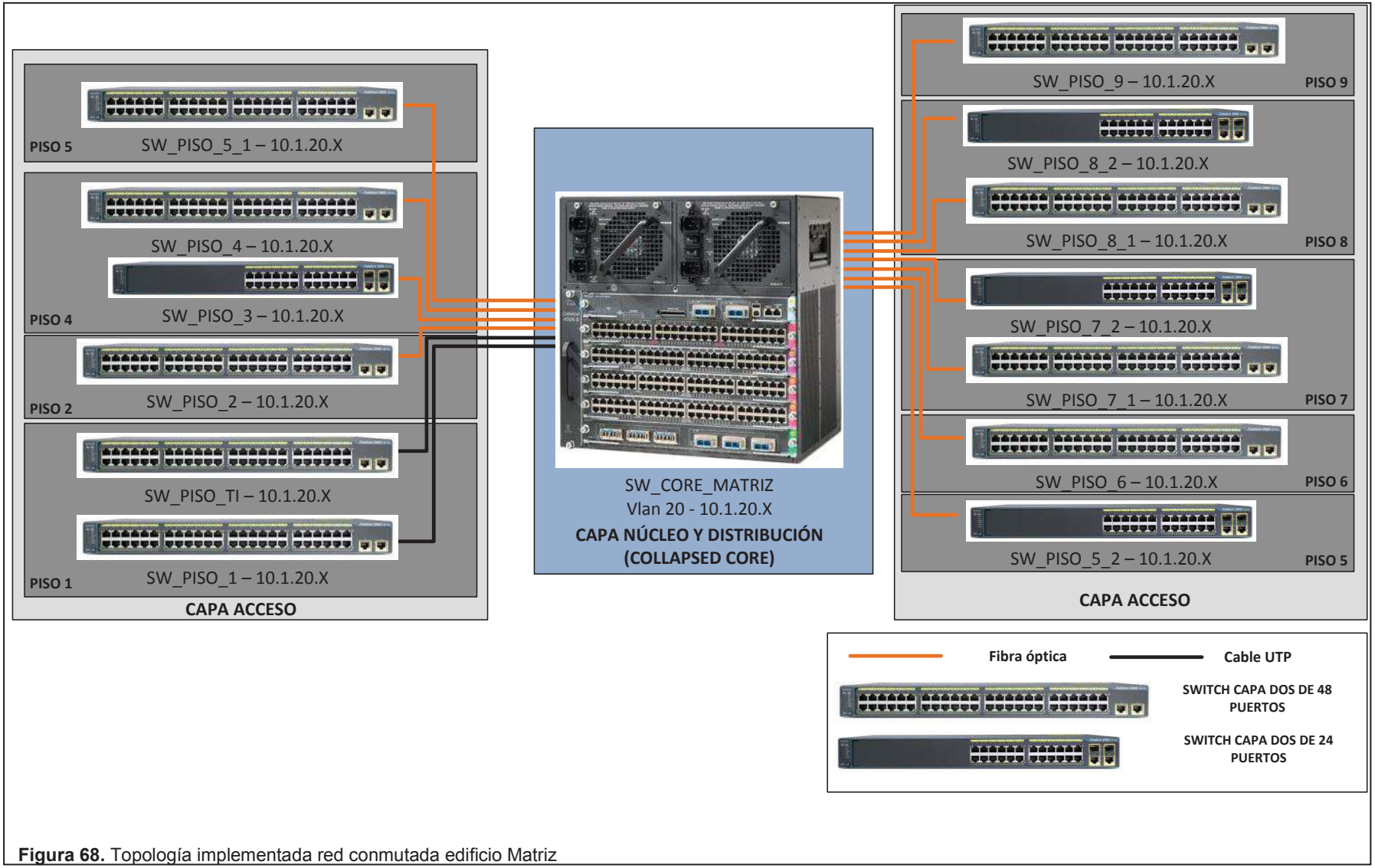


Figura 68. Topología implementada red conmutada edificio Matriz

5.2. Pruebas de funcionamiento de la red conmutada

La red conmutada se encuentra implementada y está funcionando de acuerdo al diseño para la fase uno especificado en el capítulo III. Las siguientes capturas obtenidas de la plataforma Cisco Prime Infrastructure muestran los dispositivos de *networking* funcionando y detalles específicos que nos permiten tener claro el funcionamiento actual de la red conmutada. La siguiente imagen muestra los equipos de *networking* registrados correctamente en la plataforma Cisco Prime.

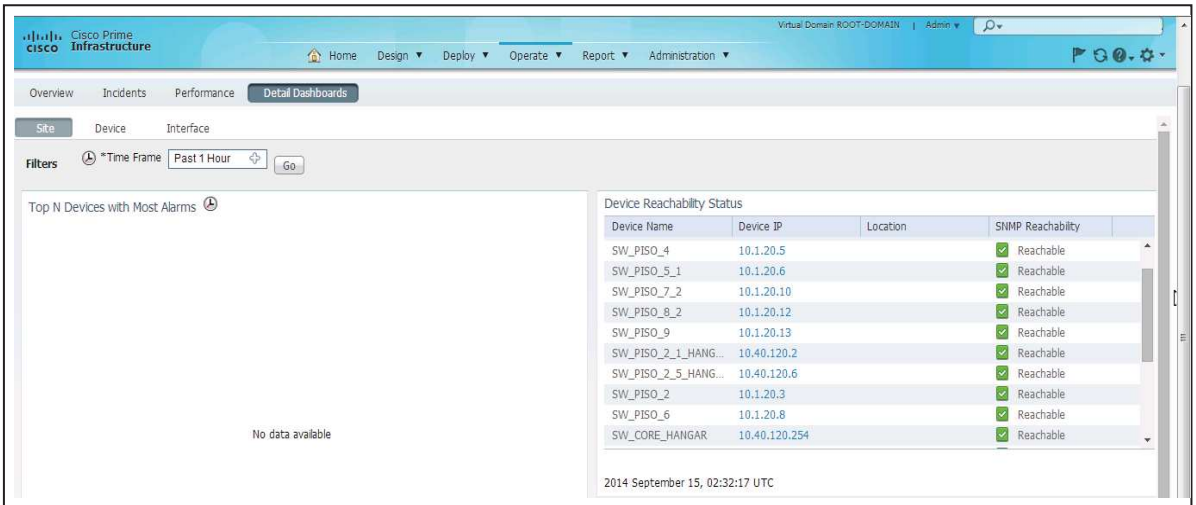


Figura 69. *Switches* registrados en la plataforma Cisco Prime

La siguiente imagen muestra los equipos de *networking* con mayor uso tanto en CPU como en memoria.

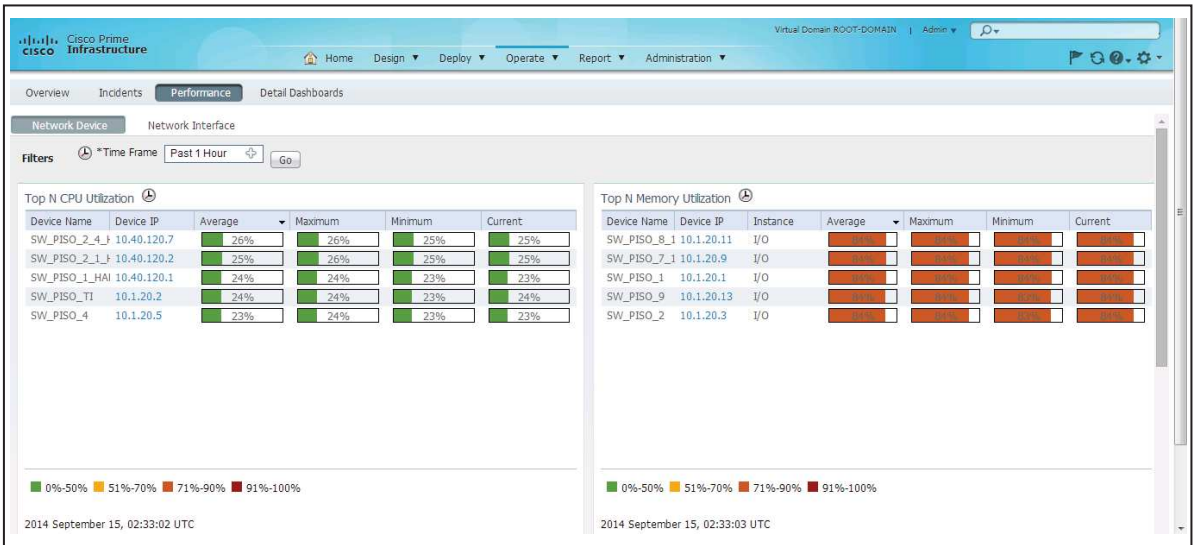


Figura 70. Estadísticas de uso de CPU y memoria

La siguiente imagen muestra detalles específicos de un *switch* implementado como la dirección IP de administración, la versión de sistema operativo, el estado de sus interfaces y la dirección MAC del *switch*.

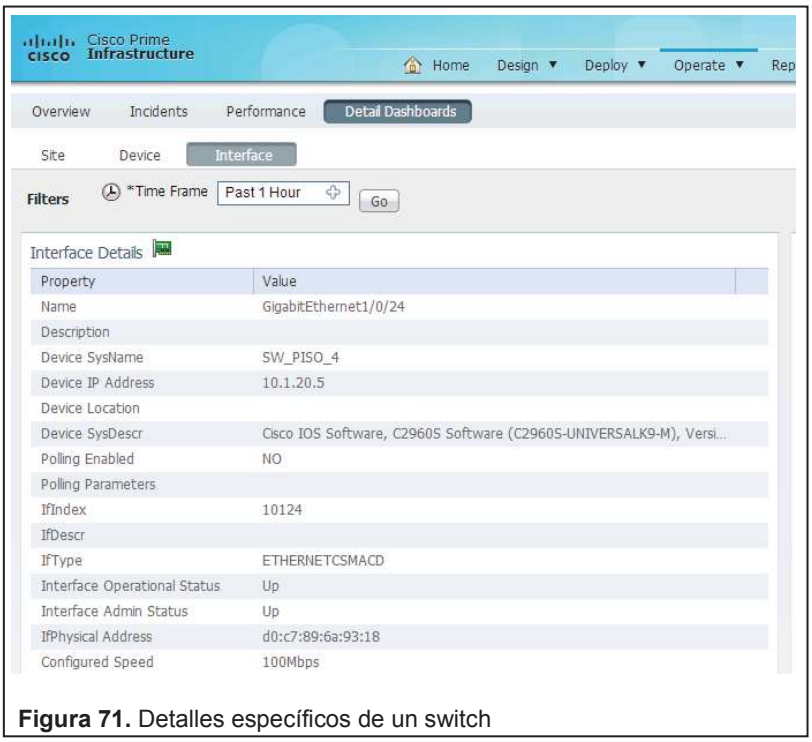


Figura 71. Detalles específicos de un switch

La siguiente imagen muestra la tendencia en el uso de la memoria y del CPU de un *switch* específico a los largo de dos semanas.

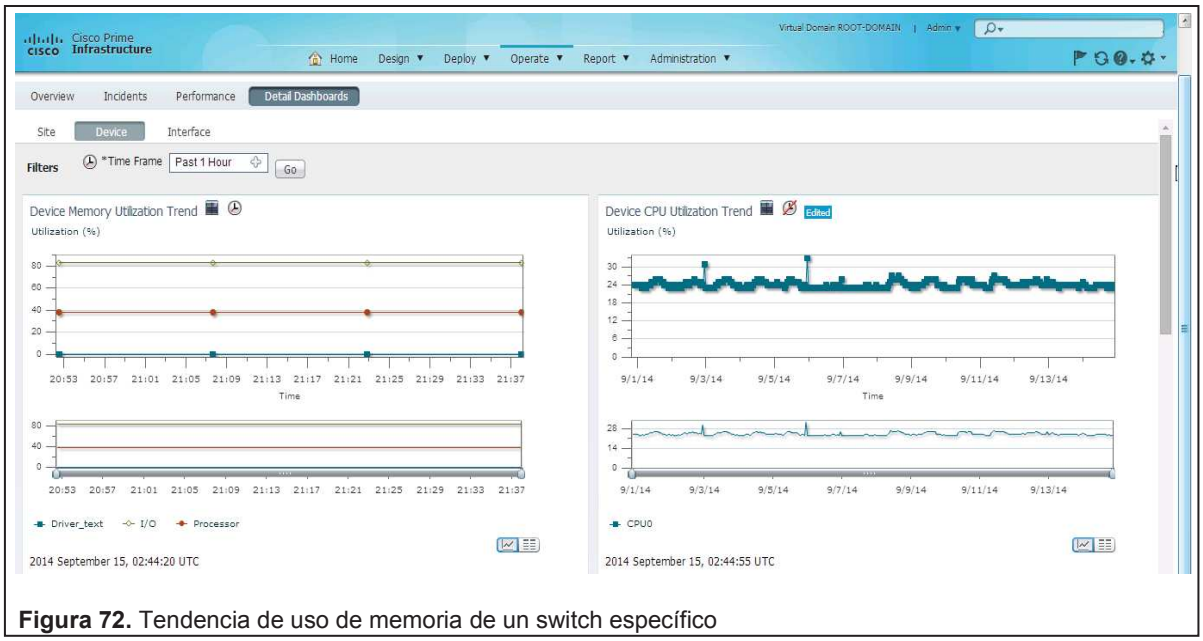


Figura 72. Tendencia de uso de memoria de un switch específico

Debido a que el *software* Cisco Packet Tracer no permite simular la tecnología VSS como se mencionó en el capítulo III, se realizó una simulación con HSRP (usando este *software* con la versión 6.0). A pesar que HSRP no tiene todas las ventajas de VSS, nos brindará una idea de la redundancia que se espera lograr a nivel de puerta de enlace predeterminada. La siguiente imagen ilustra dos *switches* de núcleo colapsado funcionando con HSRP, un *switch* de acceso que brinda servicio al piso 1 y un usuario final, como se puede observar el usuario tiene conectividad a nivel de capa 3 con la dirección IP virtual, que está asociada al *switch* SW_CORE_1.

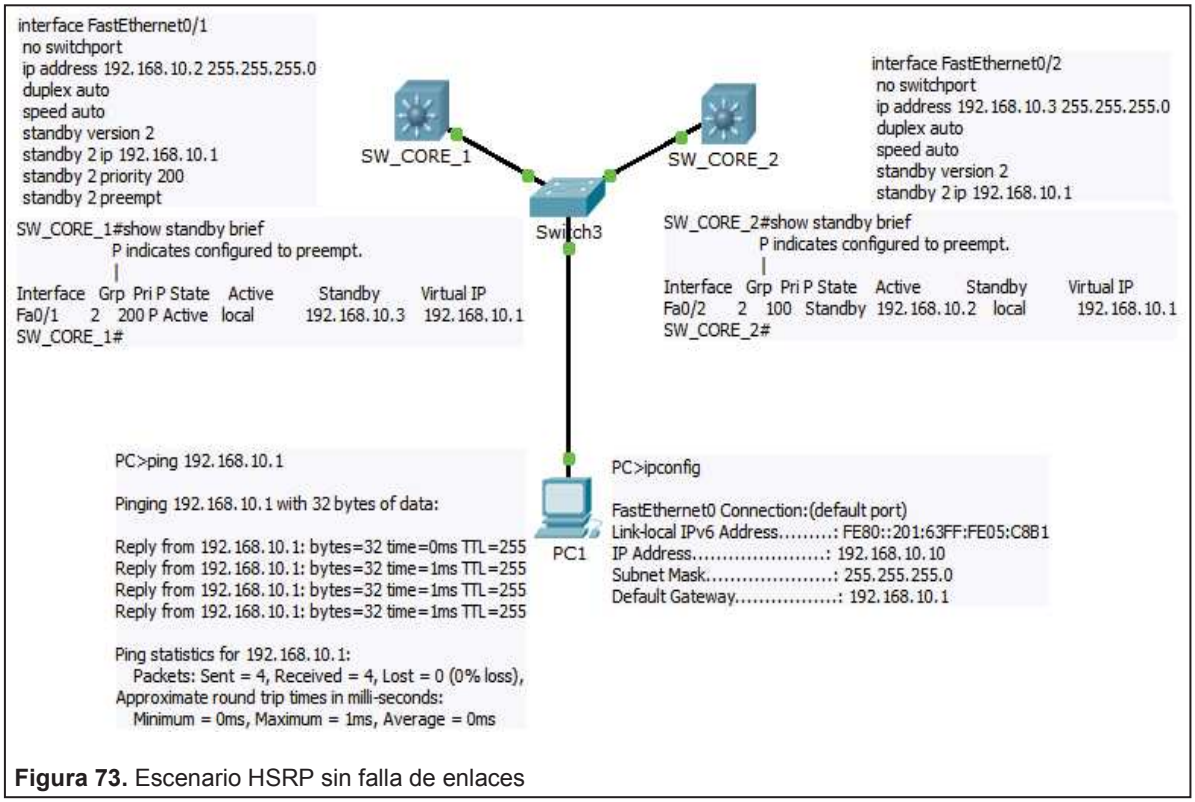


Figura 73. Escenario HSRP sin falla de enlaces

Para simular una falla en el enlace principal se deshabilitó la interfaz del *switch* SW_CORE_1 que se conecta contra el *switch* de acceso. Como se puede observar en la siguiente imagen el usuario pierde dos paquetes ICMP contra la dirección IP virtual mientras el protocolo HSRP converge, ahora la dirección IP virtual está asociada al *switch* SW_CORE_2. De esta manera se configura redundancia a nivel de puerta de enlace predeterminada y a pesar que la infraestructura de red sufrió una falla grave, para el usuario final este incidente es transparente.

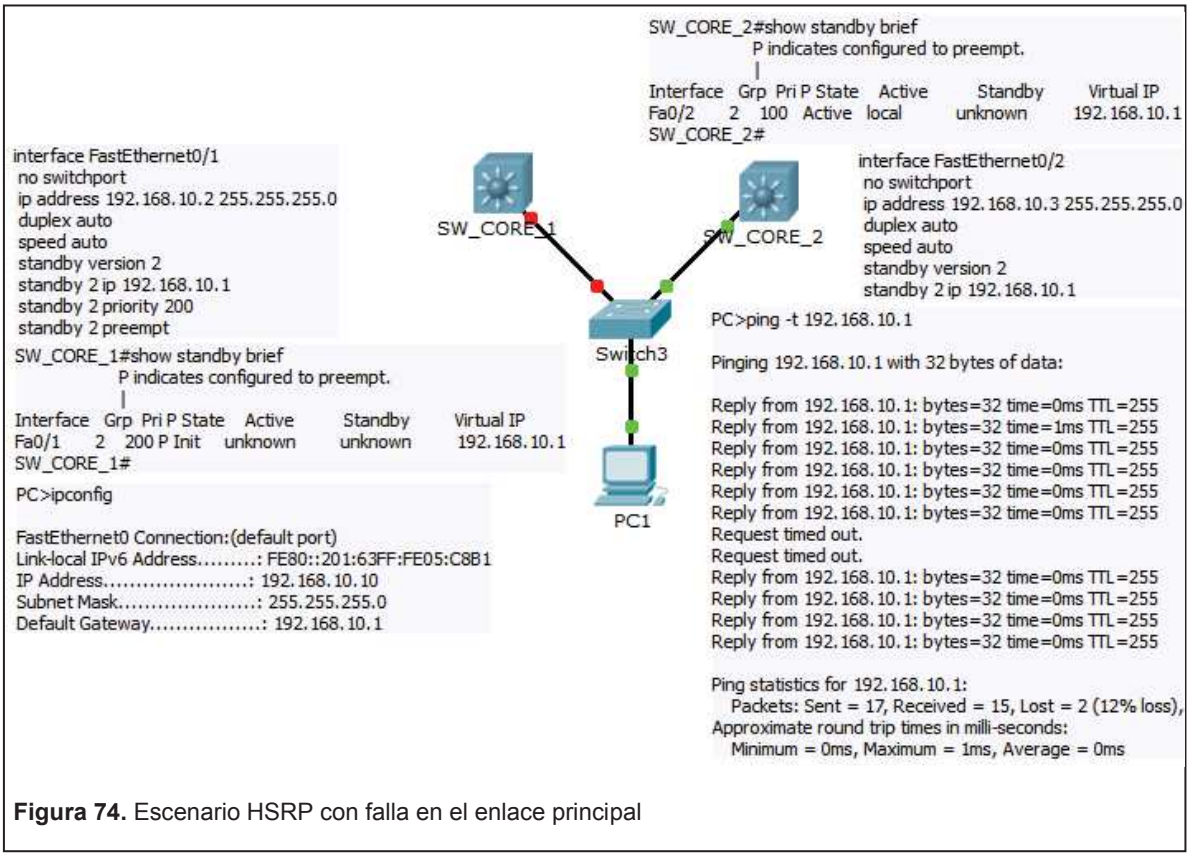


Figura 74. Escenario HSRP con falla en el enlace principal

5.3. IBNS (Servicio de red basado en identidad)

5.3.1. Introducción

De acuerdo con los requerimientos de servicios de red basado en identidad (IBNS) y del diseño propuesto en el capítulo III Cisco Secure ACS es un servidor de control de acceso, de alto rendimiento que funciona como servidor RADIUS y/o TACACS+ centralizado y además controla las funciones AAA para los usuarios que acceden a los recursos de TAME EP a través de la red.

El CSACS, permite a los administradores de red controlar el acceso de los usuarios a la red, autorizar diferentes servicios de red para usuarios o grupos de usuarios (mediante RADIUS) y mantener un registro de contabilidad de todas las acciones realizadas por los usuarios en la red (*accounting*).

Asimismo, los administradores de la red pueden usar la misma estructura AAA para gestionar (mediante TACACS+) el acceso a los equipos de *networking* activos de la red (*switches* y *router*s) y brindar distintos niveles de autorización.

Los *switches* descritos en la sección anterior tomarán el papel de autenticador en la solución IBNS.

5.3.2. Direccionamiento IP

Las VLAN y segmentos de red definidos en el capítulo III en la sección Diseño del nuevo direccionamiento IP están creadas en el *switch* de núcleo colapsado, al igual que su respectiva interface VLAN y su respectivo pool DHCP en el Microsoft Server 2012. Para cada nueva VLAN se creó un objeto network en el *firewall* de última generación marca Check Point y se le asignó al grupo “GRP_TAME” que tiene permisos de navegación. Las nuevas rutas para las nuevas VLANs también están agregadas en el equipo Check Point.

5.3.3. Configuraciones generales

El sistema CSACS está virtualizado en los *blade* IBM que contiene a la mayoría de servicios principales y está ubicado en la VLAN de servidores de su

respectiva localidad. Los requerimientos mínimos para instalar el sistema operativo del CSACS en una máquina virtual son:

CPU:	2 CPUs
Memory:	4GB RAM
Hard Risk:	Mínimo de 60GB máximo de 700GB
NIC:	1 interfaz Gibabit dedicada
Hypervisor:	VMware ESXi 5.0

5.3.4. *High availability*

El sistema de IBNS está configurado en alta disponibilidad (*high availability*), es decir se tiene configurado dos CSACSs para que exista redundancia en el servicio IBNS y se alcance un tiempo de disponibilidad aceptable. El CSACS principal (*primary*) está virtualizado en el *blade* IBM en el edifico Matriz y se encuentra ubicado en la VLAN 1, mientras que el CSACS secundario (*secondary*) está virtualizado en el *blade* IBM en Tababela (Hangar) y se encuentra ubicado en la VLAN 15.

Está configurado para que todos los equipos de *networking* activos y usuarios del edifico Matriz se autentiquen, autoricen y se contabilicen (*accounting*) contra el CSACS ubicado en Matriz (*Primary*) y en caso de que el CSACS primario no esté disponible se autentiquen, autoricen y se contabilice (*accounting*) contra el CSACS secundario ubicado en Tababela.

En lo que respecta a los equipos de *networking* activos y usuarios en Tababela está configurado para que todos los equipos se autentiquen, autoricen y se contabilicen (*accounting*) contra el CSACS ubicado en Tababela/Hangar (*Secondary*) y en caso de que el CSACS secundario no esté disponible se autentiquen, autoricen y se contabilice (*accounting*) contra el CSACS primario ubicado en Matriz, está configurado de esta manera para que no se consuma el ancho de banda de la WAN.

Cabe recalcar que en un modelo de alta disponibilidad el CSACS secundario copia todas las configuraciones del CSACS primario, es decir la base de datos del CSACS primario se replica en el CSACS secundario.

5.3.5. Configuraciones principales

Las configuraciones principales del CSACS principal se detallan a continuación:

IP:	10.1.X.X/24
Gateway:	10.1.X.X
Dominio:	tame-ep.net.ec
Nombre:	acs-uio
Usuario web:	AXXXXXXn
Password web:	TXXXXXXX1
DNS/NTP:	10.1.X.X
Zona Horaria:	América/Guayaquil

Las configuraciones principales del CSACS secundario se detallan a continuación:

IP:	10.40.X.X/24
Gateway:	10.40.X.X
Dominio:	tame-ep.net.ec
Nombre:	acs-naiq
Usuario web:	AXXXXXXn
Password web:	TXXXXXXX1
DNS/NTP:	10.1.X.X
Zona Horaria:	América/Guayaquil

5.3.6. Configuraciones específicas

En esta sección se especificarán las configuraciones necesarias para el despliegue de IBNS a nivel corporativo en TAME EP.

5.3.6.1. Recursos de red

En esta sección se configuran los parámetros básicos para el despliegue de la solución IBNS como son localidad, tipo de dispositivo y dispositivos de red.

5.3.6.2. Localidad

Se configuró 4 localidades como se ilustra en la siguiente figura.

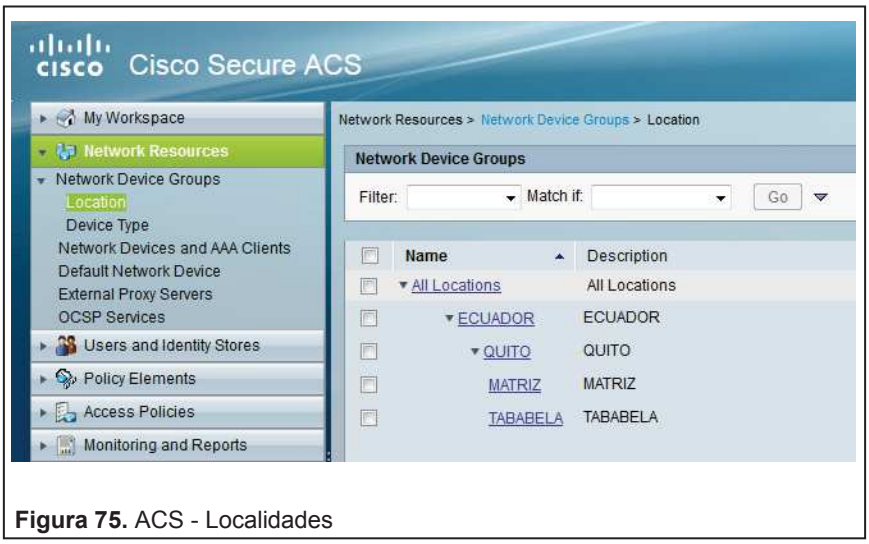


Figura 75. ACS - Localidades

5.3.6.3. Tipo de dispositivo

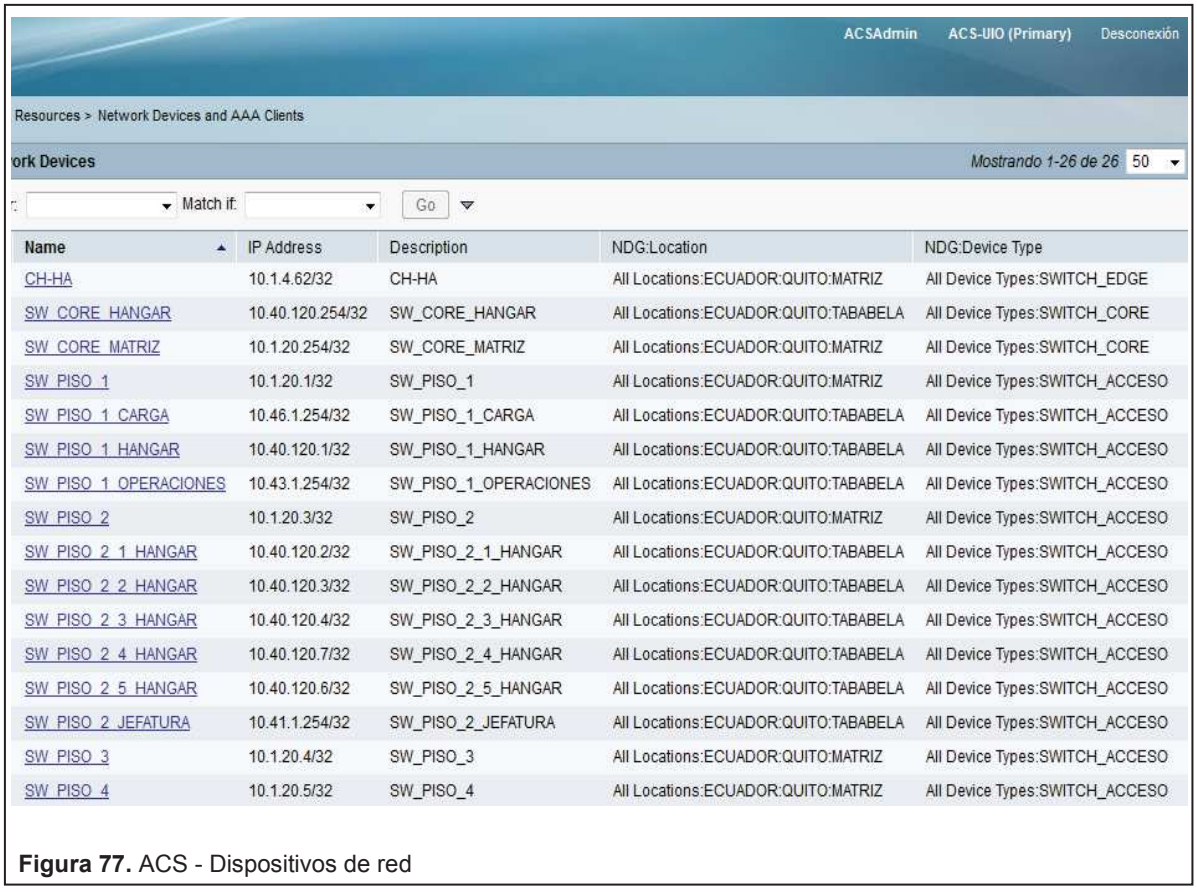
Se configuró 5 tipos de dispositivo como se ilustra en la siguiente figura.

Figura 76. ACS - Tipo de dispositivo

5.3.6.4. Dispositivos de red y clientes AAA

Se configuró 26 dispositivos de red como se ilustra en la siguiente figura, que incluyen todos los *switches* de la red (acceso y núcleo colapsado).

Cada objeto está definido con su dirección IP de administración, en el edificio Matriz la VLAN de administración es la 20 mientras que en Tababela es la VLAN 120. La PSK (Pre-shared Key) es: CXXXoXXXeXX3, tanto para RADIUS como para TACACS+.



Name	IP Address	Description	NDG:Location	NDG:Device Type
CH-HA	10.1.4.62/32	CH-HA	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_EDGE
SW_CORE_HANGAR	10.40.120.254/32	SW_CORE_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_CORE
SW_CORE_MATRIZ	10.1.20.254/32	SW_CORE_MATRIZ	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_CORE
SW_PISO_1	10.1.20.1/32	SW_PISO_1	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_ACCESO
SW_PISO_1_CARGA	10.46.1.254/32	SW_PISO_1_CARGA	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_1_HANGAR	10.40.120.1/32	SW_PISO_1_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_1_OPERACIONES	10.43.1.254/32	SW_PISO_1_OPERACIONES	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2	10.1.20.3/32	SW_PISO_2	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_ACCESO
SW_PISO_2_1_HANGAR	10.40.120.2/32	SW_PISO_2_1_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2_2_HANGAR	10.40.120.3/32	SW_PISO_2_2_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2_3_HANGAR	10.40.120.4/32	SW_PISO_2_3_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2_4_HANGAR	10.40.120.7/32	SW_PISO_2_4_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2_5_HANGAR	10.40.120.6/32	SW_PISO_2_5_HANGAR	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_2_JEFATURA	10.41.1.254/32	SW_PISO_2_JEFATURA	All Locations:ECUADOR:QUITO:TABABELA	All Device Types:SWITCH_ACCESO
SW_PISO_3	10.1.20.4/32	SW_PISO_3	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_ACCESO
SW_PISO_4	10.1.20.5/32	SW_PISO_4	All Locations:ECUADOR:QUITO:MATRIZ	All Device Types:SWITCH_ACCESO

Figura 77. ACS - Dispositivos de red

5.3.7. Archivo de identidades y usuarios

En esta sección se configuran otros parámetros necesarios para el despliegue de la solución IBNS como son grupos de identidad, usuarios internos y *hosts*.

5.3.7.1. Grupos de identidad

Se configuró 3 grupos de identidad como se ilustra en la siguiente figura

Figura 78. ACS - Grupos de identidad

5.3.7.2. Archivos de identidades internas

En esta sección se configura los objetos internos del ACS.

5.3.7.3. Usuarios

Se configuró 2 usuarios internos como se ilustra en la siguiente figura. Las credenciales del usuario administrador son:

Username: adXXXXXtXXXor

Password: ciXXXtXXe

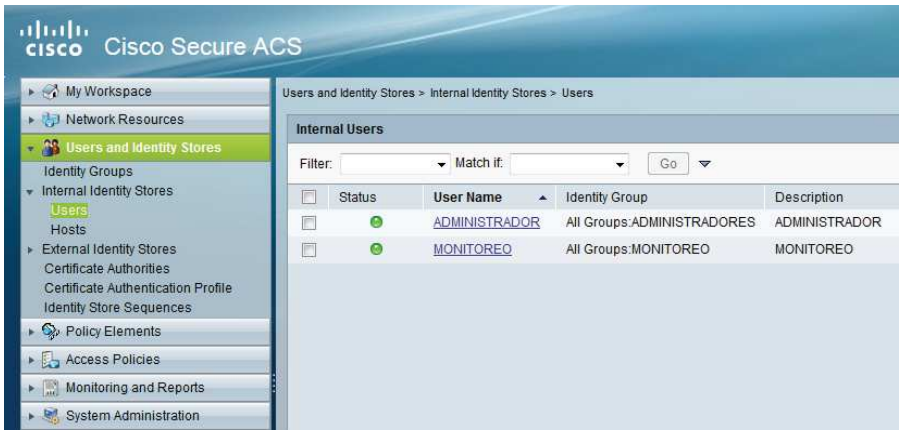


Figura 79. ACS - Usuarios internos

5.3.7.4. *Hosts*

Se configuró 215 *hosts* con su respectiva dirección MAC para autenticación vía MAB (*MAC Authentication Bypass*). Se muestra un extracto de la configuración en la siguiente figura.

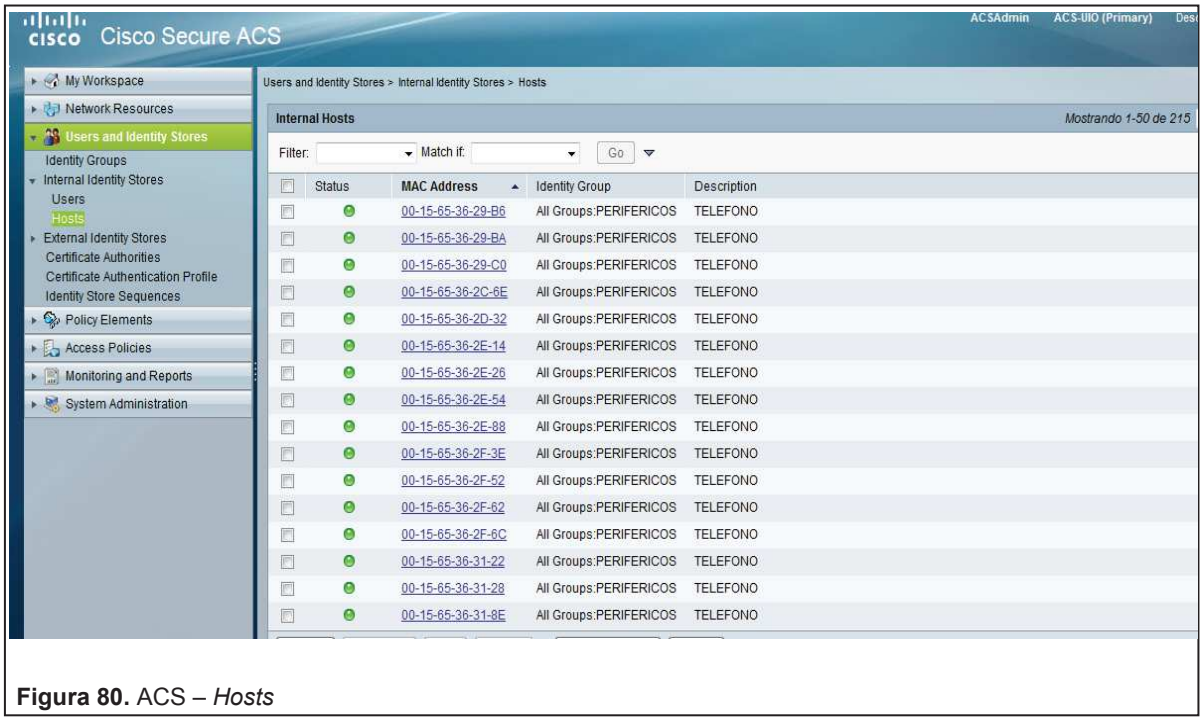


Figura 80. ACS – *Hosts*

5.3.7.5. Directorio activo

En esta sección se configura la integración contra el directorio activo para poder dar perfiles de autorización dependiendo de a qué grupo de seguridad pertenece el usuario. La siguiente figura ilustra la integración tanto del ACS primario como del ACS secundario contra el directorio activo.

Figura 81. Integración Active Directory

5.3.7.6. Secuencia de base de datos de identidad

Esta sección indica el orden en que se buscará las credenciales de los usuarios para la autenticación. La secuencia de las bases de datos de identidad es: usuarios internos, Active Directory y dispositivos internos (*internal hosts*). La siguiente figura ilustra la secuencia de base de datos de identidad.

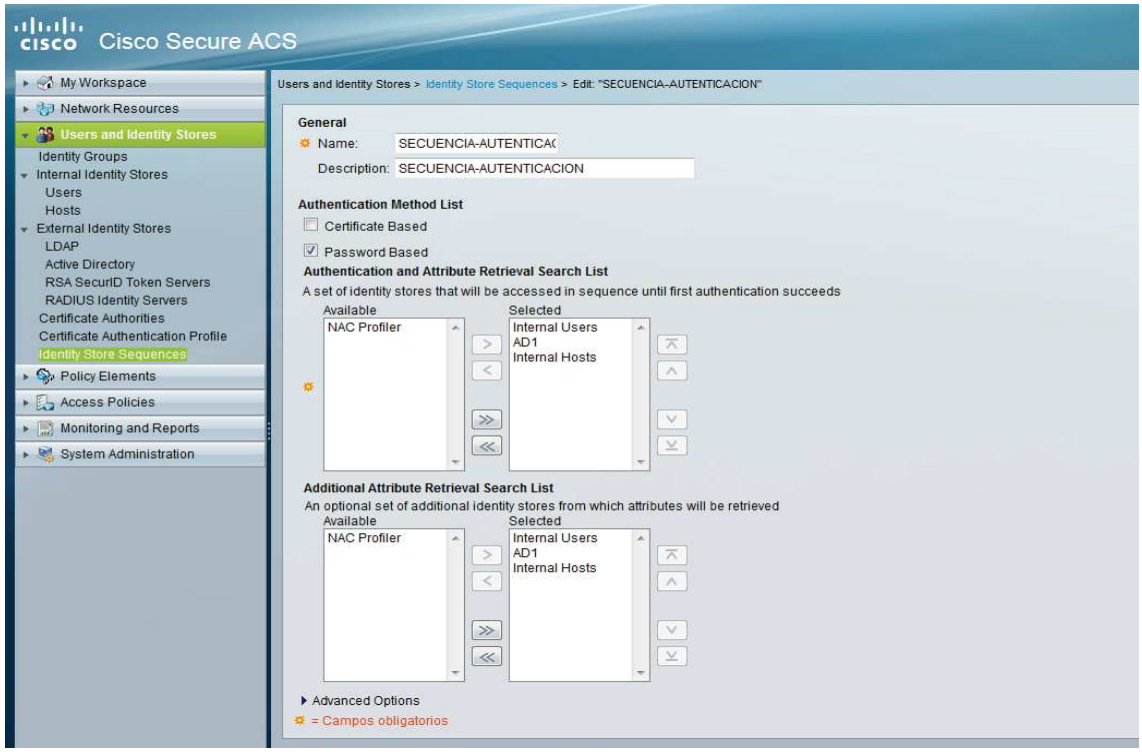


Figura 82. ACS – Secuencia de base de datos de identidad

5.3.8. Elementos de la política

En esta sección se configuran los perfiles de autorización y los perfiles *Shell*.

5.3.8.1. Perfiles de autorización

La siguiente figura muestra los perfiles de autorización creados.

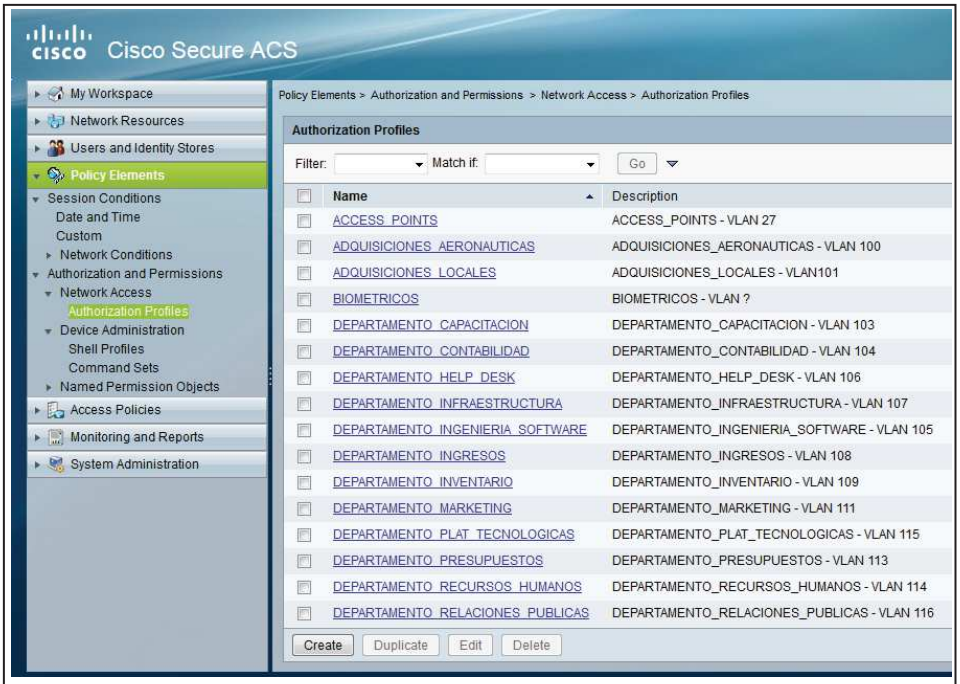


Figura 83. ACS - Perfiles de autorización

5.3.8.2. Perfiles *shell*

La siguiente figura muestra los perfiles *Shell* creados. El perfil de ADMINISTRADOR_NETWORKING tiene privilegios nivel 15 (todos los comandos), mientras que el perfil MONITOREO_NETWORKING tiene privilegios nivel 3 (*show running-config, show startup-config*).

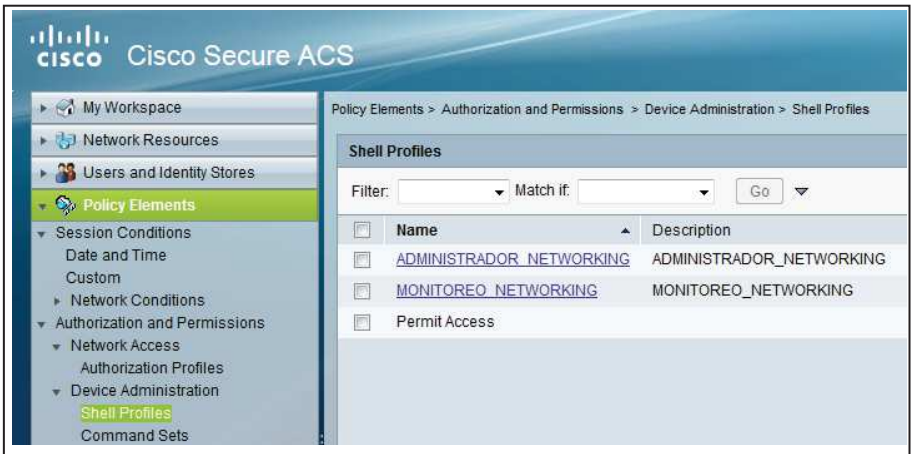


Figura 84. ACS - Perfiles shell

5.3.9. Políticas de acceso

Esta sección es la más importante y es donde se configura la forma en que se van a autenticar los usuarios, los equipos de *networking* y los equipos que no hablen IEEE 802.1X (MAB) y donde se integran todos los objetos creados anteriormente.

5.3.9.1. Servicios de acceso

La siguiente figura ilustra los 3 servicios de acceso creados que son: MAB, RADIUS y TACACS.

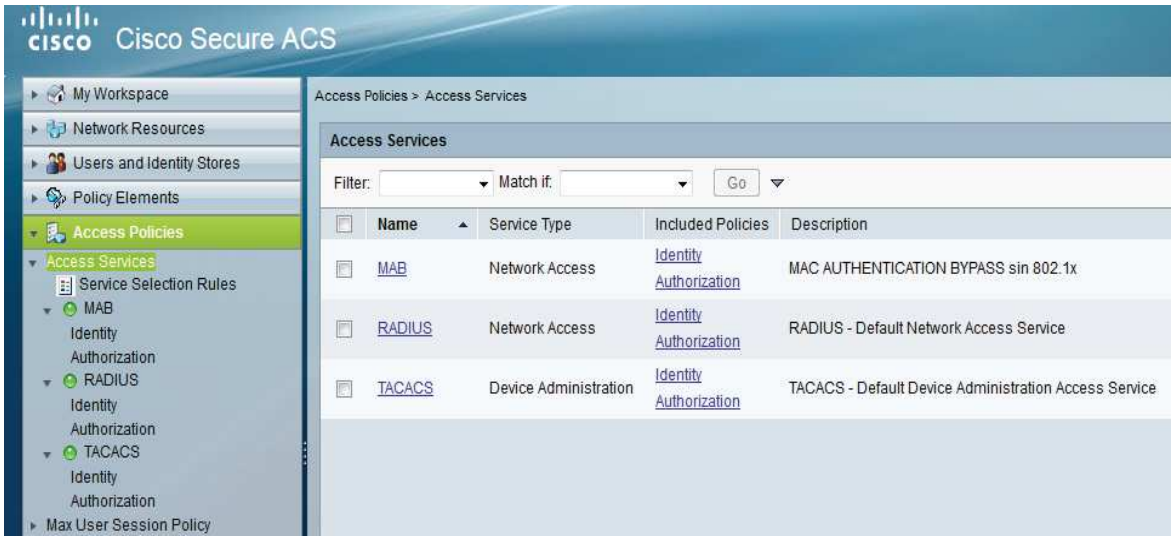


Figura 85. ACS - Servicios de acceso (MAB, RADIUS Y TACACS)

5.3.9.1.1. Reglas de selección de servicio

La siguiente figura ilustra las 4 reglas de selección de servicio.

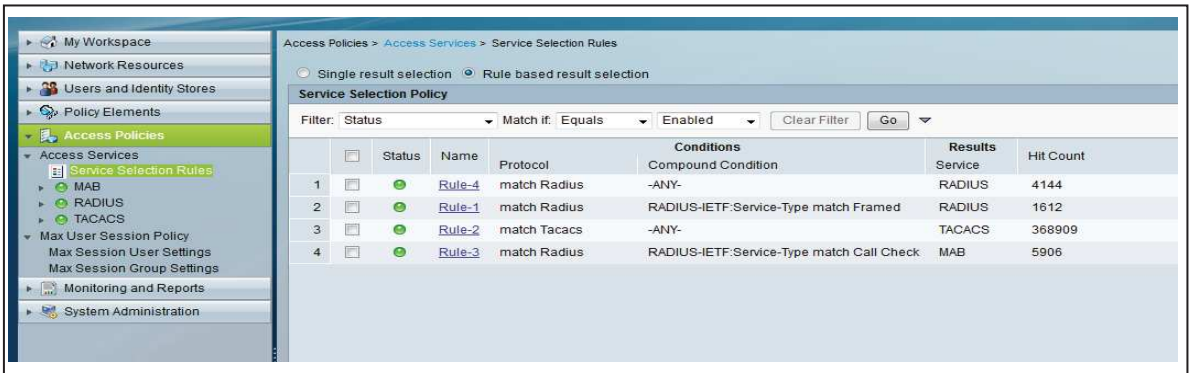


Figura 86. ACS - Reglas de selección de servicio

5.3.9.1.2. MAB

5.3.9.1.2.1. *Identity*

La siguiente imagen ilustra la identidad de la política de acceso MAB

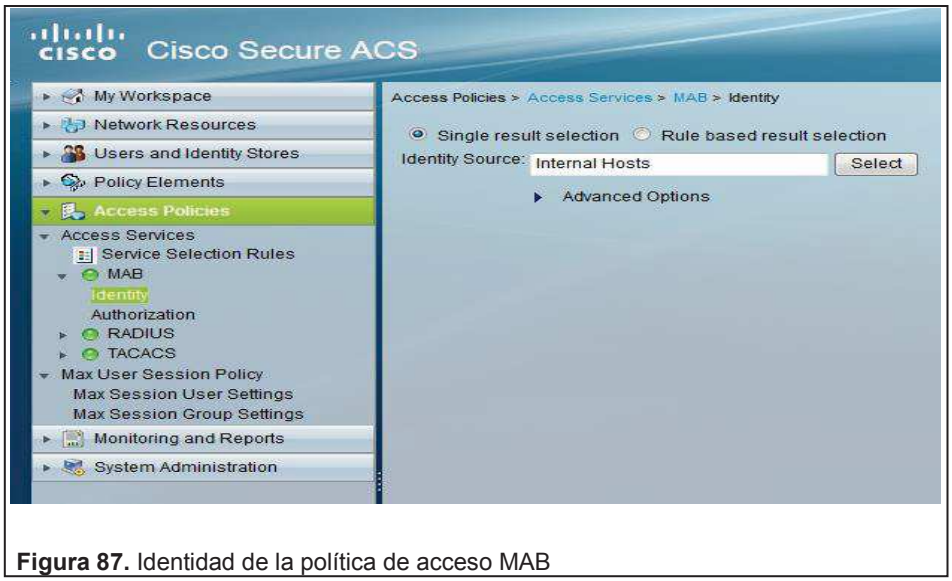


Figura 87. Identidad de la política de acceso MAB

5.3.9.1.2.2. *Authorization*

La siguiente imagen ilustra la autorización de la política de acceso MAB

Figura 88. Autorización de la política de acceso MAB

5.3.9.1.3. RADIUS

5.3.9.1.3.1. *Identity*

La siguiente imagen ilustra la identidad de la política de acceso RADIUS.

Figura 89. Identidad de la política de acceso RADIUS

5.3.9.1.3.2. *Authorization*

La siguiente imagen ilustra la autorización de la política de acceso RADIUS

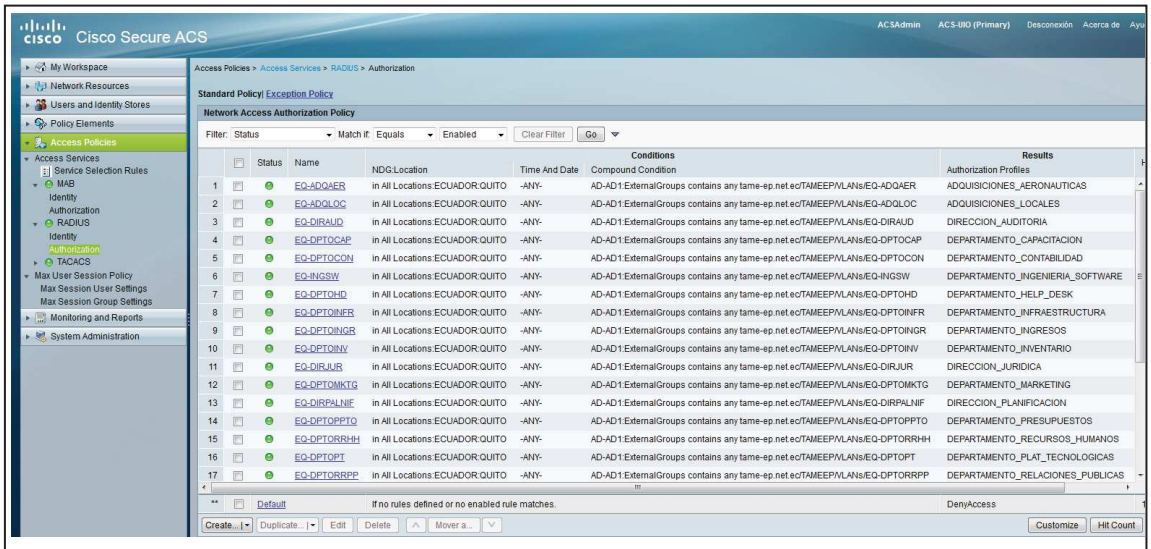


Figura 90. Autorización de la política de acceso RADIUS

5.3.9.1.4. TACACS+

5.3.9.1.4.1. *Identity*

La siguiente imagen ilustra la identidad de la política de acceso TACACS+.

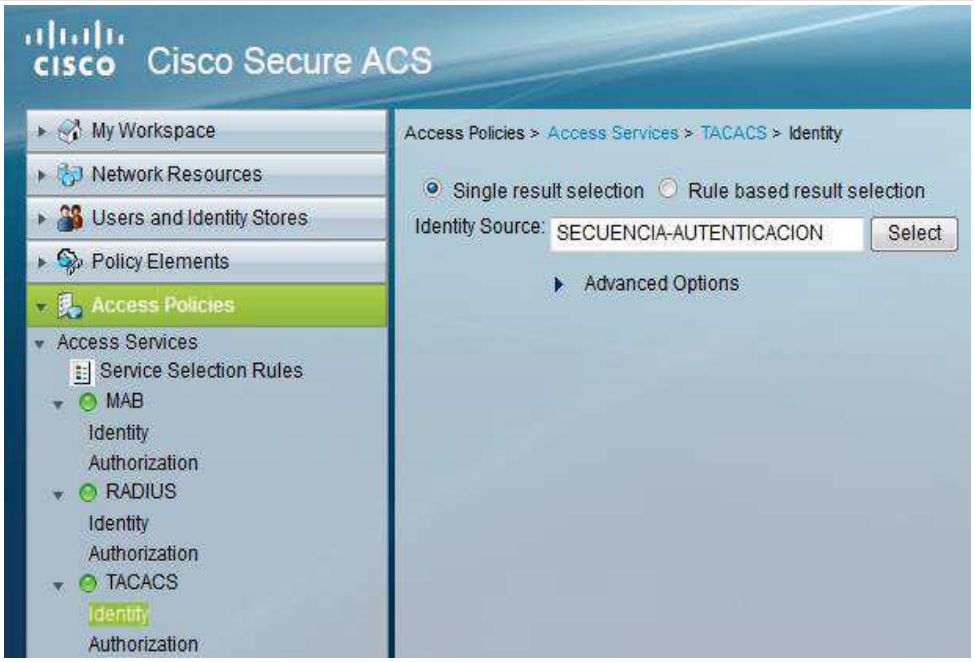


Figura 91. Identidad de la política de acceso TACACS+

5.3.9.1.4.2. *Authorization*

La siguiente imagen ilustra la autorización de la política de acceso TACACS+

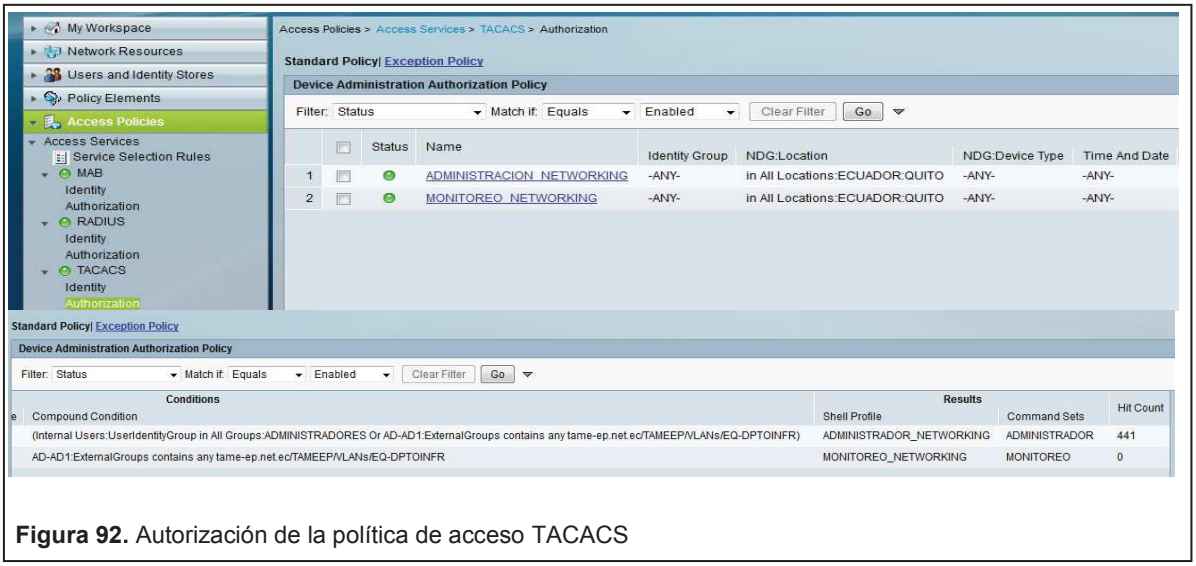


Figura 92. Autorización de la política de acceso TACACS

5.3.10. Resumen funcionamiento IBNS

5.3.10.1. Resumen funcionamiento TACACS+

El protocolo TACACS+ servirá para la autenticación y la autorización para la administración de los equipos de *networking*. Como ya se describió anteriormente la secuencia está configurada para que el CSACS primero busque en su base de datos interna y luego en una base de datos externa (*Active Directory*).

Solo los usuarios que pertenecen al grupo de seguridad Plataformas Tecnológicas podrán acceder a la configuración de los equipos de *networking*. Si se pierde la conexión contra el *Active Directory* existen dos usuarios creados en el CSACS para la administración de los equipos. En caso de que se pierda conectividad contra el CSACS están creados usuarios locales dentro de cada *switch* para la administración remota.

5.3.10.2. Resumen funcionamiento RADIUS

El protocolo RADIUS servirá para la autenticación y la autorización de los usuarios finales. En resumen si un usuario pertenece a una grupo de seguridad específico el puerto al cual está conectado ese usuario pasará dinámicamente a pertenecer a la VLAN que se haya configurado para ese grupo de seguridad. Por ejemplo, el usuario Daniel Quinatoa, que pertenece al grupo de seguridad Departamento de Infraestructura, el momento que ingrese sus credenciales en cualquier computadora que esté dentro del dominio tame-ep.net.ec, el puerto al que esté conectado esa máquina pasará a la VLAN de datos 107 de manera automática. La siguiente tabla indica que VLAN está asignada a cada grupo de seguridad del directorio activo, en otras palabras que VLAN se asignará a cada usuario.

Tabla 41. Resumen funcionamiento RADIUS

RESUMEN FUNCIONAMIENTO RADIUS		
VLAN	**DEPARTAMENTO**	**NOMBRE DEL GRUPO DE SEGURIDAD**
VLAN100	Departamento de Adquisiciones Aeronáuticas	EQ-ADQAER

VLAN101	Departamento de Adquisiciones Locales	EQ-ADQLOC
VLAN102	Dirección de Auditoría	EQ-DIRAUD
VLAN103	Departamento de Capacitación	EQ-DPTOCAP
VLAN104	Departamento de Contabilidad	EQ-DPTOCON
VLAN105	Departamento de Ingeniería de Software	EQ-INGSW
VLAN106	Departamento de Help Desk	EQ-DPTOHD
VLAN107	Departamento de Infraestructura	EQ-DPTOINFR
VLAN108	Departamento de Ingresos	EQ-DPTOINGR
VLAN109	Departamento de Inventarios	EQ-DPTOINV
VLAN110	Dirección Jurídica	EQ-DIRJUR
VLAN111	Departamento de Marketing	EQ-DPTOMKTG
VLAN112	Dirección de Planificación	EQ-DIRPALNIF
VLAN113	Departamento de Presupuesto	EQ-DPTOPPTO
VLAN114	Departamento de Recursos Humanos	EQ-DPTORRHH
VLAN115	Departamento de Plataformas Tecnológicas	EQ-DPTOPT
VLAN116	Departamento de Relaciones Públicas	EQ-DPTORRPP
VLAN117	Departamento de Renovación de Flota	EQ-RENOFTA
VLAN118	Departamento de Reservaciones	EQ-DPTORSVA
VLAN119	Departamento de Revenue Management	EQ-DPTORM
VLAN120	Departamento de Seguros	EQ-DPTOSEG
VLAN121	Departamento de Tesorería	EQ-DPTOTES
VLAN122	Departamento de Ventas	EQ-DPTOVEN
VLAN123	Gerentes EQ	EQ-GERENTES
VLAN124	Invitados	EQ-INVITADOS
VLAN125	Usuarios Deshabilitados	EQ-CESADOS

5.3.10.3. Agentes RADIUS y TACACS+ en los *switches* Cisco

Para que los *switches* puedan autenticar los usuarios contra el CSACS vía RADIUS y que los *switches* se autentiquen vía TACACS+ contra el CSACS se deben configurar los comandos que se describen a continuación, en otras palabras para que el *switch* pueda interpretar los VSA (*Vendor Specific Attributes*) que son enviados desde el servidor AAA (CSACS).

5.3.10.3.1. Configuraciones generales

La siguiente tabla muestra los comandos que se configuraron en el modo de configuración global en el *switch* y para qué sirve cada comando.

Tabla 42. Comandos generales RADIUS y TACACS+

COMANDOS GLOBALES AGENTES RADIUS Y TACACS+	
COMANDOS	**DESCRIPCIÓN**
aaa new-model	Habilita de manera global la autenticación, autorización y la contabilidad (*accounting*)
aaa authentication login default group tacacs+ local	Crea una lista de métodos de autenticación basada en TACACS+, primero trata de autenticar usando el servidor TACACS+, si este método devuelve un error (no si falla la autenticación) pasa al método de autenticación local (usuarios locales).
aaa authentication dot1x default group radius	Crea una lista de métodos de autenticación basada en 802.1X
aaa authorization exec default group tacacs+ local	Usado para configurar la lista de métodos de autorización por defecto para el acceso al modo de usuario privilegiado, primero busca autorización en el servidor TACACS+ si este método devuelve un error pasa al método de autorización local (comandos locales).
aaa authorization network default group radius	Requerido para la asignación de VLANs y ACLs.
aaa accounting exec default start-stop group tacacs+	Habilita la contabilidad para TACACS+
aaa accounting network default start-stop group radius	Habilita la contabilidad para RADIUS
dot1x system-auth-control	Habilita globalmente la autenticación basada en 802.1X
tacacs-server host 10.1.X.X key CXsXXTXXeXX3	Especifica la dirección IP del servidor TACACS+ primario y la llave pre compartida
tacacs-server host 10.40.X.X key CXsXXTXXeXX3	Especifica la dirección IP del servidor TACACS+ secundario y la llave pre compartida
tacacs-server directed-request	Permite especificar contra qué servidor TACACS+ me quiero autenticar. Sin este comando el equipo autenticador envía las credenciales a los servidores en el orden que estén configurados.
radius-server host 10.1.X.X auth-port 1645 acct-port 1646 key CXsXXTXXeXX3	Especifica la dirección IP del servidor RADIUS primario, los puertos y la clave pre compartida
radius-server host 10.40.X.X auth-port 1645 acct-port 1646 key CXsXXTXXeXX3	Especifica la dirección IP del servidor RADIUS secundario, los puertos y la clave pre compartida

radius-server vsa send accounting	Permite la comunicación usando el atributo “cisco-av-pair” para contabilidad
radius-server vsa send authentication	Permite la comunicación usando el atributo “cisco-av-pair” para autenticación
ip radius source-interface vlan XX	Especifica la dirección IP origen del paquete RADIUS que se enviará hacia el servidor RADIUS
ip tacacs source-interface vlan XX	Especifica la dirección IP origen del paquete TACACS+ que se enviará hacia el servidor TACACS
username aXXXn privilege 15 password ciXXXtXXe	Crea un usuario local con privilegio nivel 15 para en el caso de que se pierda conectividad contra el CSACS igual se pueda ingresar al *switch*

5.3.10.3.2. Configuraciones por puerto

La siguiente tabla muestra los comandos que se deben configurar en el modo de configuración específica dentro de cada interfaz del *switch* y para qué sirve cada comando.

Tabla 43. Comandos específicos RADIUS y TACACS+

COMANDOS ESPECÍFICOS AGENTES RADIUS Y TACACS+	
COMANDOS	**DESCRIPCIÓN**
switchport mode access	Configura el puerto en modo acceso
switchport access vlan X	Específica a qué VLAN pertenece el puerto, esta configuración es necesaria para realizar escritorio remoto
switchport voice vlan 40	Especifica la VLAN de voz (VoIP)
authentication event fail action authorize vlan 90	Especifica la acción si la autenticación falla, para que la autenticación falle el usuario final debe ingresar contraseñas incorrectas 3 veces. En este caso coloca el puerto del *switch* en la VLAN 90 (VLAN restringida) que solo tiene acceso al servidor DHCP
authentication event server dead action authorize vlan 90	Sirve para configurar una VLAN de datos crítica (VLAN 90) en caso de que el servidor AAA (CSACS) deje de funcionar
authentication event no-response action authorize vlan 90	Sirve para configurar una VLAN de datos de invitados (VLAN 90) en caso de que el cliente final no envíe las credenciales 802.1X o no soporte 802.1X
authentication event server alive action reinitialize	Reinicializa una sesión autorizada cuando un servidor AAA (CSACS) que estaba inalcanzable esté disponible
authentication host-mode multi-domain	Habilita un solo teléfono IP en el dominio de voz y varios clientes en el dominio de

	datos
authentication open	Habilita la pre-autenticación en acceso abierto (sin restricciones) y no ejecuta ningún tipo de autorización. El nivel de autorización siempre es *open*, independiente de si la autenticación es exitosa o no. SOLO SE USA PARA LA ETAPA INICIAL DE MONITOREO.
authentication order mab dot1x	Especifica el orden de los métodos de autenticación usados, en este caso primero es MAB y luego 802.1X
authentication priority dot1x mab	Especifica la prioridad de los métodos de autenticación usados, en este caso primero es 802.1X y luego MAB
authentication port-control auto	Habilita la autenticación basada en puerto en la interfaz
authentication violation replace	Habilita el puerto para remover la sesión actual e iniciar otra sesión de autenticación cuando se conecta un nuevo dispositivo
mab	Habilita MAB
dot1x pae authenticator	Habilita la autenticación 802.1X en la interfaz
spanning-tree portfast	Habilita *spanning-tree portfast* en la interfaz

5.3.10.4. Pruebas de funcionamiento del sistema IBNS

5.3.10.4.1. TACACS+

Todas las pruebas fueron satisfactorias al momento de ingresar a los equipos de *networking*. Se probó que si no existe conectividad contra el *Active Directory* se puede ingresar al equipo de networking usando las credenciales de los usuarios creados en el ACS. Además que si no existe conectividad contra el ACS se puede ingresar al equipo de *networking* usando los usuarios internos creados en cada equipo de *networking*. La siguiente imagen muestra los registros (*logs*) del ACS donde se puede apreciar la autenticación exitosa vía TACACS+ para la administración de los *switches*.

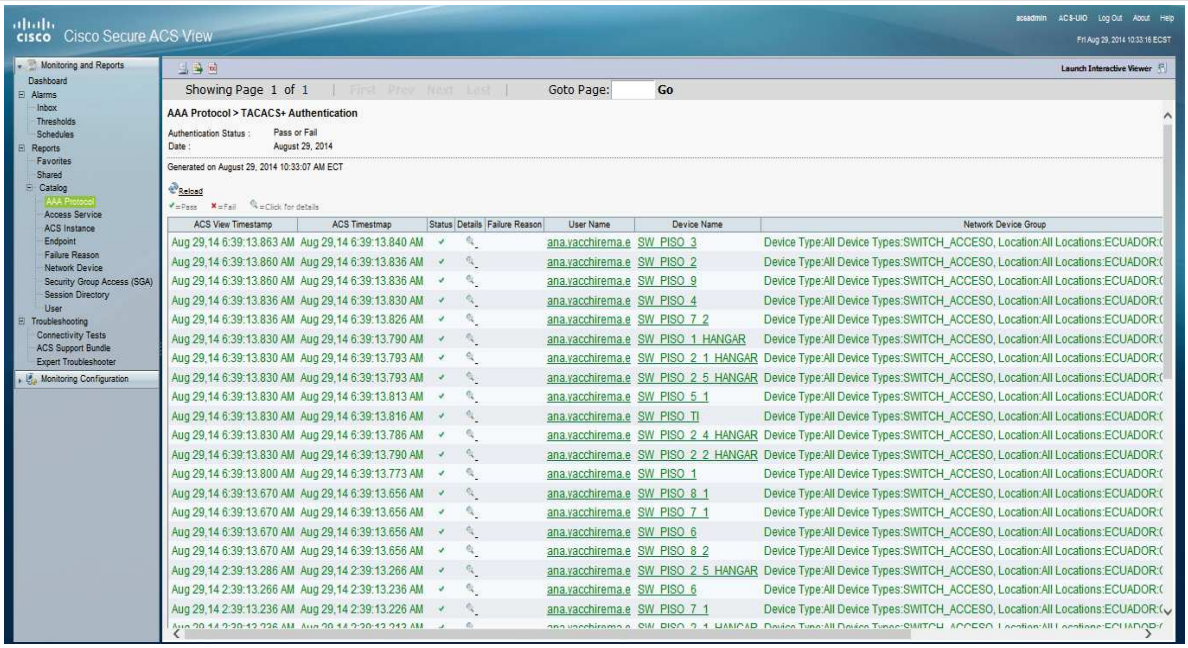


Figura 93. Pruebas de funcionamiento TACACS+

5.3.10.4.2. RADIUS

Todas las pruebas fueron satisfactorias al momento de ingresar a las máquinas de los usuarios finales y al momento de la asignación dinámica de la VLAN. A pesar de que las pruebas fueron satisfactorias se tuvo problemas con las máquinas con el sistema operativo Windows XP.

Esto se debe a que a pesar que en la política creada en el Directorio Activo de Microsoft para activar IEEE 802.1X indica a las máquinas del dominio que no pidan un certificado digital, las máquinas con Windows XP piden este certificado. Por lo que se creó el certificado en el CSACS, se lo firmó por el Directorio Activo y se distribuyó el certificado a las máquinas.

Para que no exista problemas con máquinas con Windows XP antes de configurar el puerto del *switch* para la autenticación se debe verificar que la máquina tenga la política 802.1X y confíe en el certificado digital del CSACS. La siguiente imagen muestra los registros (*logs*) del CSACS donde se puede apreciar la autenticación exitosa vía RADIUS de los empleados de la organización.

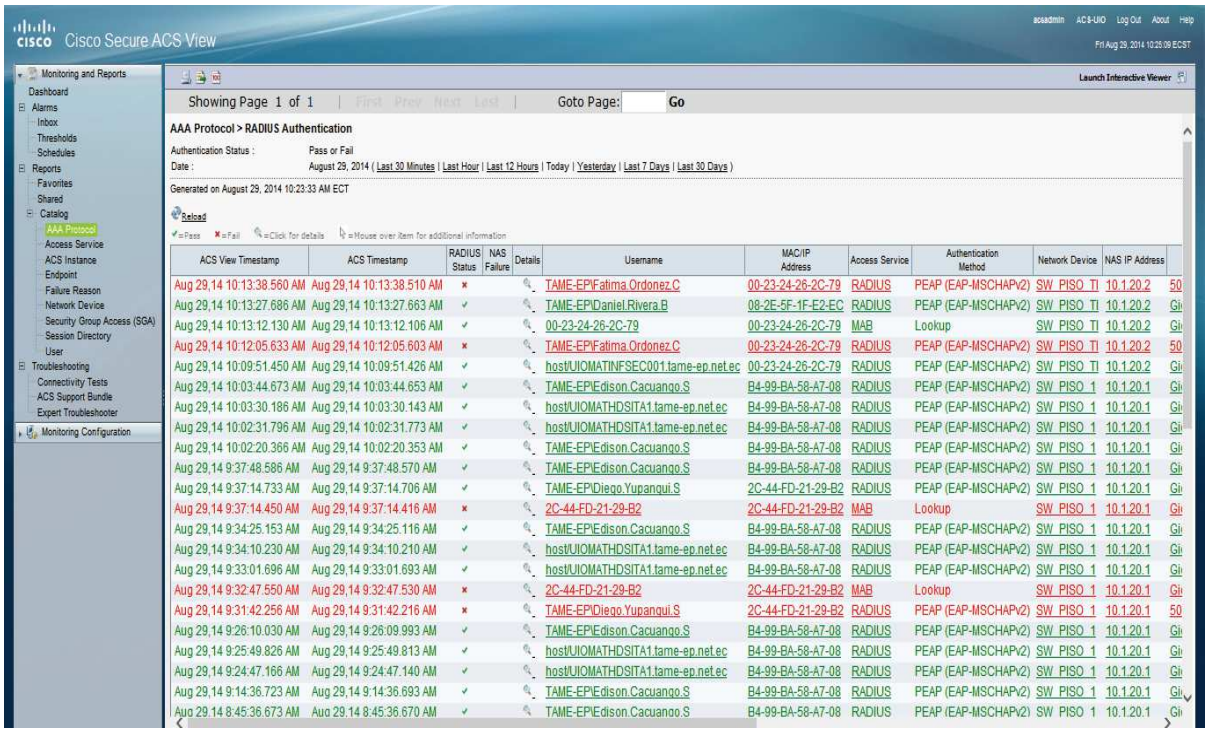


Figura 94. Pruebas de funcionamiento RADIUS

5.3.10.5. Información importante *Cisco Secure Access Control Server*

5.3.10.5.1. Licencias

La siguiente figura muestra el licenciamiento de los dos equipos

Figura 95. Licenciamiento CSACS

5.3.10.5.2. Certificados digitales

La siguiente figura muestra los certificados digitales, el propio del CSACS y el certificado firmado por la identidad certificadora del dominio.

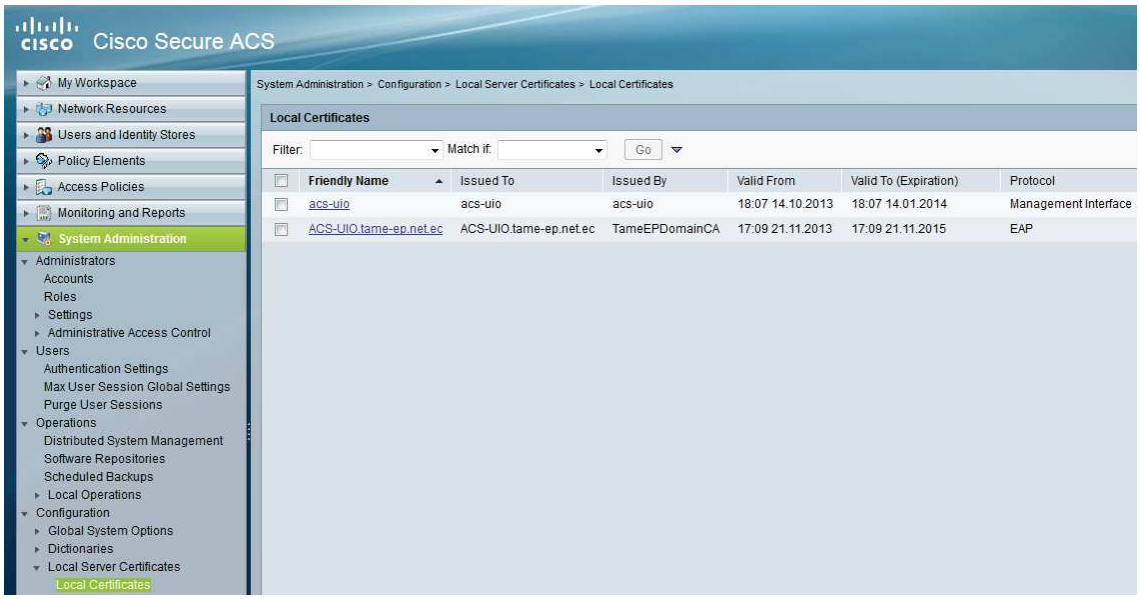


Figura 96. Certificados digitales – CSACS

5.3.10.5.3. High availability

La siguiente figura ilustra los dos CSACS en configuración de alta disponibilidad, desde este punto también se puede obtener *backups* de la configuración.

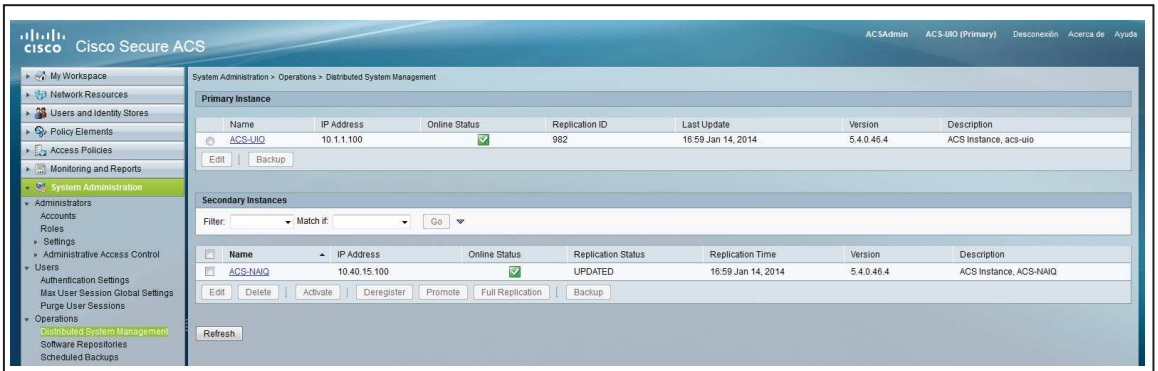


Figura 97. *High availability* - CSACS

5.4. Topología implementada completa

A pesar de que el presente proyecto no abarca la seguridad perimetral, ni la implementación de la red conmutada del Hangar ubicado en Tababela, la siguiente figura ilustra la topología completa actual de TAME EP, que permite obtener una idea detallada de toda la red de información.

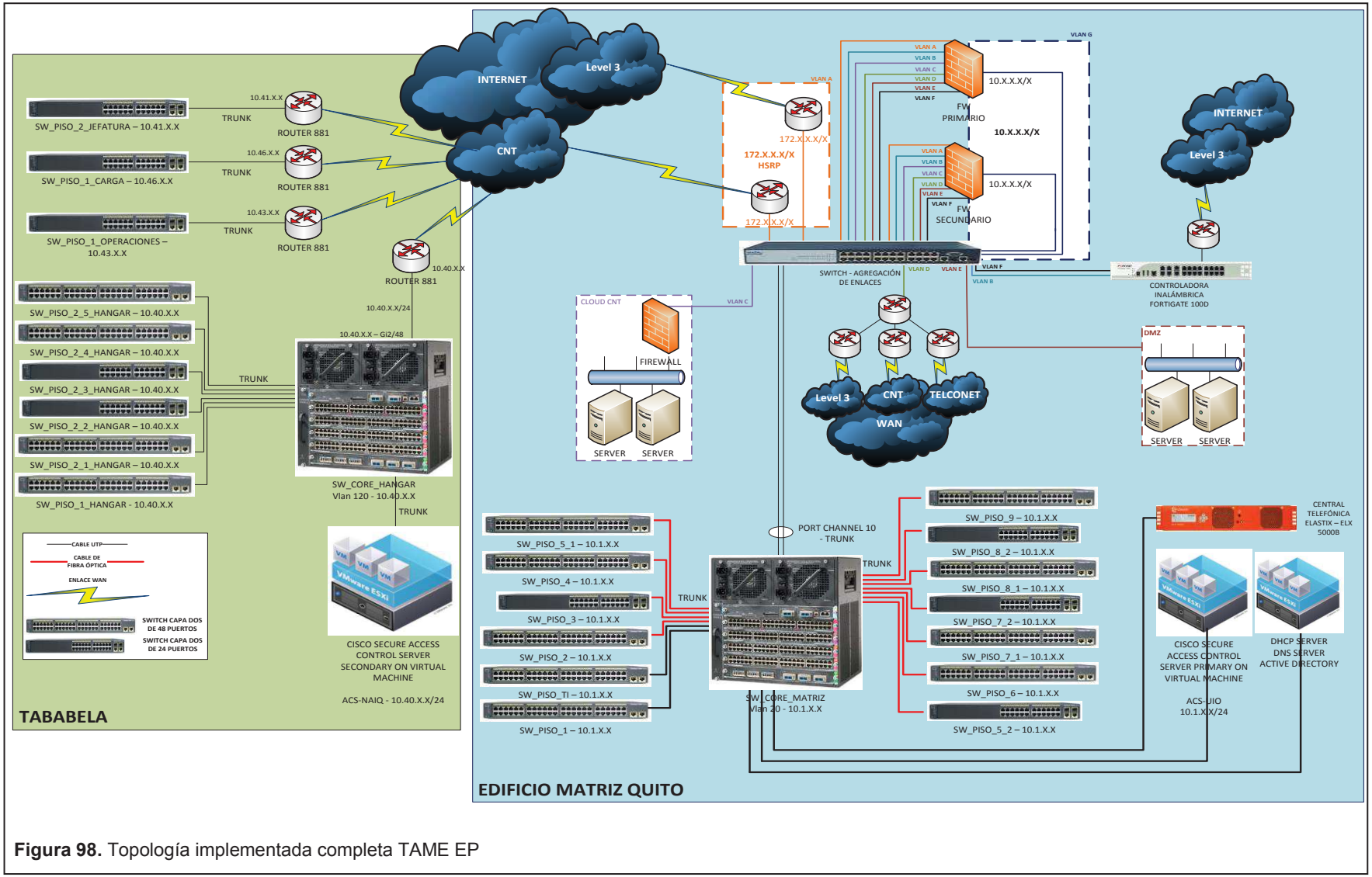


Figura 98. Topología implementada completa TAME EP

6. Capítulo VI. Conclusiones y recomendaciones

En el presente y último capítulo del proyecto, se presenta las conclusiones observadas a lo largo del diseño e implementación de la solución; así mismo se presenta las recomendaciones para que sean tomadas como base de mejora de la red, siempre buscando que la red se torne más robusta y segura para lograr obtener el máximo rendimiento.

6.1. Conclusiones

Con el levantamiento de información realizado se pudo observar que en la red anterior existían puntos críticos de falla como por ejemplo conexiones en cascada, falta de redundancia, capacidad de crecimiento nula en la mayoría de los pisos, lo que reduce el rendimiento de la red y permite que la misma esté propensa a fallas.

Para complementar lo anterior, el acceso a la información con un nivel mínimo o nulo de seguridad desde la red interna pone en grave riesgo la confidencialidad, integridad y disponibilidad de la información de la empresa, al no tener control de las personas que acceden a los servicios de la LAN, cuándo y desde qué equipos, ni de los cambios que realicen.

Con la implementación de los equipos siguiendo el nuevo diseño de la red de información, se potencia el rendimiento de la misma, ya que el nuevo diseño permite realizar la división de la red en diferentes grupos lógicos (VLANs) y con ello se reduce el transporte innecesario de información sobre toda la red como por ejemplo las tramas *broadcast* en los enlaces troncales, facilita la administración de la red debido a que los usuarios con similares funciones y requerimientos se asignan a la misma VLAN, es posible brindar un trato diferenciado a cada tipo de tráfico por ejemplo se separa la información sensible de la empresa en un VLAN diferente del resto; los nuevos equipos al presentar mayores características tanto en *hardware* como en *software* aumenta el *throughput* de la red que se evidencia en una mejor experiencia hacia el usuario final al utilizar la infraestructura de red.

Al implementar la solución con equipos de la misma marca, se explota al máximo los beneficios de cada equipo, evitando tener incompatibilidades al utilizar equipos de distintos fabricantes, además representa un ahorro significativo en cuanto a costos por soporte técnico pues no se necesitará expertos en cada marca, asimismo no se puede dimensionar y mantener reservas de repuestos distintos para cada marca, logrando reducir aún más los costos de operación y al mismo tiempo optimizar el personal de la empresa.

El sistema IBNS incrementa el nivel de seguridad de la infraestructura de red, enfocada en el acceso a la red interna, pues permite tener una visualización completa de los usuarios que ingresan a la red, tanto empleados como invitados, con un sistema AAA centralizado mediante el uso del *Cisco Secure Access Control System* y con equipos que actúan como autenticadores, como en este despliegue, los *switches* Cisco; además teniendo en cuenta que la mayoría de ataques o robos de información nacen de la parte interna de la red ya sea por empleados o por invitados, el uso de IBNS da solución a este problema, pues permite que los dispositivos finales tengan acceso seguro a la infraestructura de red utilizando autenticación específica, sea ésta del usuario final (credenciales) o del dispositivo (dirección MAC).

Al tener identificado cada equipo, tener centralizada la información y realizar respaldos periódicamente, se mejora y se facilita la administración y el control de la red de forma notoria.

Con la reingeniería de la red conmutada y la implementación de una solución que permita servicios de red basados en identidad (IBNS) para la aerolínea TAME EP en su edificio matriz, se logró mejorar el rendimiento de la red, se tiene escalabilidad, alistamiento para alta disponibilidad (redundancia) y menores tiempos de caída de la red; consiguiendo así mejorar la eficiencia y seguridad de la infraestructura de red.

6.2. Recomendaciones

La capacitación permanente al personal técnico en las nuevas tecnologías instaladas proporcionará ayuda eficaz para que realicen un adecuado uso de la

infraestructura de red, así como enfocar esfuerzos en generar una cultura de buen manejo de la información interna, teniendo en cuenta que la mayoría de ataques y robos de información surgen internamente.

Se recomienda elaborar y aplicar una política de seguridad en el que se detalle todos los procedimientos aplicables al manejo y uso de la red, permitiendo tener un mejor control ante diversas situaciones, así mismo cualquier modificación que se planee realizar en la red, primeramente debe ser valorada y puesta en conocimiento del administrador de red, para que se evalúe el alcance de los cambios y no se afecte repentinamente la operación de la red y por ende de la empresa.

Actualmente la mayoría de usuarios activos cuentan con sistemas operativos obsoletos y no existe un registro actualizado, por lo que se recomienda estandarizar los sistemas operativos de las máquinas a Windows 7 o Windows 8, además de que ya no existe soporte de Microsoft para Windows XP.

Se recomienda adquirir equipamiento *wireless* que se integre a nivel nativo con el CSACS para que se pueda utilizar el sistema IBNS con todas sus características, como el CoA (*Change of Authorization)*, a nivel WLAN *(Wireless Local Area Network)*.

Se recomienda el análisis para una futura actualización en cuanto a seguridad interna se refiere, en el cual se actualice el sistema IBNS actual, a un sistema de control de acceso usando ISE (*Cisco Identity Services Engine)* por tener las siguientes ventajas frente al sistema de control de acceso actual: es más robusto puesto que combina las principales características de IBNS y NAC, es decir, permite control de acceso a la red basado en identidad (IBNS) usando IEEE 802.1X, *MAC-Authentication Bypass* (MAB) y *Web-Authentication*, y además permite autenticar, autorizar y remediar usuarios (cableados, inalámbricos, remotos) y sus dispositivos antes de que puedan acceder a la red (NAC) para cumplir con la política de seguridad de la organización en cuanto a la red interna se refiere; ofrece visibilidad sin igual, es decir, tiene la capacidad de analizar e identificar con precisión a los usuarios y dispositivos que se

conecten a la red; garantiza los límites para mejorar el cumplimiento de las políticas y directrices de la empresa; permite poner limitaciones, por ejemplo, cualquier dispositivo con sistema operativo Android que no ingrese a la organización, característica que no es posible aplicar con IBNS.

REFERENCIAS

Alvarez M, Valdivieso C. (2011). Implementación de un sistema de video vigilancia utilizando Wi-Fi para el Conjunto residencial "EL Prado". Quito, Ecuador.

Cisco Systems. (s.f.). *Cisco Certified Network Associate* Security. (Versión 1.1). Recuperado el 27 de Julio de 2014.

Cisco Systems. (2007). *Cisco Certified Network Associate* Exploration Network Fundamentals.

Cisco Systems. (2009). *Designing Cisco Enterprise Campus Architecture Models*. Recuperado el 10 de Julio de 2013 de http://www.ciscopress.com/articles/article.asp?p=1315434.

Cisco Systems. (2011). *Cisco Support Community CAM VS TCAM*. Recuperado el 10 de Diciembre de 2013 de https://supportforums.cisco.com/document/60831/cam-vs-tcam.

Cisco Systems. (2008a). *Configuring VLANs*. Recuperado el 10 de Julio de 2013 de http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/VLANs.html.

Cisco Systems. (2005b). Seguridad de principio a fin. Recuperado el 10 de Julio de 2013 de http://www.cisco.com/web/ES/publicaciones/07-01-cisco-TCN280.pdf.

Cisco Systems. (2007c). *Understanding VLAN Trunk Protocol*. Recuperado el 10 de Julio de 2013 de http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml.

Cisco Systems. (2009d). *Identity Based Networking Services*. Recuperado el 10 de Julio de 2013 de

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/at_a_glance_c45-504537.pdf.

Cisco Systems. (2010e). *Identity Based Networking Services*. Recuperado el 10 de Julio de 2013 de http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_c27-574041.pdf.

Cisco Systems. (2013f). *Cisco Identity Services Engine (ISE)*. Recuperado el 14 de Septiembre de 2014 de http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-654884.pdf.

Cisco Systems. (2010). *Cisco SAFE Reference Guide*. Recuperado el 10 de Diciembre de 2013 de http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap5.html#wp1068516.

Cisco Systems. (2008). *TACACS+ and RADIUS Comparison.* Recuperado el 17 de Abril de 2014 de http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html.

Cisco Systems. *Identity Based Networking Services*. Recuperado el 3 de Marzo de 2014 http://www.cisco.com/c/en/us/products/ios-nx-os-software/identity-based-networking-services/index.html.

Cisco System. (2006). *Implementing Cisco Quality of Service 2(2). USA: Cisco Press.*

Edward. (2012). Redes de computadores. Recuperado 23 de Febrero de 2014 de http://edwcifu.blogspot.com/.

Guide to Networks. (2013). *Topologies and Ethernet Standards*. Recuperado el 14 de Septiembre de 2014 de http://cis155al.blogspot.com/2013/02/chapter-5-topologies-and-ethernet.html.

IEFT. (2006). *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. Recuperado el 10 de Julio de 2013 de http://tools.ietf.org/html/rfc4510.

Industrial Solutions. (s.f.). *Strategic Security*. Recuperado el 5 de Marzo de 2014 de http://www.indsol.com.mx/Soluciones.html?target=Autenticacion.

IETF RFC 2001 TCP *Slow Start, Congestion Avoidance, Fast Retransmit*. Recuperado el 21 de octubre 2012 de http://www.faqs.org/rfcs/rfc2001.html.

Lammle,T. (2011). *Cisco Certified Network Associate*. Indianapolis, USA:Wiley

Szigeti,T. y Hatting,C. (2005). *End-to-End QoS Network Design*. Indianapolis, USA: Cisco Press.

Talk to an IT. (2009). Las 7 capas. Recuperado el 10 de Enero de 2014 de http://www.talktoanit.com/c_old/index.php?option=com_content&view=article&id=1:las-7-capas&catid=36:redes&Itemid=82.

TAME EP. (2013). Página Oficial. Misión, Visión y Valores. Recuperado el 10 de Julio de 2013 de https://www.tame.com.ec/index.php?option=com_content&view=frontpage&Itemid=1&lang=es.

Textos Científicos. (2007). TCP/IP y el Modelo OSI. Recuperado el 8 de Enero de 2014 de http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi.

Universidad Miguel Hernández. (s.f.). Redes de Computadores. Recuperado el 10 de Enero de 2014 de http://isa.umh.es/asignaturas/sii/Tema5%20Redes%20SII.pdf.

ANEXOS

ANEXO 1 CARTA DE AUSPICIO

Quito, 27 de Agosto de 2013

Señor Ingeniero
Ángel Jaramillo
COORDINADOR DE LA CARRERA DE INGENIERÍA EN REDES Y TELECOMUNICACIONES
Universidad de las Américas

Por medio de la presente, queremos comunicar a su distinguida institución educativa nuestro compromiso de auspiciar el proyecto de tesis de los señores: Álvarez Figueroa Mayra Lucía y Valdivieso Salazar César Luis; consistente en REINGENIERÍA DE LA RED CONMUTADA E IMPLEMENTACIÓN DE UNA SOLUCIÓN QUE PERMITA SERVICIOS DE RED BASADOS EN IDENTIDAD (IBNS) PARA LA AEROLÍNEA TAME EN SU EDIFICIO MATRIZ, bajo las siguientes condiciones:

- Nuestra empresa se compromete a proveer los dispositivos y materiales necesarios para la realización del proyecto y facilitará los trabajos de estudio de funcionamiento, instalación, pruebas y monitoreo dentro de nuestras instalaciones.
- La empresa TAME en su calidad de auspiciante y propietario de los equipos, tiene derecho a realizar en el futuro las modificaciones y ampliaciones que considere convenientes.
- La información que se entregue será clasificada por la empresa y podrá ser divulgada solo con autorización expresa de nuestra parte.
- Se deberá firmar un acuerdo de confidencialidad, directo con TAME.
- Se llevará seguimiento al trabajo efectuado, comprometiéndonos a entregar una carta de conformidad al finalizar el proyecto.

Atentamente,

Ing. Fabián Moreano
GERENTE TECNOLOGÍA DE LA INFORMACIÓN

Empresa Pública Tame Línea Aérea del Ecuador "TAME EP"