UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DIVISIÓN DE INGENIERÍA ELÉCTRICA

DISEÑO DE UNA RED DE TELECOMUNICACIONES MULTI-SERVICIOS PARA UN SISTEMA DE TRANSPORTE DE LA CIUDAD DE MÉXICO

INFORME DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN TELECOMUNICACIONES

PRESENTA

HUGO JAVIER VALDÉS PEÑA

TUTOR: M.I. Juventino Cuéllar González

CIUDAD UNIVERSITARIA, FEBRERO 2016

ÍNDICE

Actividades de la Empresa y Puesto Desempeñado

Actualmente laboro para una empresa dedicada a brindar soluciones en materia de telecomunicaciones desempeñando el puesto de Ingeniero de Pre-ventas en la Ciudad de México. Dentro de mis actividades como ingeniero de pre-ventas, se encuentran el diseño de soluciones de redes de datos, recomendaciones en cuanto a la arquitectura de red de proyectos específicos, misma que incluye la proposición del equipo activo y su respectiva configuración, entre otras.

La empresa para la que laboro, está enfocada a la distribución de soluciones de valor agregado en Tecnologías de la Información y Comunicaciones en la República Mexicana. Cuenta con gran experiencia y personal altamente calificado para satisfacer todas las necesidades de sus canales de integración (Business Partner) y clientes.

La misión de nuestra empresa tiene como objetivo satisfacer las expectativas tecnológicas de nuestros clientes enfocadas a las telecomunicaciones; con soluciones de calidad que incrementen la competitividad y productividad de sus empresas.

La visión de la empresa consiste en consolidar nuestra Red de Distribuidores a nivel Nacional y ser reconocidos como una empresa que ofrece soluciones en aplicaciones y servicios de telecomunicación de valor agregado.

Introducción

En el informe presente, se pretende describir el diseño de una red que optimice tanto operativa, como económicamente, los servicios tecnológicos existentes en la red del cliente.

En la actualidad la transformación de las redes se ha convertido en una necesidad urgente. La adopción de la virtualización, la computación en la red (Cloud Computing)[1] y las redes definidas por software[2], SDN por sus siglas en inglés, siguen en aumento. También crecen las aplicaciones, los medios y los dispositivos a los que las redes dan soporte. La inteligencia, agilidad y capacidad de ampliación de la red ya no son opciones, sino imperativos.

Ha incrementado también, el uso de dispositivos móviles, tales como teléfonos inteligentes, tabletas electrónicas, computadoras portátiles, entre otros. Esta tendencia, dentro del mundo de las redes de datos empresariales, se denomina *Bring Your Own Device* (*BYOD)*. El hecho de que cada vez más personas cuenten con dispositivos móviles y hagan uso de la red, presenta un riesgo en varios aspectos para esta misma. Por ello es necesario que las redes empresariales sean más robustas, más seguras y que satisfagan las necesidades de los usuarios.

Actualmente, existen muchas empresas que ofrecen soluciones en redes empresariales. Estas empresas necesitan tener modelos inteligentes para gestionar exigentes entornos BYOD y aplicaciones en tiempo real, de tal forma que se satisfaga la creciente demanda de aplicaciones multimedia y las necesidades de virtualización de las empresas.

La solución requerida necesita "entender" a los dispositivos y a las aplicaciones asociadas. La comprensión contextual de las conversaciones entre dispositivos y aplicaciones permite optimizar la experiencia de usuario y el rendimiento de la red, reduciendo al mismo tiempo las inversiones de capital y los gastos de explotación.

Para facilitar el diseño de la arquitectura, es necesario que la red cuente con los aspectos que se listan a continuación:

[1]. Diccionario Español de Ingeniería (1.0 edición), Real Academia de Ingeniería de España, 2014, consultado el 4 de mayo de 2014.
[2] "Software-Defined Networking: The New Norm for Networks". White paper. Open Networking Foundation. Abril 13, 2012.

- **Arquitectura Flexible**

  El concepto de Arquitectura Flexible puede representarse mediante cuatro aspectos fundamentales:

  - *Red Simplificada*

    Reducción del número de capas para formar la red, que resulte en una disminución de la latencia durante la transferencia de información. Esto provoca que se requiera una menor cantidad de equipos para llevar a cabo el desarrollo de la red y así se disminuyen los gastos, tanto de operación como de capital.

  - *Virtualización de la Red*

    Implementación de herramientas de virtualización que permitan manejar diferentes sistemas físicos como un sistema lógico para reducir costos de mantenimiento. Además, en caso de que se presente una falla en la red, se minimice el tiempo al haber recuperación automática. Otro aspecto importante es que todos los enlaces que conforman la red, estén en uso.

  - *Resilencia*

    Cuando exista una falla en la red, la recuperación rápida debe hacer posible que las aplicaciones se queden activas, por lo que los usuarios de aplicaciones de voz y vídeo no deben percatarse de que existió tal falla. Al tener una virtualización de la red, se tienen diferentes maneras de mover el tráfico de datos a través de la red.

  - *Seguridad Embebida*

    Se pueden disminuir las amenazas internas que pueden atentar contra la integridad de la red. Además, el perfilamiento por usuario y el reconocimiento de dispositivo, asegura que los usuarios tengan acceso únicamente a los recursos de la red que les están permitidos.

- **Operaciones Simplificadas**

  El concepto de Operaciones Simplificadas puede representarse mediante cuatro aspectos fundamentales:

  - *Aprovisionamiento Automático*

    Contar con identificación automática de dispositivos (Teléfonos IP, Puntos de Acceso inalámbricos, entre otros), usuarios y aplicaciones virtualizadas. Además auto-configurar parámetros de la red tales como calidad de servicio (QoS), seguridad, por mencionar algunos, basándose en usuario, dispositivo o aplicación. Cuando ocurra un cambio de lugar ya sea de usuario, dispositivo o aplicación virtualizada, la red debe ajustarse automáticamente, entregando los parámetros que se tenían anteriormente.

  - *Administración Convergente*

    La solución debe contar con herramientas que permiten la visualización de aplicaciones y con herramientas de troubleshooting, con el fin de reducir el tiempo fuera de operación en caso de una falla.

  - *Sistema Operativo Común*

    Al tener un sistema operativo común entre todos los conmutadores de red se pueden reducir errores en la configuración que resultan de tener múltiples sistemas operativos. También se simplifican los nuevos desarrollos y los mantenimientos.

  - *Eficiencia Energética*

    Conmutadores de red que ofrezcan un ahorro energético de hasta 70%, hecho que reduce drásticamente los gastos de operación. También, al tener una red simplificada, se puede ahorrar en espacios, enfriamiento y mantenimiento.

- **Control Automático**
  El Control Automático se puede resumir en los aspectos siguientes:

  - *Perfilamiento*
    El conmutador es capaz de “entender” al usuario, al dispositivo, a la aplicación y a los requerimientos de seguridad elegidos para poder brindar una política contextual dirigida.

  - *Auto-detección*
    Existe detección automática de usuarios, dispositivos y máquinas virtuales dentro de la red, junto con su ubicación. Además, es posible simplificar la asignación de calidad de servicio y de políticas de seguridad para tener niveles de servicio apropiados.

  - *Políticas*
    Asignación de políticas que permita que la red se ajuste automáticamente a las características del usuario, dispositivo o aplicación virtualizada.

Después de haber dado una introducción de este trabajo, a continuación se presenta una breve explicación de los temas cubiertos en cada uno de los capítulos.

En el capítulo 1, “Diseño de la Topología de Red”, se describe el modelo de red que se utilizó para el diseño de la solución.

En el capítulo 2, “Características Técnicas de los Equipos de Red”, se describen cada una de las características técnicas con las cuales debieron cumplir los equipos para poder ser integrados a la red.

Finalmente, en el capítulo 3, se presentan los resultados que se obtuvieron a través del diseño de la red, así como las conclusiones y la participación profesional directa.

Antecedentes del Proyecto

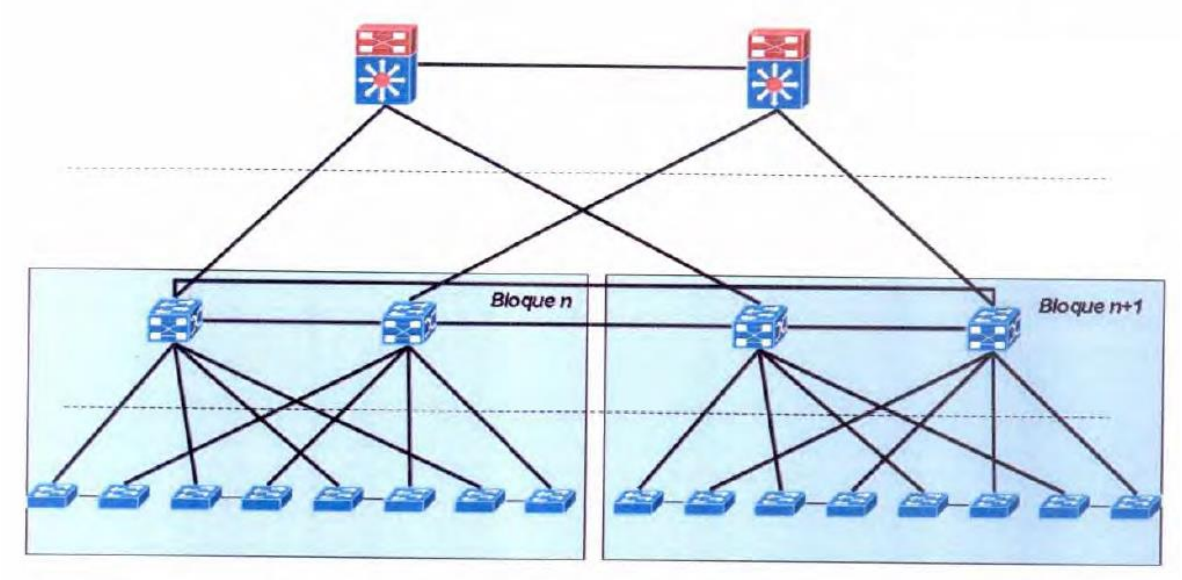
La dependencia para la cual se diseñó la red multi-servicios contaba con una red de telefonía analógica que proporcionaba el servicio a las áreas operativas, administrativas en toda la dependencia, la obsolescencia tecnológica y los altos costos de operación y mantenimiento, demandaban urgentemente una actualización y/o migración de la telefonía por tecnologías de información que permitieran modernizar y optimizar las comunicaciones y abatir los costos de operación por este concepto.

En lo que respecta a la red de datos, se presentaban los problemas siguientes:

- Proliferaban las redes LAN (Local Area Networks por sus siglas en inglés), sin comunicación en una MAN (Metropolitan Area Network por sus siglas en inglés) o WAN (Wide Area Network por sus siglas en inglés)
- Conmutadores de red en riesgo de falla
- Sin planeación en el crecimiento de nodos de red
- Arquitectura de hardware y software no estándar
- Sin convergencia de tecnologías

En cuanto a la LAN, no había un esquema de Alta Disponibilidad, siendo esta red un vulnerable a fallas.

La topología Actual de esta red es la que se muestra en la siguiente figura:



Como se puede ver, existe una conexión entre los nodos de acceso y no se tiene un doble enlace de cada conmutador de red de acceso a cada conmutador de red de distribución. Esto no es un esquema de redundancia.

La capa de distribución está formada por un anillo, lo que tampoco resulta del todo conveniente.

En la topología propuesta se mostrará un esquema de doble enlace de acceso a distribución y un esquema de malla en la distribución y en el core, con el fin de tener una red en Alta Disponibilidad, robusta y segura.

Debido a ello la dependencia decidió elaborar un modelo tecnológico para implementar una red de voz, datos y video bajo el protocolo Internet, para sustituir y/o actualizar gradualmente la infraestructura de telefonía analógica, optimizando operativamente y reduciendo drásticamente los costes y fallas de la telefonía.

Marco Teórico

El fundamento teórico reside primeramente en el análisis de los tipos de redes de datos y topologías, esto con el fin de poder llevar a cabo un diseño de red óptimo y adecuado a las necesidades del cliente.

Para hacer el diseño de la red primero se debe tomar en cuenta qué topología física tendrá. Una vez definida, se deben contemplar los servicios que soportará dicha red, con el fin de establecer el número de puertos de los conmutadores de red, tipo de interfaces y transceptores a utilizar, velocidades de transmisión, dualidad de enlaces, entre otras características físicas.

Posterior al diseño físico, se contempla la teoría necesaria para llevar a cabo el diseño lógico. En este trabajo se hace énfasis en protocolos a nivel de capa de enlace, según el modelo OSI. Entre los protocolos más importantes se encuentran los de autenticación de usuarios, principalmente el protocolo 802.1X, que es una extensión del Protocolo de Autenticación Extensible sobre una Red de Área Local (EAPOL). Se propone hacer uso de este método de autenticación debido a las ventajas y a la seguridad que ofrece.

Dadas las condiciones del proyecto, el diseño a nivel de capa de red aún no se lleva a cabo, sin embargo se está haciendo el planteamiento y la propuesta de utilizar el protocolo OSPF, un protocolo de enrutamiento dinámico de Gateway interior basado en la tecnología de estado de enlace. Se propone utilizar este protocolo debido al tamaño de la red, pues el despliegue de ésta, hará obsoleto el uso de protocolos de enrutamiento estático.

Objetivos

- Identificar los requerimientos y necesidades de la red actual, anticipando las demandas de servicios

- Proponer especificaciones técnicas detalladas, que permitan transformar la situación actual a una Oportunidad de Mejora cuantificable y medible.

- Diseñar una solución integral que resuelva de origen las necesidades de red, reduciendo complejidad y agregando valor.

1. DISEÑO DE LA TOPOLOGÍA DE RED

1.1. Topologías de Red

La topología define la representación geométrica de todos los enlaces que conforman a la red y de los dispositivos asociados a ella. Existen muchos tipos de topologías de red, sin embargo los más conocidos son: bus, anillo, estrella y malla.

- La topología ***bus*** es aquella en la que un enlace único interconecta a todos los dispositivos de la red, de tal forma que se constituya una red en forma de tronco.
- En la topología en ***anillo***, cada dispositivo perteneciente a la red tiene una línea de conexión con cada uno de los otros dispositivos que conforman la red, de tal forma que se despliegue una red en forma de anillo.
- La topología en ***estrella*** se compone de un controlador central que tiene un enlace dedicado con cada uno de los dispositivos que conforman la red.
- La topología en ***malla*** es un poco más compleja que las anteriores, pues en esta topología, cada dispositivo tiene un enlace punto a punto dedicado con cualquier otro dispositivo perteneciente a la red. El término dedicado, implica que dicho enlace distribuye únicamente el tráfico de datos de los dispositivos que interconecta.

En la figura 1.1.1 se muestran las topologías de red más utilizadas en la actualidad.

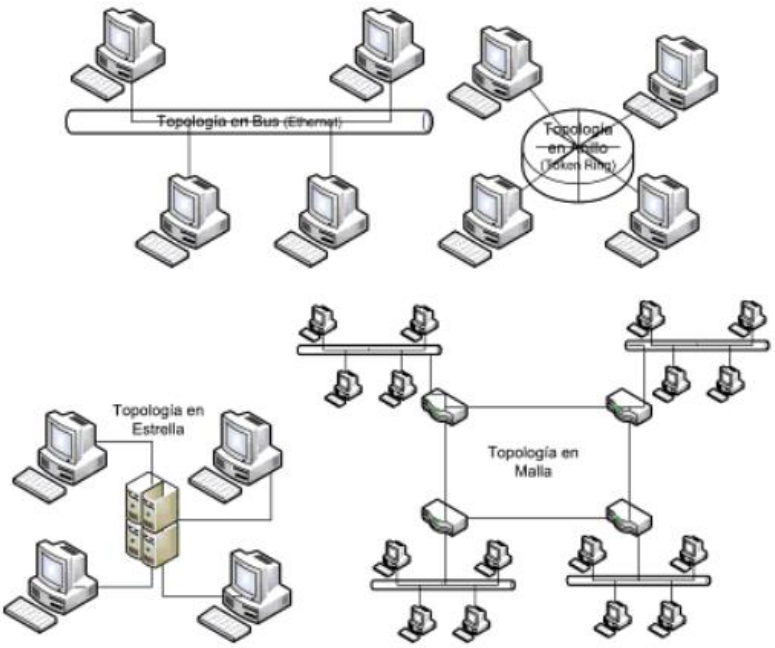


Figura 1.1.1 Topologías de Red

La topología en malla ofrece ventajas múltiples con respecto al resto de topologías. Una de ellas es que ofrece una mayor tolerancia a fallos y fiabilidad. El uso de enlaces dedicados garantiza que cada conexión transporte únicamente el tráfico de datos de los dispositivos que interconecta. Además, es fácil para el administrador de la red localizar y detectar, las causas de las fallas, en caso de que se llegasen a presentar. Una desventaja de la topología en malla es la complejidad en el despliegue, pues se tienen que invertir en más recursos para poder implementarla

Para el caso del proyecto que se realizó, se propuso una topología jerárquica, la cual contempla tres capas: la capa de núcleo, que es donde se lleva a cabo la mayor parte del procesamiento de información, la capa de distribución o agregación que es la encargada de establecer el enlace entre las diferentes capas de la red y, finalmente, la capa de acceso, que es donde se brindan los servicios al usuario final.

En el siguiente apartado se describirán los elementos que se consideraron para el diseño de la red.

1.2 Estructura Física de la Red

Las redes empresariales, generalmente, están constituidas por tres capas principales: la capa de ***núcleo*** o CORE, la capa de ***distribución*** o agregación, y la capa de ***acceso*** o borde. A continuación se describe brevemente cada una de las capas mencionadas.

- **Capa de Núcleo**
  Está formada por equipos dedicados al manejo de grandes cantidades de tráfico. Por ello, dichos equipos deben cumplir con características muy específicas, como baja latencia, alta disponibilidad, redundancia física y lógica, entre otras.
  Actualmente, los equipos que conforman las capas de núcleo, cuentan con capacidad para formar centros de datos; por ello, manejan estándares que contemplan la generación de máquinas virtuales como el seguimiento automático de éstas.
  Las funciones de los equipos de la capa de núcleo no contemplan generación de grupos, redes virtuales, listas de acceso, entre otras, con el fin de evitar latencia y congestión en los puertos. Asimismo, es sumamente recomendable que los puertos de los equipos, además de soportar grandes tasas de transmisión de datos, siempre estén activos, por ello se debe evitar el uso de protocolos como *STP* y utilizar nuevos protocolos como *SPB*.

- **Capa de Distribución**
  Los equipos que conforman esta capa, están destinados, principalmente a manejar el enrutamiento entre la capa de acceso y la de núcleo. De hecho, es en esta capa donde reside la mayor parte de la configuración de la red, como las políticas, las redes virtuales, entre otras.
  Es recomendable que los equipos de la capa de distribución cuenten con protocolos de enrutamiento avanzado, con el fin de satisfacer las necesidades de las grandes empresas. También, es deseable que se tengan puertos de alta velocidad para enlazar las otras dos capas. Generalmente se utilizan enlaces de 10 Gb.

- **Capa de Acceso**
  En esta capa se da acceso a los usuarios de la red. Por ello, los equipos que la conforman deben contar con características de seguridad muy especiales, tales como el perfilamiento automático del usuario, creación de políticas de acceso, protocolos de contención de ataques informáticos, entre otros. Lo anterior para asegurar la red internamente y así evitar que los usuarios puedan acceder a sitios a los que no se les está permitido.
  Es deseable que los equipos cuenten con puertos de alta velocidad, pues se debe hacer el enlace con equipos de otra capa. También, se recomienda que los equipos tengan la posibilidad de ser apilables y modulares, con el fin de dar acceso a la red a todos y cada uno de los usuarios.

En la actualidad, algunos fabricantes están reduciendo el número de capas con el fin de optimizar costos de operación y de mantenimiento.

El número de capas puede reducirse u optimizarse dependiendo del tamaño de la red, pues en una red metropolitana, como es el caso del proyecto en curso, es mejor segmentar el tráfico de información para evitar congestionamientos en la red.

En las figuras 1.2.1 y 1.2.2 se muestran los despliegues de red según su tamaño.

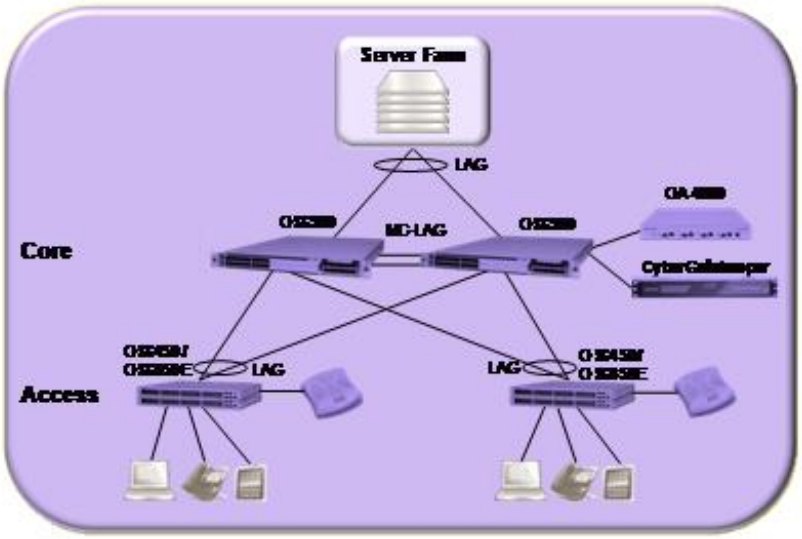


Figura 1.2.1 Red Jerárquica Compacta

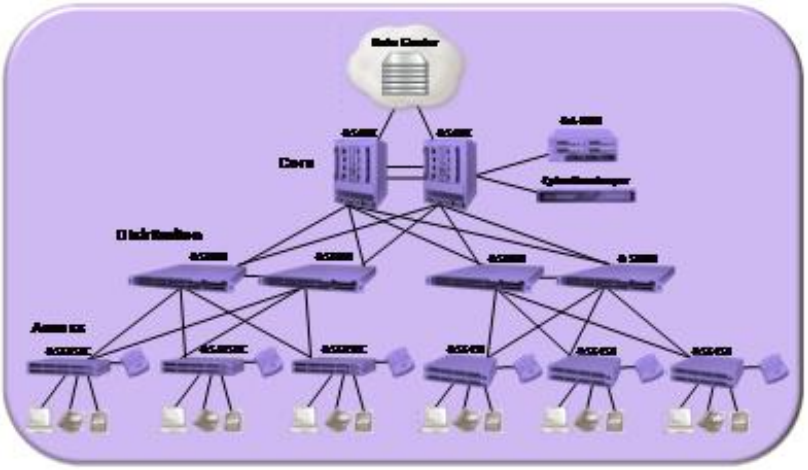


Figura 1.2.2 Red Jerárquica Densa

La red que se diseñó es una red metropolitana, lo que implica que está desplegada por gran parte del territorio de la Ciudad de México.

En un inicio se había propuesto prescindir de la capa de ***distribución***, sin embargo existieron factores que imposibilitaron este esquema, tales como el incremento del costo del proyecto y el incremento de la complejidad en el despliegue de la red, entre otros. Tomando en cuenta lo anterior, se diseñó la red considerando tres capas: núcleo, distribución y acceso.

La red que se diseñó es una *red multi-servicios*, lo que implica que soportará diversos servicios tales como cámaras de vigilancia, comunicaciones unificadas, aplicaciones de centro de datos, seguridad perimetral, telefonía por IP, entre otras.

Se consideraron más ***5000 nodos de acceso***, los cuales estaban distribuidos a través de más de 150 sitios, para los cuales se decido colocar un conmutador de red por sitio.

Teniendo en cuenta las características mencionadas, se procedió con el diseño de las capas que conformarían la red.

1.2.1. Capa de Núcleo

Para la capa de núcleo se consideraron cuatro sitios. El sitio uno, también denominado como principal, fue el destinado para procesar la mayor cantidad de información así como para desplegar el centro de datos y los sistemas de almacenamiento.

Los otros tres sitios se eligieron de tal forma que la trayectoria de la fibra óptica permitiera su interconexión física, tal como se muestra en la figura 1.2.1.1 :

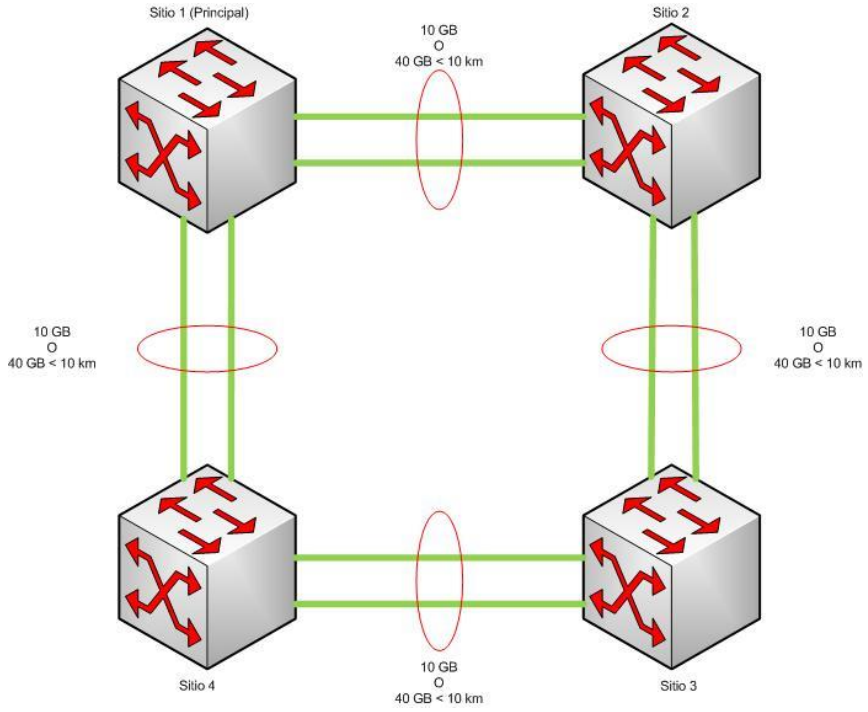


Figura 1.2.1.1 Red de Núcleo

Tal como se muestra en la figura, existe un doble enlace entre cada sitio. Esto con el fin de brindar un esquema de alta disponibilidad en full-dúplex.

Para los enlaces entre cada equipo se consideró el uso de ***fibra óptica monomodo*** mediante transceptores que soportan una tasa de transmisión de 10 Gbps. Lo ideal era considerar el enlace a 40 Gbps, sin embargo, la distancia entre algunos sitios excede los 20 km y no se contaba con un ***SFP***[3] que soportara esa tasa de transmisión a una distancia mayor de 20 km, además, de haber contado con él, la solución se habría encarecido drásticamente.

Dadas las exigencias tecnológicas de la dependencia, los equipos destinados a formar la red de núcleo debían cumplir con ciertas características, mismas que serán descritas en el capítulo siguiente.

Para el diseño de la capa de núcleo se consideraron conmutadores de red de una unidad de rack con una gran densidad de puertos de alta velocidad de transmisión. En cada sitio se propuso colocar dos conmutadores de red que actuaran como una sola unidad lógica y que sumaran sus capacidades de conmutación. La tecnología que permite conjuntar las capacidades de conmutación de los dos conmutadores de red, se denomina ***Chasis Virtual***.

En la actualidad es de suma importancia resaltar las bondades que ofrece la virtualización, sobre todo en un centro de datos, pues al implementar un esquema de chasis virtual se ofrecen múltiples ventajas que impactan en la optimización de costos tanto de operación como de capital.

Dentro de la propuesta se incluyó la interconexión de las dos unidades de rack de cada sitio, mediante enlaces de 40 Gbps, con el fin de maximizar la trasmisión de información y brindar a la dependencia, la alta disponibilidad que requiere.

[3] Un transceptor SFP, del inglés small form-factor pluggable, es un transceptor compacto y conectable en caliente utilizado para las aplicaciones de comunicaciones de datos y telecomunicaciones. Están diseñados para soportar Sonet, canal de Fibra, Gigabit Ethernet y otros estándares de comunicaciones.

El esquema de chasis virtual se muestra en la figura 1.2.1.2

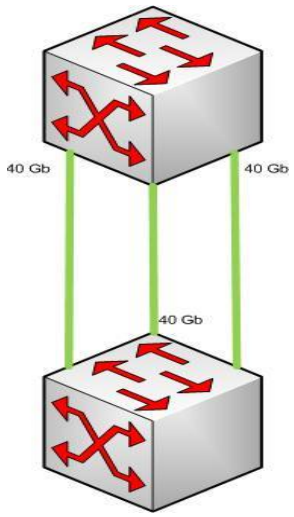


Figura 1.2.1.2 Chasis virtual en Núcleo

El chasis virtual proporciona redundancia tanto física como lógica. Uno de los conmutadores funge como maestro y el otro como esclavo, en caso de presentarse alguna falla en el conmutador maestro, automáticamente el conmutador esclavo toma el rol de maestro, logrando con ello que no se pierda la comunicación.

Los cuatro sitios siguen el mismo esquema de conexión. Cada sitio está enlazado de tal forma que se sigue una topología en anillo. Se planeaba hacer una topología en malla con el fin de ofrecer mayor seguridad en la red, sin embargo la trayectoria del tendido de fibra óptica no era la más conveniente para realizar dicha topología, pues se incrementaría la complejidad del despliegue y podrían presentarse problemas en la propagación de la señal óptica.

1.2.2. Capa de Distribución

Tal como se comentó, en un inicio se planeaba prescindir de una capa intermedia entre el núcleo y el acceso, pues todos los equipos involucrados tenían la capacidad de procesar la información y transmitirla a través de puertos que siempre se encuentran activos. Sin embargo, esto no resultó del todo conveniente, pues en vez de hacer más eficiente la solución, tanto tecnológica como económicamente, se incrementaban costos y se incrementaba también la complejidad del despliegue de la red.

La distancia entre los sitios de acceso y los sitios de núcleo excedía, en algunos casos, los 20 km, por lo que se requería un transceptor de rango extendido el cual, evidentemente, es mucho más costoso que uno de rango largo. Además, si bien es cierto que los equipos de acceso tienen la capacidad de hacer un enrutamiento básico, se requería de protocolos dinámicos, por lo que se debían utilizar otros equipos y licencias que hacían aún más cara y menos eficiente la solución.

Al hacer el conteo del número de transceptores de rango extendido que se requerirían para establecer los enlaces a 10 Gb, se llegó a la conclusión de colocar equipos intermedios que se encargaran de hacer el enrutamiento hacia la capa de núcleo mediante enlaces de 10 Gb con transceptores de rango largo.

La capa de distribución se formó por dos conmutadores de red de una unidad de rack a través del chasis virtual. Estos equipos cuentan con capacidad para hacer enrutamiento avanzado y cuentan con la disponibilidad de puertos para llevar a cabo los enlaces a 10 Gb.

Es de suma importancia mostrar las bondades que trae consigo un esquema de virtualización, tales como ahorro energético, ahorro en espacios, ahorro en los costos de operación y mantenimiento, entre otros.

Evidentemente, los equipos de esta capa son de capacidades menores a los de la capa de núcleo, al menos en hardware. El esquema de conexión de los conmutadores se muestra en la figura 1.2.2.1:

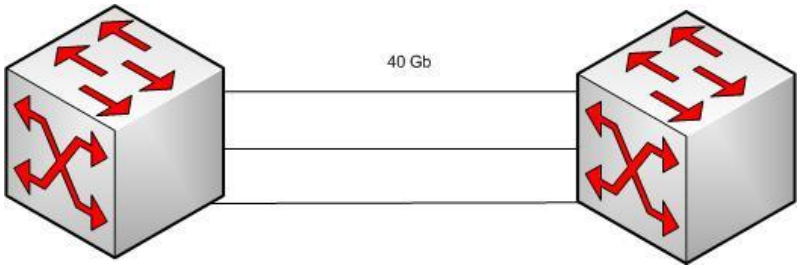


Figura 1.2.2.1 Chasis Virtual en Distribución

En este caso se contempló utilizar la funcionalidad de chasis virtual remoto, pues cada conmutador se colocó en un sitio de tal forma que la distancia no excediera los 20 km hacia el acceso y hacia el núcleo. Evidentemente, los sitios para colocar los conmutadores de distribución, se eligieron de tal manera que no existiera una distancia mayor a 10 km entre ellos, para que el enlace del chasis virtual pudiera hacerse a 40 Gb.

1.2.3. Capa de Acceso

Para formar la capa de acceso se tomaron en cuenta más de 150 sitios, los cuales están distribuidos en gran parte de la Ciudad de México.

Se planeó un conmutador de red por cada sitio. Estos conmutadores deben cumplir con ciertas características: tener los puertos suficientes para brindar enlaces a 10 Gb, tener los puertos suficientes para poder ser apilables en caso de requerirse y tener los puertos suficientes para dar acceso a todos los usuarios de la red.

Se contemplaron dos puertos a 10 Gb para el enlace a los conmutadores de distribución, además se agregaron módulos de expansión con el fin de tener disponibilidad de puertos en caso de que se requiera apilar los conmutadores.

Anteriormente existía un anillo entre los equipos de acceso, pero se descartó esta topología generando el doble enlace hacia los equipos de distribución.

El esquema general propuesto por sitio se muestra en la figura 1.2.3.1:

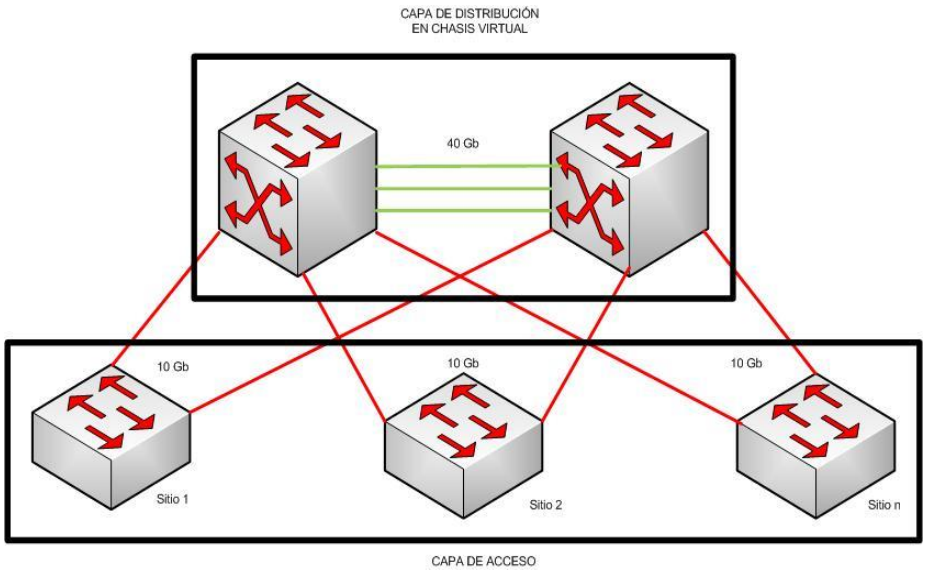


Figura 1.2.3.1 Capa de Acceso

1.2.4. Topología Física General

Teniendo ya la descripción individual por cada capa, se llega al esquema topológico general, el cual está representado en la figura 1.2.4.1 :

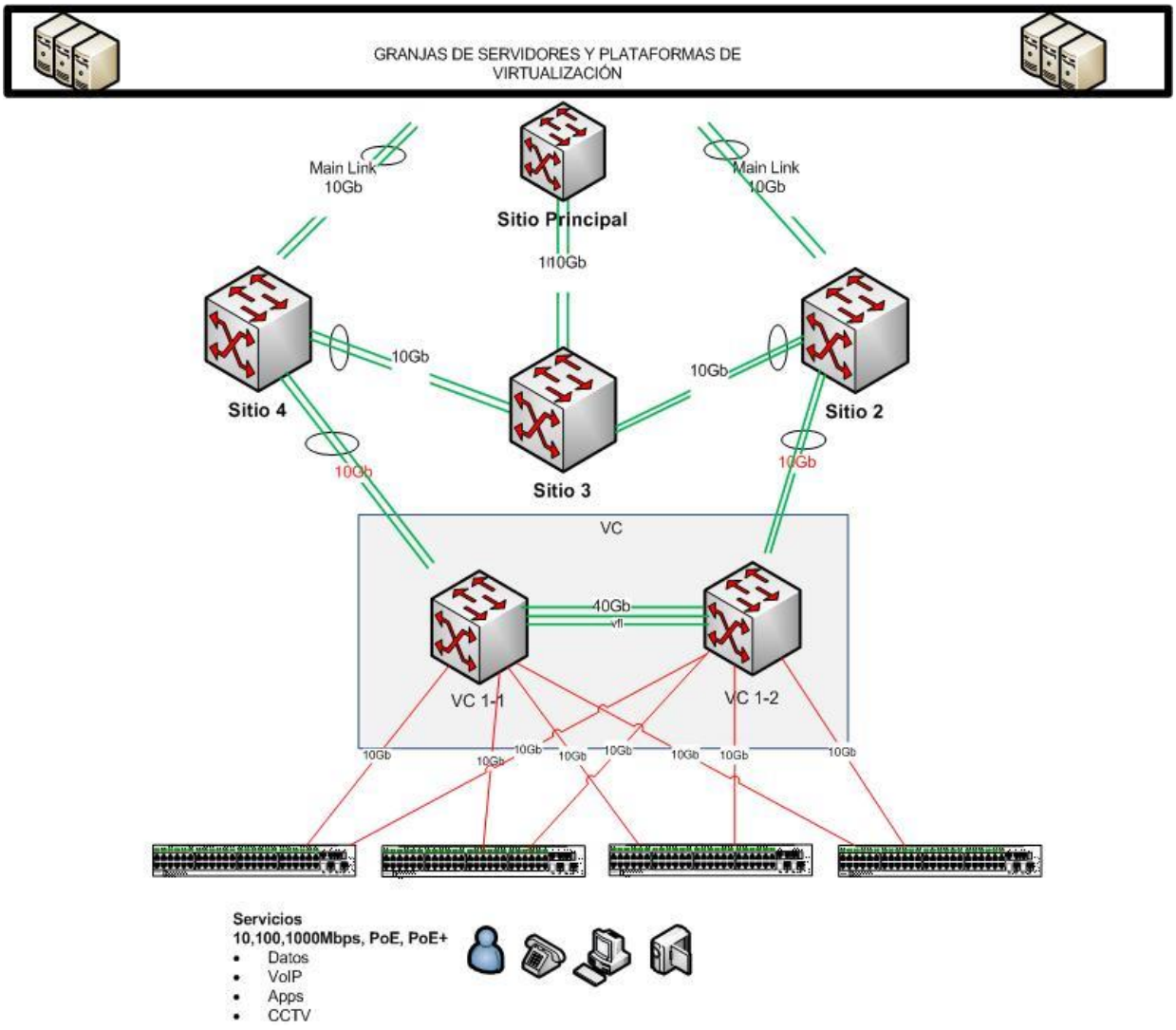


Figura 1.2.4.1 Topología Física de la Red

1.3 Estructura Lógica de la Red

Una vez definida la topología física de la red, se procedió con el diseño lógico de ésta. Para ello resultó más sencillo comenzar el análisis por capas, tal como se menciona a continuación.

1.3.1. Diseño a Nivel de Capa de Enlace

Para el diseño a nivel de capa de enlace, tomando en cuenta el modelo de referencia OSI, se hicieron varias consideraciones. Una de ellas fue la creación de diferentes redes virtuales de área local, VLAN por sus siglas en inglés. Una VLAN es un método para crear redes lógicas independientes dentro de una misma red física[4]. Varias VLAN pueden coexistir en un conmutador de red o en una única red física.

Se propuso a la dependencia un esquema de segmentación basado en perfiles, con el fin de que la red estuviera preparada para ajustar automáticamente su configuración en función del movimiento de usuarios y dispositivos en la red, en lugar del enfoque tradicional de configuraciones estáticas basado en puertos de conmutación.

Dentro de la propuesta se consideraron los puntos siguientes:

- Minimizar el esfuerzo al eliminar la necesidad de volver a configurar manualmente la red cuando los dispositivos se mueven alrededor.

- Mejorar el rendimiento de entrega de aplicaciones para la movilidad de los usuarios con la sintonización fina de la red para que los usuarios tengan la misma experiencia donde quiera que estén conectados.

- Proporcionar seguridad coherente en toda la red

[4] James F. Kurose, Keith W. Ross (2012). *Computer Networking:A Top-Down Approach*. Pearson Education. ISBN 978-0-13-136548-3.

Bajo este esquema, la red puede contar con múltiples ventajas y puede ofrecer a los usuarios un acceso seguro, una prioridad y una calidad de servicio determinada, como se muestra en la figura 1.3.1.1:

Figura 1.3.1.1 Ventajas en Red de Acceso

El funcionamiento de esta propuesta está basado en diferentes protocolos de autenticación, el principal de ellos es el estándar 802.1X. El protocolo 802.1X es una extensión del Protocolo de Autenticación Extensible sobre una Red de Área Local (EAPOL). Este protocolo es empleado para transportar credenciales de información entre dos dispositivos. Actualmente se manejan concepciones erróneas al hacer equivalentes el estándar 802.1X y la autenticación basada en puertos, pues ésta última se compone de tres elementos de los cuales, el más importante resulta ser precisamente el estándar 802.1X. Los otros dos elementos son los Métodos del protocolo de Autenticación Extensible (EAP-Methods) y el Marcado de Autenticación Remota en Servicio del Usuario (RADIUS).

Dentro del proceso de autenticación existen tres dispositivos participantes: el primero es el dispositivo que desea acceder a la red, llamado *suplicante*. El segundo dispositivo es al que el suplicante des|ea autenticarse, que es llamado *autenticador* y el tercer dispositivo en juego y que posee las credenciales de información, es usualmente un servidor RADIUS y es conocido como el *Servidor de Autenticación*.

Bajo este esquema, cuando un dispositivo intenta ingresar a la red a través del protocolo http mediante un puerto determinado, enviará sus credenciales de autenticación al conmutador. Este procedimiento se conoce como el *inicio de sesión.*

El siguiente paso es el denominado *proceso de autenticación*, que ocurre cuando el conmutador de red envía las credenciales de autenticación recibidas por parte del dispositivo suplicante hacia el servidor de autenticación que, como se mencionó, generalmente es un servidor RADIUS; para que éste verifique la identidad del dispositivo.

El último paso es el *proceso de autorización*, que se lleva a cabo cuando el servidor de autenticación envía los resultados de la verificación de identidad. Si el servidor no encuentra registro del dispositivo suplicante, enviará al conmutador la respuesta de que las credenciales de autenticación son inválidas, por lo que el suplicante deberá comenzar el proceso nuevamente. En caso de que el servidor encuentre las credenciales de autenticación, el puerto al que el suplicante ingresó, será colocado en una VLAN con los parámetros que se hayan establecido para ésta, como el nivel de calidad de servicio (QoS), el nivel de acceso, el nivel de ancho de banda, etcétera.

Puede existir el caso en el que un invitado llegue a la red. En este esquema, el invitado pasará a un portal cautivo. Para que el invitado pueda acceder a la red, un empleado de la dependencia deberá llevar a cabo el registro del invitado y entregarle credenciales de acceso (usuario y contraseña). Así, el invitado pasará a una VLAN de invitados, valga la redundancia, la cual puede tener diferentes parámetros de calidad en el servicio.

Es importante mencionar que el suplicante contará con los mismos atributos en cualquier puerto al que se conecte, ya sea por medio cableado o inalámbrico, logrando que se minimice el esfuerzo del personal de tecnología de la información en cuanto a configuración de la red.

En la figura 1.3.1.2 se pueden observar los dispositivos requeridos para poder aplicar el protocolo de autenticación 802.1X

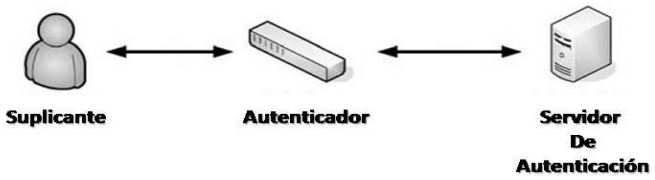


Figura 1.3.1.2 Dispositivos Participantes en 802.1X

1.3.2. Diseño a Nivel de Capa de Red

Para el diseño de la capa de red, de acuerdo a las necesidades de la dependencia, se consideró el Protocolo ***Open Shortest Path First (OSPF)***. OSPF es un protocolo de enrutamiento jerárquico de gateway interior o IGP (Interior Gateway Protocol), que usa el algoritmo SmoothWall Dijkstra enlace-estado, para calcular la ruta más idónea.

OSPF es probablemente el protocolo IGP más utilizado en redes grandes. Como sucesor natural de RIP, acepta Máscaras de Subred de Longitud Variable y Enrutamiento entre Dominios sin Clases desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede formar por diferentes áreas. Hay un área especial llamada área backbone que forma la parte central de la red a la que se encuentran conectadas el resto de áreas de la misma. Las rutas entre las diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectarse con éste. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

OSPF organiza un sistema autónomo en áreas. Estas áreas son grupos lógicos de enrutdores cuya información se puede resumir para el resto de la red. Un área es una unidad de enrutamiento, es decir, todos los enrutadores de la misma área mantienen la misma información topológica en su base de datos de estado-enlace de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

Existen diferentes roles de los enrutadores dentro de una red OSPF. Los enrutadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los enrutadores eligen a un enrutador designado (Designated Router, DR) y un enrutador designado secundario o de copia (Backup Designated Router, BDR). OSPF puede usar tanto multidifusiones (multicast) como unidifusiones (unicast) para enviar paquetes de bienvenida y actualizaciones de enlace-estado.

Un enrutador OSPF clásico es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra. Para el encaminamiento entre distintas áreas del Sistema Autónomo y desde el Sistema Autónomo hacia el exterior, OSPF utiliza enrutadores especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

- **Enrutadores fronterizos de área o Area Border Routers (ABR),** que mantienen la información topológica de su área y la conectan con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red (inter-area routing).

- **Enrutadores fronterizos del Sistema Autónomo o Autonomous System Border Routers (ASBR)**, que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet.

Cuando los sistemas autónomos son grandes por sí mismos y nada sencillos de administrar. OSPF les permite dividirlos en áreas numeradas donde un área es una red o un conjunto de redes inmediatas.

OSPF distingue los siguientes tipos de área:

- **Área Backbone**

  El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área.

- **Área stub**

  Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de encaminamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

- **Área not-so-stubby**

  También conocidas como NSSA, constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

Para el caso de este proyecto, se tomaron en cuenta las áreas que la dependencia ya tenía definidas, sin embargo, no se nos dio acceso a esa información, por lo que no pudimos llevar a cabo un diseño de enrutamiento como tal.

2. CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS DE RED

En este capítulo se describirán las características técnicas de los equipos de red que se propusieron para el diseño de la red multi-servicios. Con el fin de hacer más descriptivo el análisis, se expondrán las características por cada capa de la red.

2.1. Características de los Equipos de la Capa de Núcleo

Como se mencionó en el capítulo anterior, para la capa de núcleo se propusieron conmutadores de red de una unidad de rack destinados al manejo de gran cantidad de tráfico de datos. Se seleccionaron estos equipos debido a que ofrecen una gran densidad de puertos y una gran capacidad de procesamiento, además que son más económicos con respecto a los conmutadores tipo gabinete. Las características principales de los conmutadores seleccionados, se muestran en la tabla 1:

Tabla 1

Funciones	Ventajas
Alto rendimiento en conmutación y enrutamiento con puertos Ethernet no-bloqueantes a velocidades de 40 GigE, 10 GigE, 1 GigE y 100Base-T	Capacidad de conmutación de hasta 2.56 Tb/s por unidad y latencia de sub-microsegundos para clústeres de servidores de alto rendimiento y conectividad de núcleo sobre QSFP, SFP +, DAC o CAT 5/6.
Hasta 104 puertos 10 GigE (SFP+), 32 puertos de 40 GigE (QSFP+) y puertos dedicados para Canales de Fibra a través de Ethernet (FCoE).	• Excelente rendimiento para el soporte de voz, datos, almacenamiento y aplicaciones de vídeo en tiempo real para redes convergentes escalables. • Soporta servicios de próxima generación con una densidad de puertos muy alta en una unidad de rack.
• Funciones Avanzadas del Sistema Operativo: calidad de servicio (QoS), listas de control de acceso (ACL), funciones de capa 2 / capa-3, LAN virtual (VLAN), apilamiento e IPv6. • Hardware de alta disponibilidad Virtual Extensible LAN (VXLAN), virtual Tunnel End Point gateway (VTEP) para la virtualización de red. • Política de control inteligente a través de OpenFlow 1.3.1 / 1.0.	• La arquitectura del conmutador simplifica el despliegue de almacenamiento convergente para FC, Fibre Channel over Ethernet (FCoE), Internet Small Computer System Interface (iSCSI) y Network-Attached Storage (NAS). • Software Defined Networking (SDN) incorporado para controlar los perfiles de red virtuales y gestión de políticas.
• Enrutamiento automático hacia la red troncal y aprovisionamiento al acceso, Shortest Path Bridging (SPB) para servicios enrutados y puenteos, Edge Virtual Bridging (EVB), protocolo de Registro de VLAN Múltiples (MVRP) y Virtual Network Profile (VNP) dinámico.	• Evita errores humanos mediante la automatización de configuraciones estandarizadas y reproducibles. • Evita explosión dirección de host y las inundaciones con una función de soporte de servicio SLA a bajos costos operativos y de capital y basada en estándares probados interoperables.

- **Características detalladas del conmutador**

  Los conmutadores de red de la capa de núcleo cuentan con un total de 32 puertos fijos QSFP en el panel frontal. Los puertos pueden ser de cobre o fibra operando a 40 GigE o 4x10 GigE utilizando divisores ópticos, alcanzando una densidad de puertos de 10 GigE de 104 puertos.

  - **Administración Simplificada**
    - Interfaz de línea de comandos intuitiva en un ambiente programable de Python y Bash a travpes de la consola, Telnet o Shell Seguro (SSH V2) para IPv4 e IPv6.
    - Interfaz Web gráfica para administración del equipo a través de HTTP y HTTPS para IPv4 e IPv6.
    - Utilización del Protocolo SNMP en sus versiones 1, 2 y 3 para la administración y generación de reportes, y para facilitar la administración de la red a terceros.
    - Carga de archivos por medio de USB, TFTP, FTP, SFTP o SCP a través de IPv4 e IPv6.
    - Dirección IP de Loopback para la administración por servicio.
    - Monitoreo basado en políticas y en puertos.
    - sFlow V5 y Monitoreo Remoto de la Red (RMON).
    - Detección de Enlace Unidireccional (UDLD) y Monitoreo de Diagnóstico Digital (DDM).
    - Soporte de servidor DHCP v4 y DHCP v6.
    - Soporte de Protocolo de Tiempo de Red (NTP)

- **Resistencia y Alta Disponibilidad**
  - Administración Unificada, Tecnología de Chasis Virtual.
  - ITU-T G.8032/Y1344 2010: Ethernet Ring Protection.
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1D Spanning Tree Protocol (STP) y IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).
  - Per-VLAN spanning tree (PVST+) y modo STP 1x1.
  - IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP).
  - Virtual Router Redundancy Protocol (VRRP) con capacidades de rastreo.
  - Fuentes de poder redundantes con capacidad de cambio durante la operación.
  - Bandejas de ventiladores redundantes y con capacidad de cambio durante la operación.
  - Protección interna en el CPU contra ataques maliciosos.

- **Funciones de Centro de Datos**

  - IEEE 802.1Qbg Edge Virtual Bridging (EVB).
  - IEEE 802.1Qbb Priority Flow Control (PFC).
  - IEEE 802.1Qaz Enhanced Transmission Selection (ETS).
  - IEEE 802.1Qaz Data Center Bridging Capabilities Exchange Protocol (DCBX).
  - IEEE 802.1aq Shortest Path Bridging (SPB-M).
  - RFC 7843 Virtual eXtensible Local Area Network (VXLAN).

- **Software Defined Networking (SDN)**

  - OpenFlow 1.3.1 completamente programable y agente 1.0 para el control de OpenFlow nativo y puertos híbridos.
  - Plug-in de OpenStack compatible con Grizzly o mayor.
  - Soporte de VXLAN y VTEP.

- **Almacenamiento Convergente**

  - Soporte de Fibre Channel (FC) nativo, de acuerdo con ANSI INCITS FC-PI-4 y FC-PI-5
  - Soporte de Fibre Channel over Ethernet (FCoE) de acuerdo con T11-BB-6.
  - Adaptador de Red Convergente para FCoE de extremo a extremo con respecto a T11-BB-6.
  - Mapeo de Virtual SAN (VSAN) a VLAN y FIP snooping bridge (FSB).

- **Seguridad Avanzada**

  - Soporte de 802.1X multi-cliente y multi-VLAN para servicios de SPBM/VXLAN.
  - Acceso basado en MAC para usuarios sin 802.1X.
  - SSH con Infraestructura de Llave Pública (PKI) para servicios SPBM/VXLAN.
  - Soporte de cliente Terminal Access Controller Access-Control System Plus (TACACS+).

  - Administrador centralizado de autenticación, Remote Access Dial-In User Service (RADIUS) y Lightweight Directory Access Protocol (LDAP).
  - Learned Port Security (LPS) o bloqueo de direcciones MAC.
  - Filtrado de IP de origen como un mecanismo de protección y eficaz contra los ataques ARP.

- **Calidad de Servicio (QoS)**

  - Colas de prioridad: ocho colas de prioridad por puerto.
  - Priorización de tráfico.
  - Administración de tráfico y de ancho de banda basada en flujo.
  - Clasificación de máscaras no contiguas para IPv4 (32 bits) e IPv6 (128 bits).
  - Evasión de Congestión: Soporte de prevención de bloqueo end-to-end head-of-line (E2E-HOL), IEEE 802.1Qbb control de flujo basado en prioridades y control de flujo IEEE 802.3x.

- **Enrutamiento IPv4**

  - VRF múltiple.
  - Enrutamiento estático con etiquetado de ruta.
  - Protocolo de Información de Ruta (RIP) v1 y v2.
  - Open Shortest Path First (OSPF v2).
  - Protocolo Sistema Intermedio a Sistema Intermedio (IS-IS).
  - Border Gateway Protocol (BGP v4).
  - Encapsulación Genérica de Enrutamiento (GRE) y túneles IP/IP.
  - Virtual Router Redundancy Protocol (VRRP v2).
  - Servidor DHCP v4.
  - Enrutamiento basado en políticas y servidor de balanceo de cargas.

- **Enrutamiento IPv6**

  - VRF múltiple.
  - Protocolo de Control de Mensaje de Internet (ICMP v6).
  - Enrutamiento estático.
  - Protocolo de información de Ruta de Siguiente Generación (RIPng).
  - OSPF v3.
  - IS-IS.
  - IS-IS con topología multiple.
  - Extensiones multiprotocolo de BGP v4 para enrutamiento en IPv6 (MP-BGP).
  - VRRP v3.
  - Protocolo de Descubrimiento de Vecinos (NDP).
  - Enrutamiento basado en políticas y servidor de balanceo de cargas.
  - Servidor DHCP v6.

- **Multicast (IPv4/IPv6)**

  - Protocolo de Administración de Grupos de Internet (IGMP v1/v2/v3).
  - Protocolo de Multicast Independiente en Modo Esparcido (PIM-SM) y Multicast de Fuente Específica (PIM-SSM).
  - Protocolo de Multicast Independiente en Modo Denso (PIM-DS) y Bidireccional (PIM-BiDir).
  - Protocolo Vector-Distancia de Enrutamiento de Multicast (DVMRP).

- **Servicios Avanzados de Capa 2**

  - Soporte de servicios de Ethernet mediante el uso del protocolo 802.1ad (también conocido como Q-in-Q o apilamiento de VLAN).
  - Servicios de Virtualización 802.1aq Shortest Path Bridging (SPB-M) y VXLAN.
  - Soporte de tramas JUMBO.
  - Bloqueo de BPDU.

2.2. Características de los Equipos de la Capa de Distribución

Como se mencionó, los equipos que se consideraron en la propuesta para formar la capa de distribución de la red, son muy similares a los equipos de núcleo pues comparten muchas de las funcionalidades técnicas. La diferencia, básicamente, reside en el hardware, pues la densidad de puertos requerida es un poco menor, tal y como se describe en la tabla 2:

Tabla 2

Funciones	Ventajas
Alto rendimiento en conmutación y enrutamiento con puertos Ethernet no-bloqueantes a velocidades de 40 GigE, 10 GigE, 1 GigE y 100Base-T	Capacidad de conmutación de hasta 640 Gb/s por unidad y latencia de sub-microsegundos para clústeres de servidores de alto rendimiento y conectividad de núcleo sobre QSFP, SFP +, DAC o CAT 5/6.
Hasta 32 puertos SFP+/FCoE, 3 puertos de 40 GigE (QSFP+) o 12 puertos GFC (FCoE).	• Excelente rendimiento para el soporte de voz, datos, almacenamiento y aplicaciones de vídeo en tiempo real para redes convergentes escalables. • Soporta servicios de próxima generación con una densidad de puertos muy alta en una unidad de rack.
• Funciones Avanzadas del Sistema Operativo: calidad de servicio (QoS), listas de control de acceso (ACL), funciones de capa 2 / capa-3, LAN virtual (VLAN), apilamiento e IPv6. • Política de control inteligente a través de OpenFlow 1.3.1 / 1.0.	• La arquitectura del conmutador simplifica el despliegue de almacenamiento convergente para FC, Fibre Channel over Ethernet (FCoE), Internet Small Computer System Interface (iSCSI) y Network-Attached Storage (NAS). • Software Defined Networking (SDN) incorporado para controlar los perfiles de red virtuales y gestión de políticas.
• Enrutamiento automático hacia la red troncal y aprovisionamiento al acceso, Shortest Path Bridging (SPB) para servicios enrutados y puenteos, Edge Virtual Bridging (EVB), protocolo de Registro de VLAN Múltiples (MVRP) y Virtual Network Profile (VNP) dinámico.	• Evita errores humanos mediante la automatización de configuraciones estandarizadas y reproducibles. • Evita explosión dirección de host y las inundaciones con una función de soporte de servicio SLA a bajos costos operativos y de capital y basada en estándares probados interoperables.

- **Características detalladas del conmutador**
  Los conmutadores de red de la capa de distribución cuentan con un total de 20 puertos fijos SFP+ 1/10 GigE, dependiendo del transceptor que se utilice, y un módulo de expansión en la parte frontal.

- **Administración Simplificada**
  - Interfaz de línea de comandos intuitiva en un ambiente programable de Python y Bash a travpes de la consola, Telnet o Shell Seguro (SSH V2) para IPv4 e IPv6.
  - Interfaz Web gráfica para administración del equipo a través de HTTP y HTTPS para IPv4 e IPv6.
  - Utilización del Protocolo SNMP en sus versiones 1, 2 y 3 para la administración y generación de reportes, y para facilitar la administración de la red a terceros.
  - Carga de archivos por medio de USB, TFTP, FTP, SFTP o SCP a través de IPv4 e IPv6.
  - Dirección IP de Loopback para la administración por servicio.
  - Monitoreo basado en políticas y en puertos.
  - sFlow V5 y Monitoreo Remoto de la Red (RMON).
  - Detección de Enlace Unidireccional (UDLD) y Monitoreo de Diagnóstico Digital (DDM).
  - Soporte de servidor DHCP v4 y DHCP v6.
  - Soporte de Protocolo de Tiempo de Red (NTP)

- **Resistencia y Alta Disponibilidad**
  - Administración Unificada, Tecnología de Chasis Virtual.
  - ITU-T G.8032/Y1344 2010: Ethernet Ring Protection.
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1D Spanning Tree Protocol (STP) y IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).
  - Per-VLAN spanning tree (PVST+) y modo STP 1x1.
  - IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP).
  - Virtual Router Redundancy Protocol (VRRP) con capacidades de rastreo.
  - Fuentes de poder redundantes con capacidad de cambio durante la operación.
  - Bandejas de ventiladores redundantes y con capacidad de cambio durante la operación.
  - Protección interna en el CPU contra ataques maliciosos.

- **Funciones de Centro de Datos**

  - IEEE 802.1Qbg Edge Virtual Bridging (EVB).
  - IEEE 802.1Qbb Priority Flow Control (PFC).
  - IEEE 802.1Qaz Enhanced Transmission Selection (ETS).
  - IEEE 802.1Qaz Data Center Bridging Capabilities Exchange Protocol (DCBX).
  - IEEE 802.1aq Shortest Path Bridging (SPB-M).
  - RFC 7843 Virtual eXtensible Local Area Network (VXLAN).

- **Software Defined Networking (SDN)**

  - OpenFlow 1.3.1 completamente programable y agente 1.0 para el control de OpenFlow nativo y puertos híbridos.
  - Plug-in de OpenStack compatible con Grizzly o mayor.
  - Soporte de VXLAN y VTEP.

- **Almacenamiento Convergente**

  - Soporte de Fibre Channel (FC) nativo, de acuerdo con ANSI INCITS FC-PI-4 y FC-PI-5
  - Soporte de Fibre Channel over Ethernet (FCoE) de acuerdo con T11-BB-6.
  - Adaptador de Red Convergente para FCoE de extremo a extremo con respecto a T11-BB-6.
  - Mapeo de Virtual SAN (VSAN) a VLAN y FIP snooping bridge (FSB).

- **Seguridad Avanzada**

  - Soporte de 802.1X multi-cliente y multi-VLAN para servicios de SPBM/VXLAN.
  - Acceso basado en MAC para usuarios sin 802.1X.
  - SSH con Infraestructura de Llave Pública (PKI) para servicios SPBM/VXLAN.
  - Soporte de cliente Terminal Access Controller Access-Control System Plus (TACACS+).

  - Administrador centralizado de autenticación, Remote Access Dial-In User Service (RADIUS) y Lightweight Directory Access Protocol (LDAP).
  - Learned Port Security (LPS) o bloqueo de direcciones MAC.
  - Filtrado de IP de origen como un mecanismo de protección y eficaz contra los ataques ARP.

- **Calidad de Servicio (QoS)**

  - Colas de prioridad: ocho colas de prioridad por puerto.
  - Priorización de tráfico.
  - Administración de tráfico y de ancho de banda basada en flujo.
  - Clasificación de máscaras no contiguas para IPv4 (32 bits) e IPv6 (128 bits).
  - Evasión de Congestión: Soporte de prevención de bloqueo end-to-end head-of-line (E2E-HOL), IEEE 802.1Qbb control de flujo basado en prioridades y control de flujo IEEE 802.3x.

- **Enrutamiento IPv4**

  - VRF múltiple.
  - Enrutamiento estático con etiquetado de ruta.
  - Protocolo de Información de Ruta (RIP) v1 y v2.
  - Open Shortest Path First (OSPF v2).
  - Protocolo Sistema Intermedio a Sistema Intermedio (IS-IS).
  - Border Gateway Protocol (BGP v4).
  - Encapsulación Genérica de Enrutamiento (GRE) y túneles IP/IP.
  - Virtual Router Redundancy Protocol (VRRP v2).
  - Servidor DHCP v4.
  - Enrutamiento basado en políticas y servidor de balanceo de cargas.

- **Enrutamiento IPv6**

  - VRF múltiple.
  - Protocolo de Control de Mensaje de Internet (ICMP v6).
  - Enrutamiento estático.
  - Protocolo de información de Ruta de Siguiente Generación (RIPng).
  - OSPF v3.
  - IS-IS.
  - IS-IS con topología multiple.
  - Extensiones multiprotocolo de BGP v4 para enrutamiento en IPv6 (MP-BGP).
  - VRRP v3.
  - Protocolo de Descubrimiento de Vecinos (NDP).
  - Enrutamiento basado en políticas y servidor de balanceo de cargas.
  - Servidor DHCP v6.

- **Multicast (IPv4/IPv6)**

  - Protocolo de Administración de Grupos de Internet (IGMP v1/v2/v3).
  - Protocolo de Multicast Independiente en Modo Esparcido (PIM-SM) y Multicast de Fuente Específica (PIM-SSM).
  - Protocolo de Multicast Independiente en Modo Denso (PIM-DS) y Bidireccional (PIM-BiDir).
  - Protocolo Vector-Distancia de Enrutamiento de Multicast (DVMRP).

- **Servicios Avanzados de Capa 2**

  - Soporte de servicios de Ethernet mediante el uso del protocolo 802.1ad (también conocido como Q-in-Q o apilamiento de VLAN).
  - Servicios de Virtualización 802.1aq Shortest Path Bridging (SPB-M) y VXLAN.
  - Soporte de tramas JUMBO.
  - Bloqueo de BPDU.

2.3. Características de los Equipos de la Capa de Acceso

Los equipos que se consideraron en la propuesta para formar la capa de acceso de la red tienen características muy particulares, las cuales se muestran en la tabla 3.

Tabla 3

Funciones	Ventajas
Hasta 8 conmutadores pueden ser conectados mediante la tecnología de Chasis Virtual, para crear una sola entidad lógica con 32 puertos de enlace a 10 GigE y 384 puertos GigE.	El Chasis Virtual incrementa la redundancia del sistema, la resistencia y la alta disponibilidad, a la vez que facilita el despliegue, operación y administración de la red.
Soporte del Estándar 802.3af Power over Ethernet (PoE), que ofrece hasta 30 W en cada uno de los puertos. También soporta PoE++ que ofrece hasta 60 W en cuatro puertos.	• Con sus capacidades PoE avanzadas y alta densidad de puertos PoE,es ideal para implementaciones de campus convergentes, ofreciendo flexibilidad de implementación, lo que simplifica el cableado y ayuda a reducir el tiempo de implementación de los dispositivos de última generación como teléfonos VoIP, cámaras de vigilancia, puntos de acceso y 802.11ac dispositivos que requieren mayor de 30 W, como monitores de vídeo o incluso un conmutador de red pequeña o un cliente ligero infraestructura de escritorio virtual (VDI) emergente.
• Soporte de la tecnología Deep Packet Inspection (DPI). • Monitoreo de aplicaciones y funcionalidad fingerprinting	• La tecnología DPI permite clasificación de paquetes en tiempo real a nivel de la capa de aplicación, monitoreo y tratamiento de la calidad de servicio para asignar prioridad y mayor ancho de banda a aplicaciones de negocios críticas. • Al habilitar la función de monitoreo de aplicaciones, el administrador de la red puede tener visibilidad coherente de hasta 1000 aplicaciones ejecutándose en la red.
• Soporte de autenticación automática mediante el reconocimiento de un perfil determinado	• La autenticación automática provee inteligencia a la red al adaptar automáticamente a los usuarios que se mueven dentro de ella, sin comprometer la seguridad de la misma.

- **Características detalladas del conmutador**

  El conmutador cuenta con 24 puertos 10/100/1000 Base-T, cuatro puertos fijos SPF+ (1G/10G) y dos puertos de 20GigE para enlace de chasis virtual. Incluye un co-procesador para servicios avanzados de red.
  El conmutador cuenta con una capacidad de conmutación máxima de 264 Gb/s, las cuales se suman en modo de chasis virtual.
  Los conmutadores soportan redundancia 1+1 en fuentes de poder, además de que éstas pueden ser cambiadas o reemplazadas durante la operación del conmutador.

  - **Configuración y administración simplificadas**

    - Interfaz de línea de comandos intuitiva en un ambiente programable de Python y Bash a travpes de la consola, Telnet o Shell Seguro (SSH V2) para IPv4 e IPv6.
    - Interfaz Web gráfica para administración del equipo a través de HTTP y HTTPS para IPv4 e IPv6.
    - Utilización del Protocolo SNMP en sus versiones 1, 2 y 3 para la administración y generación de reportes, y para facilitar la administración de la red a terceros.
    - Carga de archivos por medio de USB, TFTP, FTP, SFTP o SCP a través de IPv4 e IPv6.
    - Dirección IP de Loopback para la administración por servicio.
    - Monitoreo basado en políticas y en puertos.
    - sFlow V5 y Monitoreo Remoto de la Red (RMON).
    - Detección de Enlace Unidireccional (UDLD) y Monitoreo de Diagnóstico Digital (DDM).
    - Soporte de servidor DHCP v4 y DHCP v6.
    - Soporte de Protocolo de Tiempo de Red (NTP).
    - Acceso al sistema operativo mediante el uso de Bluetooth para eliminar el uso de cables de consola.

- **Resistencia y Alta Disponibilidad**
  - Administración Unificada, Tecnología de Chasis Virtual.
  - ITU-T G.8032/Y1344 2010: Ethernet Ring Protection.
  - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), IEEE 802.1D Spanning Tree Protocol (STP) y IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).
  - Per-VLAN spanning tree (PVST+) y modo STP 1x1.
  - IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP).
  - Virtual Router Redundancy Protocol (VRRP) con capacidades de rastreo.
  - Fuentes de poder redundantes con capacidad de cambio durante la operación.
  - Bandejas de ventiladores redundantes y con capacidad de cambio durante la operación.
  - Protección interna en el CPU contra ataques maliciosos.
  - Protección contra la separación del chasis virtual: detección y recuperación cuando sucede una separación del chasis virtual debido a la pérdida de un VFL o a la falla de alguno de los equipos.
  - Monitoreo basado en políticas y en puertos.

- **Seguridad Avanzada**

  - Soporte de 802.1X multi-cliente y multi-VLAN para servicios de SPBM/VXLAN.
  - Guardián de Acceso para control de acceso a la red basado en políticas de usuario coherentes.
  - Acceso basado en web (Portal cautivo): un portal web personalizable que reside en el conmutador.
  - Simplificación del control de acceso a la red al asignar dinámicamente políticas de configuración predefinidas a usuarios autenticados (VLAN, ACL, BW).
  - Acceso basado en MAC para usuarios sin 802.1X.
  - SSH con Infraestructura de Llave Pública (PKI) para servicios SPBM/VXLAN.
  - Soporte de cliente Terminal Access Controller Access-Control System Plus (TACACS+).

  - Administrador centralizado de autenticación, Remote Access Dial-In User Service (RADIUS) y Lightweight Directory Access Protocol (LDAP).
  - Learned Port Security (LPS) o bloqueo de direcciones MAC.
  - Filtrado de IP de origen como un mecanismo de protección y eficaz contra los ataques ARP.

- **Calidad de Servicio (QoS)**

  - Colas de prioridad: ocho colas de prioridad por puerto.
  - Priorización de tráfico.
  - Administración de tráfico y de ancho de banda basada en flujo.
  - Clasificación de máscaras no contiguas para IPv4 (32 bits) e IPv6 (128 bits).
  - Evasión de Congestión: Soporte de prevención de bloqueo end-to-end head-of-line (E2E-HOL), IEEE 802.1Qbb control de flujo basado en prioridades y control de flujo IEEE 802.3x.

- **Enrutamiento IPv4**

  - VRF múltiple.
  - Enrutamiento estático con etiquetado de ruta.
  - Protocolo de Información de Ruta (RIP) v1 y v2.
  - Open Shortest Path First (OSPF v2).
  - Protocolo Sistema Intermedio a Sistema Intermedio (IS-IS).
  - Border Gateway Protocol (BGP v4).
  - Encapsulación Genérica de Enrutamiento (GRE) y túneles IP/IP.
  - Virtual Router Redundancy Protocol (VRRP v2).
  - Servidor DHCP v4.
  - Enrutamiento basado en políticas y servidor de balanceo de cargas.

- **Enrutamiento IPv6**

  - VRF múltiple.
  - Protocolo de Control de Mensaje de Internet (ICMP v6).
  - Enrutamiento estático.
  - Protocolo de información de Ruta de Siguiente Generación (RIPng).
  - OSPF v3.
  - IS-IS.
  - IS-IS con topología multiple.
  - Extensiones multiprotocolo de BGP v4 para enrutamiento en IPv6 (MP-BGP).
  - VRRP v3.
  - Protocolo de Descubrimiento de Vecinos (NDP).
  - Enrutamiento basado en políticas y servidor de balanceo de cargas. Servidor DHCP v6.

- **Multicast (IPv4/IPv6)**

  - Protocolo de Administración de Grupos de Internet (IGMP v1/v2/v3).
  - Protocolo de Multicast Independiente en Modo Esparcido (PIM-SM) y Multicast de Fuente Específica (PIM-SSM).
  - Protocolo de Multicast Independiente en Modo Denso (PIM-DS) y Bidireccional (PIM-BiDir).
  - Protocolo Vector-Distancia de Enrutamiento de Multicast (DVMRP).

- **Servicios avanzados para voz, vídeo y datos**

  - Detección del Protocolo de Inicio de Sesión (SIP), monitoreo de la sesión y rastreo.
  - Perfil SIP para QoS, sintonización de prioridad para procesos de extremo a extremo.

- **Servicios Avanzados de Capa 2**

  - Soporte de servicios de Ethernet mediante el uso del protocolo 802.1ad (también conocido como Q-in-Q o apilamiento de VLAN).
  - Servicios de Virtualización 802.1aq Shortest Path Bridging (SPB-M).
  - Identificación de perfiles SAP.
  - Soporte de VLAN de servicio (SVLAN) y VLAN de cliente (CVLAN).
  - Soporte de tramas JUMBO.

2.4. Componentes de los equipos de la capa de núcleo

Una vez descritas las características técnicas de los equipos que se consideraron dentro de la propuesta para formar la capa de núcleo, se mencionan los componentes y cantidades necesarias para la solución.

- **Conmutadores de Red**

  Se consideraron **ocho conmutadores de red** de una unidad de rack con un total de 32 puertos fijos QSFP+ (40GigE) en el panel frontal.

  Como se mencionó, cada sitio estaría compuesto por *dos conmutadores en chasis virtual*. Para poder tener un chasis virtual se debe establecer un *Enlace Virtual de la Tarjeta de Fábrica (Virtual Fabric Link – VFL)*. Se consideraron *dos cables de conexión directa* de tres metros con transceptores de 40GigE para una conexión full-duplex. En total, se consideraron *ocho cables*.

  Para poder habilitar la función de chasis virtual y enrutamiento avanzado es necesario adquirir una *licencia*. Esta licencia se debe habilitar por cada conmutador, por lo que se contempló un total de *ocho licencias*.

  También se requiere una licencia por equipo para activar las funcionalidades de centro de datos, por lo que se consideraron ocho licencias más.

  Debido a que los cuatro sitios que se tienen contemplados para colocar los equipos de núcleo están localizados a más de 10 km de distancia entre sí, se propuso establecer la conexión entre ellos con enlaces de 10Gb, con el fin de hacer menos costosa la solución. Se propuso el uso de transceptores *SFP-10G-LR*, que *soportan fibra óptica monomodo* en una longitud de onda nominal de *1310 [nm]* con un conector LC. El alcance típico para evitar dispersión y pérdidas de la señal óptica es de 10 km, en una fibra de 9 [µm] o 125 [µm] de núcleo. Se propuso enlace full-duplex, por lo que se consideraron un total de ocho transceptores.

  Para asegurar la alta disponibilidad se consideró una fuente de poder de corriente alterna de 450 W adicional por cada equipo y se propone también, adquirir bandejas de ventiladores en caso de que se presente alguna falla.

En la tabla 4 se muestra el resumen de los componentes activos, licencias y cables que se contemplaron dentro de la propuesta, para formar la capa de núcleo de la red.

Tabla 4

Cantidad	Equipo
8	Conmutador de red de una unidad de rack con 32 puertos QSFP+ (40GigE). El conmutador incluye una fuente de poder de corriente alterna de 450 W, cordón de energía, manuales de usuario, montajes para el bastidor y adaptador de USB a RJ-45.
8	Licencia Advanced routing software. Incluye soporte para Policy Based Routing, VRF, BGP, OSPFv2, PIMSM/DM, DVMRP, IPv6 Routing, OSPFv3, RIPng, VRRPv3, SPB y Chasis Virtual (VC).
8	Data Center Software para el Soporte de DCBX, FCoE y EVB.
8	Fuente de poder de respaldo modular en corriente alterna que provee enfriamiento de frente hacia atrás.
8	Cables de conexión directa QSPF+ (40GigE) de 3 m.
8	Transceptor *SFP-10G-LR.*

2.5. Componentes de los equipos de la capa de distribución

- **Conmutadores de Red**

  Se consideraron un total de veintidós conmutadores de red, los cuales cuentan con un total de 20 puertos fijos SFP+ 1/10 GigE, dependiendo del transceptor que se utilice, y un módulo de expansión en la parte frontal.
  Al igual que en la capa de núcleo, se propuso que los equipos de la capa de distribución estuvieran en chasis virtual, esto con el fin de facilitar la administración de la red y de tener mayor capacidad de conmutación y mayor disponibilidad de puertos.

  Como se mencionó, es necesario contar con una licencia por equipo para habilitar la función de chasis virtual y las funciones de enrutamiento avanzado. En los equipos de la capa de distribución es imprescindible contar con protocolos de enrutamiento avanzado, pues es precisamente en esta capa donde se lleva a cabo la elección de la ruta de los diferentes paquetes dentro de la red.

  Para poder establecer el chasis virtual en estos conmutadores es necesario agregar un módulo con puertos que ofrezcan tasas de transmisión de 40Gbps. Se consideró agregar un módulo con tres interfaces QSPF+ (40GigE) y tres transceptores QSFP-40G-LR, que soporta fibra óptica monomodo a través de la longitud de onda de 1310 [nm], con un alcance típico de 10 km y con conectores LC dúplex. En total, se consideraron veintidós módulos y sesenta y seis transceptores QSPF+.

  Evidentemente, el costo es muy elevado respecto al enlace de 10Gbps, por lo que se ofreció la opción de establecer el chasis virtual a 10Gbps, teniendo en cuenta que no se tendría la misma tasa de transferencia de datos.

  Para hacer la conexión de chasis virtual a 10Gbps se considera un módulo que ofrece cuatro puertos SFP+ y se consideran transceptores *SFP-10G-LR.*

  Las conexiones hacia la capa de núcleo se propusieron a 10Gbps, debido a que las distancias de distribución a núcleo excedían, en la mayor parte de los casos, los 10 km. Se propuso un doble enlace a cada equipo de núcleo, por lo que se consideraron un total de ochenta y ocho transceptores *SFP-10G-LR*.

En la tabla 5 se muestra el resumen de los componentes activos, licencias y cables que se contemplaron dentro de la propuesta, para formar la capa de distribución de la red.

Tabla 5

Cantidad	Equipo
22	Conmutador de red de una unidad de rack con 20 puertos SFP/SFP+ (1/10GigE) y un módulo de expansión adicional. El conmutador incluye una fuente de poder de corriente alterna de 450 W, cordón de energía, manuales de usuario, montajes para el bastidor y adaptador de USB a RJ-45.
22	Licencia Advanced routing software. Incluye soporte para Policy Based Routing, VRF, BGP, OSPFv2, PIMSM/DM, DVMRP, IPv6 Routing, OSPFv3, RIPng, VRRPv3, SPB y Chasis Virtual (VC).
22	Fuente de poder de respaldo modular en corriente alterna que provee enfriamiento de frente hacia atrás.
22	Módulo de expansión que brinda 3 puertos QSFP+ (40GigE).
66	Transceptor QSFP-40G-LR, soporta fibra óptica monomodo en una longitud de onda de 1310 nm con un alcance típico de 10 km.
88	Transceptor *SFP-10G-LR.*

Para optimizar el costo de la solución, se propone establecer el chasis virtual a 30Gbps, utilizando tres enlaces de 10Gbps por conjunto de equipos, tal como se muestra en la tabla 6.

Tabla 6

Cantidad	Equipos
66	Transceptor SFP-10G-LR, soporta fibra óptica monomodo en una longitud de onda de 1310 nm, con un alcance típico de 10 km.

2.6. Componentes de los equipos de la capa de acceso

- **Conmutadores de Red**

  Se consideró un total de 175 conmutadores de red de una unidad de rack con 24 puertos 10/100/1000 Base-T, cuatro puertos fijos SPF+ (1G/10G) y dos puertos de 20GigE para enlace de chasis virtual. Incluye un co-procesador para servicios avanzados de red.

  En este caso no era necesario el uso de un chasis virtual, pero sí que el conmutador tuviera disponibilidad de puertos en caso de requerirlo en un futuro.

  Se propuso que en el acceso se tuvieran puertos disponibles de 10GigE, con el fin de que la dependencia pudiera utilizarlos para algunas aplicaciones de red, así como para enlace a los equipos de distribución. Por ello, se consideraron *trescientos cincuenta transceptores SFP-10G-LR*, que *soportan fibra óptica monomodo* en una longitud de onda nominal de *1310 [nm]* con un conector LC. El alcance típico para evitar dispersión y pérdidas de la señal óptica es de 10 km, en una fibra de 9 [µm] o 125 [µm] de núcleo.

  Debido a que los conmutadores de acceso son los que permiten la entrada a la red a los usuarios, se propuso la integración de servicios que pudieran detectar las aplicaciones que se ejecutan por usuario. Esta capacidad viene incluida en el conmutador con un procesador dedicado. La tecnología que permite la detección de las aplicaciones que se ejecutan dentro de la red se llama *Inspección Profunda de Paquetes*, *DPI* por sus siglas en inglés. DPI es una forma de filtrado de paquetes de red de computadoras que examina la parte de datos, y posiblemente también la cabecera, de un paquete a medida que pasa un punto de inspección, en busca de protocolo incumplimiento, virus, spam, intrusiones, o criterios definidos para decidir si el paquete puede pasar o si necesita ser encaminado a un destino diferente, o, con el propósito de recopilar información estadística.

  DPI combina la funcionalidad de un sistema de detección de intrusiones (IDS), y un sistema de prevención de intrusiones (IPS) con un firewall tradicional. Esta combinación hace posible la detección de ciertos ataques que ni los IDS / IPS ni el firewall pueden atrapar por su propia cuenta.

Por otra parte, es en los conmutadores de acceso donde se lleva a cabo el proceso de perfilamiento de usuario, el cual otorga a cada usuario un perfil que pertenecerá a una VLAN determinada con ciertos atributos y de manera automática, es decir, sin necesidad de intervención por parte del personal de tecnologías de la información.

Se propuso que el perfilamiento automático fuera una funcionalidad integrada en el conmutador, por lo que no es necesario el uso de hardware ni software adicional.

En la tabla 7 se muestran los componentes que se tomaron en cuenta para poder formular la propuesta de la capa de acceso de la red.

Tabla 7

Cantidad	Equipo
175	Conmutador de red Gigabit Ethernet L2/L3 en configuración fija de una unidad de rack con 24 puertos PoE+ RJ-45 10/100/1000, 4 de ellos proporcionan 60 W. 4 puertos fijos SFP+ (1G/10G) y 2 puertos de apilamiento de 20 GigE. Se incluye un co-procesador para servicios de red avanzados. Se incluye también una fuente de poder de CA de 600 W con soporte de PoE, cordón de energía, manuales de usuario, monturas para un bastidor de 19 pulgadas y un adaptador de micro USB a USB.
175	Fuente de poder de respaldo modular en corriente alterna que provee enfriamiento de frente hacia atrás.
350	Transceptor *SFP-10G-LR.*

2.7. Especificaciones de Fibra Óptica

Las especificaciones de la fibra óptica a utilizar para el desarrollo de este proyecto son las siguientes:

- Se utilizarán tres tipos de fibra óptica

    - Fibra óptica monomodo de 72 hilos
    - Fibra óptica monomodo de 12 hilos
    - Fibra óptica multimodo de 12 hilos

Cada uno de estos tendidos de fibra será utilizado para fines distintos en común acuerdo con la dependencia.

2.7.1 Especificaciones de la Fibra Óptica Monomodo

El tendido de fibra óptica monomodo cumple con los estándares establecidos en las normas ITU-T G.652.C y con la norma ITU-T G.652.D, conforme al listado siguiente:

- **Especificaciones Dimensionales**

    - **Revestimento**
    - Diámetro: 125 $\pm$ 0.7µm

    - **Recubrimiento**
    - Diámetro exterior: 245 ± 5 µm
- **Especificaciones Ópticas**

    - **Coeficientes de Atenuación**
    - 1310 nm $\leq$ 0.35/0.37 dB/km
    - 1383 nm $\leq$ 0.31/0.33 dB/km
    - 1550 nm $\leq$ 0.21/0.23 dB/km
    - 1625 nm $\leq$ 0.23/0.35 dB/km

    - **Atenuación por Curvatura**
    - 100 vueltas, 50 mm de diámetro a 1550 nm $\leq$ 0.05 dB

- **Coeficientes de Dispersión**
- De 1285 a 1330 nm ≤ ps/(nm*km)
- A 1550 nm ≤ 18 ps/(nm*km)
- A 1625 nm ≤ 22 ps/(nm*km)

- **Longitud de Onda de Dispersión Cero (λ_0)**
- De 1302 a 1322 nm

- **Dispersión del Modo Polarizado**
- ≤ 0.2 ps/km

- **Dispersión del Modo Polarizado en un Enlace**
- ≤ 0.08 ps/km

- **Longitud de Onda de Corte**
- ≤ 1260 nm

2.7.2 Especificaciones de la Fibra Óptica Multimodo

El tendido de fibra óptica multimodo cumple con los estándares establecidos en las normas ITU-T G.651, conforme al listado siguiente:

- **Especificaciones Dimensionales**

  - **Revestimento y Núcleo**
  - Diámetro del núcelo: 62.5 $\pm$ 2.5 µm
  - Diámetro del revestimento: 125 $\pm$ 1 µm

  - **Recubrimiento**
  - Diámetro exterior 245 $\pm$ 10 µm

- **Especificaciones Ópticas**

  - **Coeficientes de Atenuación**
  - 850 nm $\leq$ 2.9/3.0 dB/km
  - 1300 nm $\leq$ 0.6/0.7 dB/km

  - **Ancho de Banda Modal**
  - 850 nm $\geq$ 200 MHz*km
  - 1300 nm $\geq$ 600 MHz*km

  - **Apertura Numérica**
  - 0.275 $\pm$ 0.015

3. RESULTADOS OBTENIDOS

El proyecto realizado tenía varios objetivos, sin embargo, el objetivo principal, era diseñar una red multiservicios que fuera para la dependencia, una solución integral y de vanguardia que a su vez, resolviera cada una de las necesidades tecnológicas de dicha dependencia.

Como resultado se obtuvo el diseño de una red simplificada, segura y optimizada, que hará que los usuarios tengan la mejor experiencia en cuanto a servicios.

Diseñar esta red no fue cosa sencilla. Se tuvieron que tomar en cuenta muchos factores como el número de usuarios, el tipo de servicios que formarían parte de la red, el tipo de medio que se utilizaría para la interconexión de cada equipo, entre otros. Sin embargo, se tomaron en cuenta las mejores prácticas del fabricante y se propusieron los equipos adecuados para cumplir con las necesidades tecnológicas de la dependencia. Es evidente que para seleccionar no sólo los equipos, si no los transceptores, conectores, tipos de cable, tipos de fibra, se llevó a cabo un levantamiento exhaustivo en cada uno de los sitios en los que se colocarían los equipos. El levantamiento fue puramente físico, es decir, solamente se observó el hardware y las trayectorias de la fibra y cables, pues la configuración de los equipos, se mantiene en forma confidencial hasta comenzar la fase de implementación.

Posterior a realizar el diseño de la red, se presentó con el cliente y se le explicó de manera detallada cada equipo, cada funcionalidad, las ventajas que obtendrá al implementar la red, entre otras. Lo más importante fue dar una demostración acerca de la solución. Se mostró, a nivel de acceso, la seguridad embebida en el conmutador, para que el cliente pueda autenticar a cada uno de los usuarios que ingresan a la red, asignarles la vlan a la que pertenecen de acuerdo a su perfil con los atributos configurados para cada uno de éstos entre otras.

También se mostró el tratamiento a nivel de capa siete que hace el conmutador. Para mostrar esta funcionalidad se hizo uso de un sistema de gestión de red propietario, el cual se integra con el conmutador a través de una licencia.

El sistema de gestión de red muestra de manera gráfica lo siguiente:

- Las 10 aplicaciones que se están ejecutando dentro de la red y el uso de ancho de banda que hacen
- El comportamiento de los usuarios dentro de la red y las aplicaciones que están ejecutando
- Muestra una gráfica del comportamiento que ha tenido la red dentro de un lapso de tiempo para poder determinar un comportamiento futuro
- El estado de salud de los equipos que están dentro de la red. En este aspecto, el sistema de gestión es capaz de observar los equipos propietarios del fabricante, así como equipos de terceros, teniendo control parcial sobre ellos.

Adicional a esto, el sistema de gestión puede generar reportes, activar alarmas para que en caso de que algún equipo tenga una falla, se mande una alerta ya sea a un correo electrónico o como mensaje de texto a un teléfono móvil.

El sistema de gestión tiene una base de datos de 2000 firmas de aplicaciones, las más populares dentro del mercado. Se pueden añadir firmas de aplicaciones de desarrollo propio, con el fin de que el sistema sea capaz de monitorearla y tomar decisiones sobre ella.

Estas funcionalidades fueron de gran aporte para el cliente, pues es una herramienta que brinda muchas facilidades para la gestión y la toma de decisiones dentro de la red, a la vez que se puede optimizar el uso del ancho de banda, dando prioridad a aquellas aplicaciones de uso crítico y descartando aquellas que son innecesarias para cuestiones corporativas.

Para la parte de la capa de núcleo se mostraron al cliente diversas funcionalidades, como las siguientes:

- Provisión sin intervención y automatización de redes con estructura automatizada de conexión y uso inmediatos para detectar topologías y protocolos de forma automática. La detección automática de protocolos y el auto-aprovisionamiento funcionan con cualquier dispositivo de red que sea compatible con los protocolos estándar más utilizados.
  Esto hace sentido en la cuestión de chasis virtual, pues éste se auto-configura sin intervención alguna por parte de un usuario.

- Alta disponibilidad en chasis virtual. Esta funcionalidad se mostró ejecutando aplicaciones de vídeo y voz en una maqueta. La prueba consistió en desconectar el conmutador primario del chasis virtual para que el secundario tomara el rol del anterior sin perder los servicios ejecutados en ese momento. El objetivo de esta prueba fue mostrar al cliente que, aunque un elemento dentro del chasis virtual se pierda, los servicios seguirán intactos para el usuario, será trabajo del departamento de TI resolver el problema, lo cual se facilita enormemente gracias al sistema de gestión.

Sin duda alguna, lo que se mostró al cliente fue determinante para que éste quedara convencido de que la solución ofrecida era la que necesitaba.

Lo siguiente es realizar una prueba de concepto en sitio para poder probar en producción las soluciones.

4. PARTICIPACIÓN PROFESIONAL EN EL PROYECTO

Dentro del proyecto realicé varias actividades profesionales, las cuales mencionaré a continuación:

- Visité en diversas ocasiones al cliente para presentarle en principio, el catálogo de productos y los casos de éxito a nivel mundial de la solución. Posteriormente se tuvieron sesiones en conjunto con el fabricante para definir los alcances del proyecto y con ello tomar la decisión de cómo se diseñaría la red.
- Visité el sitio central del cliente para llevar a cabo el levantamiento físico de los equipos de voz y de datos. Como lo mencioné, el levantamiento fue puramente físico. Dentro del sitio central pude observar los conmutadores de red y servidores que actualmente tiene la dependencia, que son equipos de poca capacidad, pues en la parte de núcleo tiene chasises tradicionales a 1000 Mbps de velocidad, los cuales resultan insuficientes para cubrir las necesidades tecnológicas de la dependencia.

  Además de esto, el equipo de núcleo no tiene redundancia activa, por lo que en caso de que el equipo quede fuere de operación, los servicios de red se verán sumamente afectados, poniendo en riesgo la integridad de la información que se maneja.

  También, durante el levantamiento, tomé en cuenta el número de puertos en fibra y en cobre, la velocidad a la que se encontraban y, para saber hacia qué sitios se dirigía cada enlace, me basé en un diagrama topológico que me proporcionó la dependencia. En dicho diagrama se describía la cantidad de usuarios que habría por sitio y, partir de ahí, pude definir la cantidad de nodos a considerar en el proyecto.

  Teniendo en cuenta lo anterior, pude tomar la decisión de qué equipo proponer para colocarlo como núcleo de la red.

  Propuse un conmutador de alta capacidad de una sola unidad de rack. Este equipo tiene 32 puertos que pueden operar en 40GigE y mediante divisores ópticos, se puede llegar a tener una densidad de 96 puertos de 10GigE. Eso quiere decir que en un esquema de chasis virtual, consideré dos conmutadores en un sitio y dos conmutadores como respaldo en los otros tres sitios, se tienen 192 puertos de 10GigE, capacidad más que suficiente para satisfacer las necesidades tecnológicas de la dependencia.

  Cada conmutador tiene una capacidad de conmutación de 2.56 Tbps, en un chasis virtual, esa capacidad se suma por cada unidad que se agregue a éste, lo que implica que se consideró una capacidad de conmutación de 5.12 Tbps en el sitio central.

Teniendo ya los equipos destinados a la formar la capa de núcleo de la red, procedí a analizar qué tipo de interfaces se colocarían para los enlaces y enlaces agregados.

Para el chasis virtual consideré un enlace virtual de 240 Gbps en full-dúplex con transceptores QSFP+ de 40GigE.

Los enlaces agregados hacia la capa de distribución los consideré a 10GigE por medio de fibra monomodo. Para lograrlo, seleccioné transceptores de rango extendido, debido a que la distancia entre los sitios excedía el kilómetro de longitud. La distancia la determiné con el mapa topológico y con ayuda directa del cliente.

Para la capa de distribución seleccioné equipos similares a los de la capa de núcleo, debido a que en ellos residirá la mayor parte del tráfico y requieren una capacidad de conmutación robusta. Son conmutadores de 48 puertos de 10GigE y 8 puertos de 40GigE, sin embargo mediante divisores ópticos se puede tener una densidad de 72 puertos de 10GigE en una sola unidad de rack.

En estos conmutadores se llevará a cabo el enrutamiento mediante el protocolo OSPF, sin embargo no pude tener acceso a la configuración actual de la red, por lo que este tema se revisará con el cliente una vez que comience la fase de implementación.

Los enlaces hacia la capa de acceso fue uno de los temas más complejos dentro del diseño de la red, pues debido a que se trata de una red metropolitana, los sitios en los que se colocarán los conmutadores de acceso están bastante distantes de los conmutadores de distribución. Consideré dichos enlaces con tecnología 10GigE, por lo que los transceptores no solamente fueron de rango grande, sino de rango extendido, que soportan distancias de hasta 40km mediante fibra monomodo. Para determinar qué tipo de transceptor se colocaría, tuve que hacer uso de mapas aproximados, pues en el mapa topológico no se especificaban las distancias requeridas.

Cada conmutador de acceso está dotado de 4 interfaces SFP+ de 10GigE. Los enlaces hacia los conmutadores de distribución fueron considerados dobles con el fin de ofrecer redundancia, alta disponibilidad y balanceo de cargas en caso de ser requerido.

En la parte del acceso, consideré conmutadores de 48 puertos con PoE, debido a que la dependencia pretende incrementar el número de usuarios y de servicios, por lo que si hubiera considerado conmutadores de 24 puertos, se limitaba el crecimiento.
Los conmutadores de acceso son muy particulares en el mercado, pues tienen la capacidad de ofrecer servicios a nivel de capa 7. Estos servicios residen en un co-procesador integrado en el conmutador, con el fin de no mermar la capacidad o el rendimiento del éste.
Además de las funciones de capa 7, el conmutador de acceso funciona como un servidor de control de acceso a la red, funcionalidad que agrega mucho valor a la solución, pues ya no se requiere hardware ni software adicional para tener una red segura. Hice mucho énfasis en esta funcionalidad pues una red segura es lo más importante para cualquier institución.

- Elaboré la propuesta económica, considerando servicios de implementación y la capacitación tanto a los administradores de la red como a los usuarios finales.
  Esta propuesta se mantendrá confidencial hasta que el proyecto detone en su fase de asignación.

5. CONCLUSIONES

De la realización de este proyecto se pueden concluir varias cosas, las cuales mencionaré a continuación:

Se lograron identificar las necesidades de la infraestructura de red actual y con ello se propuso una arquitectura simplificada que brindara a los usuarios una experiencia diferente y que a su vez optimizara económica y operativamente la gestión de la red.

Al optimizar la gestión de la red, el personal de tecnologías de la información de la dependencia puede ocupar su tiempo en nuevos desarrollos tecnológicos y no en problemas propios de la red. Además, se propusieron a la dependencia equipos de vanguardia que aseguran al menos 5 años de avance, pues el hardware para el núcleo de la red, está preparado para soportar interfaces de 100 GigE.

Dentro* de la solución, se propuso a la dependencia tener un gestor de red que pudiera tener visibilidad, tanto de los equipos como de las aplicaciones que están ocupando el ancho de banda de la red, esto sin tener que agregar módulos o equipos adicionales. Al agregar esta solución, la dependencia puede tener la seguridad de que su ancho de banda estará siendo utilizado óptimamente, dando prioridad a aplicaciones que realmente requieran la utilización de éste. Además, puede tener visibilidad de todos y cada uno de los equipos que conforman la red, facilitando la gestión y la operación de concluir que de ésta.

En este sentido, se puede concluir que el objetivo primordial se logró, pues se le presentó al cliente una solución innovadora que cumple, no sólo con sus necesidades actuales, sino que asegura que la infraestructura propuesta estará preparada para las nuevas tecnologías del futuro.

Se logró llevar a cabo un análisis y realizar un estudio de la red actual de la dependencia, y se tomó la decisión de diseñar una nueva red que pudiera optimizar y brindar mejoras en la operación e implementación de dicha red.

El diseño de la solución se realizó de tal manera que se pudiera reducir complejidad a la operación de la red y de cierta forma, agregar valor al diseño. Esto quiere decir que no se reemplazarían los equipos actuales con las mimas configuraciones, sino que se realizaría una migración tanto física, como lógica, dejando fuera protocolos propietarios que dificultaran la futura implementación.

Además de diseñar una red simplificada, se ofreció una red segura y con alta disponibilidad, para que no se perdiera comunicación e información en caso de que llegase a presentarse alguna contingencia.

El hecho de que los conmutadores de red de acceso tengan integradas funciones de UTM básicas, fue una gran diferencial para el diseño, pues mediante esta funcionalidad se puede tener aún más seguridad en el borde.

Se propuso a la dependencia que adquirieran un Sistema de Administración de Red, el cual puede realizar múltiples funciones, tales como generación de reportes, detección de comportamientos anómalos dentro de la red, administración del ancho de banda, monitoreo de las aplicaciones que se están ejecutando y que ocupan una gran cantidad de recursos dentro de la red, entre otros. La adquisición de esta herramienta podría brindar a la dependencia más facilidades en cuanto a la administración de la red, a la vez que robustece aún más a la solución propuesta y asegura la máxima satisfacción del usuario.

Se lograron construir especificaciones técnicas detalladas de la solución propuesta, y con ello se pudo asegurar que la dependencia estará adquiriendo equipos de la más alta tecnología que asegura una óptima operación de la red y que ésta estará preparada para las tecnologías futuras.

Los equipos propuestos no hacen uso de protocolos propietarios, sino que utiliza estándares abiertos, lo que garantiza que puede interoperar con equipos de otras marcas sin presentar problema alguno.

Con el detalle de cada una de las funcionalidades y de los estándares que tienen los equipos, la dependencia puede encontrar el mejor uso de cada equipo y explotar al máximo el desempeño de éstos, logrando con ello mejoras que brindarán a los usuarios finales una gran experiencia al hacer uso de sus aplicaciones.

Es importante mencionar que el personal de la dependencia, recibirá la capacitación técnica adecuada con el fin de que pueda operar de la mejor manera la red y hacer uso de todas las funcionalidades y facilidades que tienen los equipos. Con ello, se puede asegurar que los usuarios no presenten queja alguna de los servicios brindados por el personal de TI de la dependencia.

7. BIBLIOGRAFÍA

- Gil Vázquez Pablo, “Redes y Transmisión de Datos”, Publicaciones de la Universidad Alicante, 2010.

- "Software-Defined Networking: The New Norm for Networks". White paper. Open Networking Foundation. Abril 13, 2012.

- James F. Kurose, Keith W. Ross (2012). *Computer Networking:A Top-Down Approach*. Pearson Education. ISBN 978-0-13-136548-3.

- Lyle Brown Edwin, “802.1x: Port Based Authentication”, Taylor and Francis Group, 2007.

- http://enterprise.alcatel-lucent.com/assets/documents/EMG5246110102_Application_Fluent_Network_EN.pdf

7. ANEXO

En este anexo se presentarán algunas de las configuraciones recomendadas para la red del cliente, las cuales incluyen protocolos como OSPF, VRRP y también políticas para la autenticación de los usuarios.

La siguiente configuración, corresponde a un esquema de enrutamiento de OSPF, en el que se consideran dos áreas, una stub área y el área de backbone.

```
ip load ospf
ip ospf area 0.0.0.2
ip ospf area 0.0.0.2 type stub
ip ospf interface "C1-D1"
ip ospf interface "C1-D1" area 0.0.0.0
ip ospf interface "C1-D1" status enable
ip ospf status enable
ip ospf interface "vlan51"
ip ospf interface "vlan51" area 0.0.0.0
ip ospf interface "vlan51" status enable
ip ospf interface "vlan54"
ip ospf interface "vlan54" area 0.0.0.2
ip ospf interface "vlan54" status enable
ip ospf interface SW3-SW1 auth-type md5
ip ospf interface SW3-SW2 md5 7
ip ospf interface SW3-SW2 md5 7 key XXXXX
ip ospf interface vlan-21 hello-interval 0
ip ospf interface vlan-21 dead-interval 0
```

En este script se está creando el área 0.0.0.2, que es un área stub. Evidentemente, dentro de todo esquema de OSPF debe existir el área cero, que va ligada al área backbone.

Se están asignando interfaces para cada una de las áreas, a la vez que las interfaces de los switches que participan en el enrutamiento, SW3 y SW2, se utiliza el método de autenticación MD5, que es un algoritmo que produce un valor criptográfico de 128 bits que, típicamente se expresa en formato de texto como un número hexadecimal de 32 dígitos. En este caso se está especificando una entrada de 7 caracteres, pudiendo usar cualquier serie de caracteres como contraseña.

El siguiente escenario corresponde a la maqueta utilizada para las demostraciones de los equipos con el cliente. La maqueta está basada en el protocolo de autenticación 802.1X, el cual asigna un determinado perfil, que es configurado de acuerdo a lo que el cliente requiera. Con la tecnología utilizada, se tiene la posibilidad de crear hasta 512 perfiles, a los cuales se les pueden asignar los privilegios o limitaciones de red que el cliente elija.

Para este esquema, es necesario contar un servidor de autenticación, el cual es provisto por una máquina virtual Windos Server 2003. Dentro de esta máquina virtual se encuentra un servidor RADIUS, con el cual se validarán las credenciales de cada usuario para provisionar sus servicios de red.

En caso de que el usuario no cuente con autenticación mediante el protocolo 802.1X, se validará como un usuario no suplicante y se llevará a cabo una autenticación basada en MAC Address mediante un portal cautivo que reside en el propio conmutador de red.

Figura 1. Windows Server 2003

Para poder observar el dialogo entre el servidor de autenticación y el conmutador, es necesario contar con un visor de protocolos de red, el cual será prporcionado por la misma interfaz de comandos, haciendo uso del comando **windump –i 1 –vvv udp and port 1812**, como se muestra en la siguiente imagen:

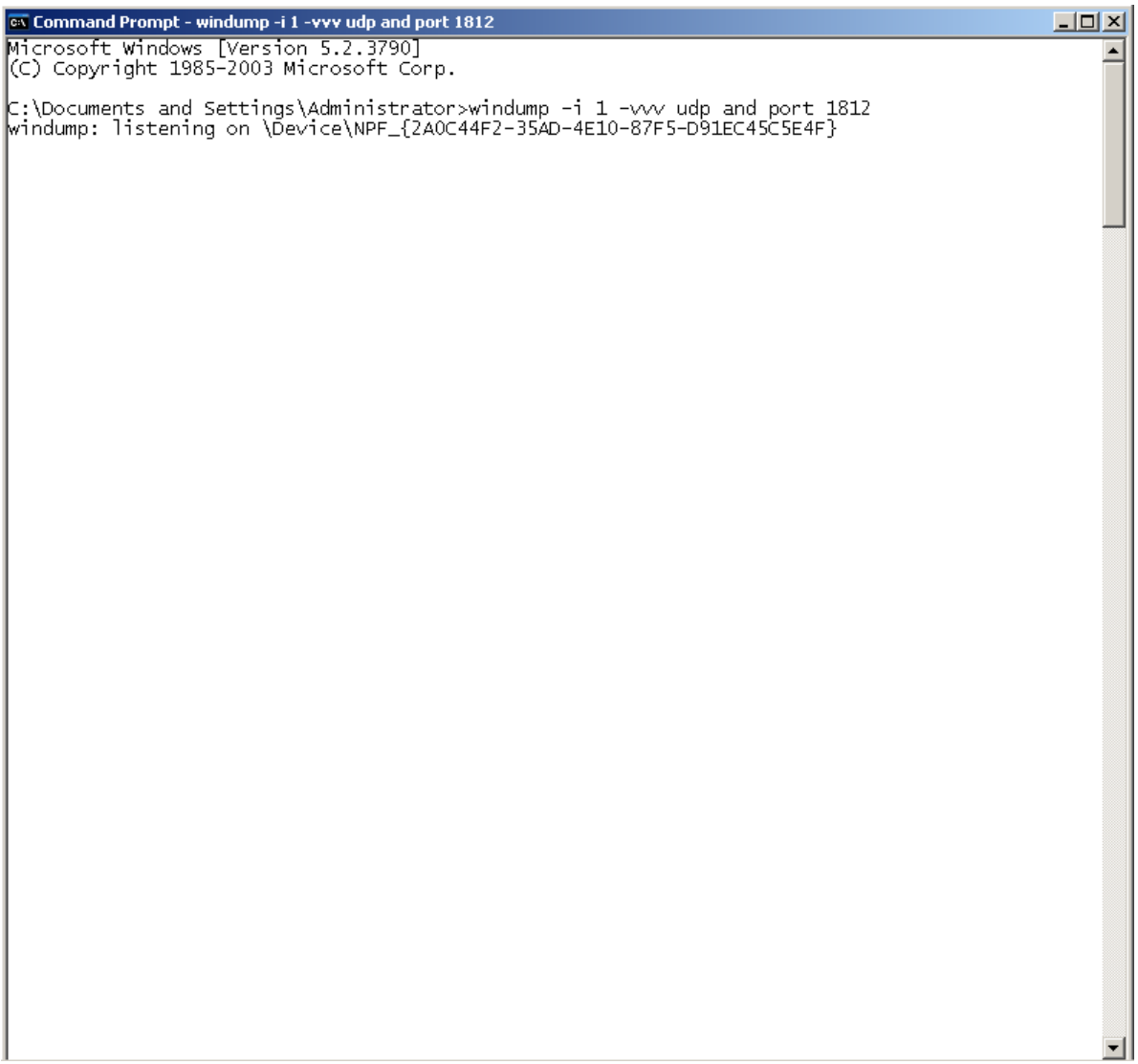


Figura 2. Diálogo entre el conmutador y el servidor RADIUS

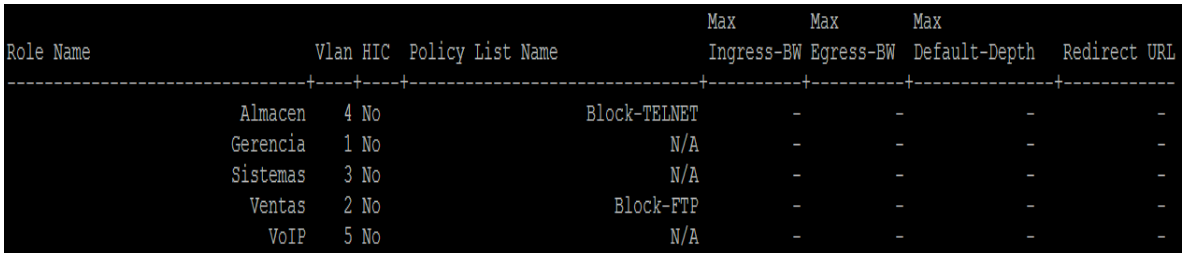
Lo siguiente en esta demostración es verificar la configuración del conmutador de red. Dentro de la configuración se definieron diversas VLAN´s. Es claro que esta configuración dependerá de las necesidades del cliente. En este caso están creadas 5 VLAN's: la VLAN 1 que tiene por nombre "Gerencia", a VLAN 2 que tiene por nombre "Ventas", la VLAN 3 que tiene por nombre "Sistemas", la VLAN 4 que tiene por nombre "Almacen" y la VLAN 5 que tiene por nombre "VoIP".

Cada una de estas VLAN tiene diferentes permisos y está asignada a una interface, en la cual se puede declarar la funcionalidad de movilidad de puerto, tal como se muestra en la siguiente figura:

```
! VLAN :
vlan 1 enable name "Gerencia"
vlan 2 enable name "Ventas"
vlan 3 enable name "Sistemas"
vlan 4 enable name "Almacen"
vlan 5 enable name "VoIP"
vlan 100 enable name "Networking"
vlan 100 port default 1/9
vlan 100 port default 1/10
vlan 172 enable name "Default"
vlan 172 port default 1/1
vlan 172 port default 1/2
vlan 172 port default 1/3
vlan 172 port default 1/4
vlan 172 port default 1/5
vlan 172 port default 1/6
vlan 172 port default 1/7
vlan 172 port default 1/8
vlan port mobile 1/1
vlan port 1/1 802.1x enable
vlan port mobile 1/2
vlan port 1/2 802.1x enable
vlan port mobile 1/3
vlan port 1/3 802.1x enable
vlan port mobile 1/4
vlan port 1/4 802.1x enable
vlan port mobile 1/5
vlan port 1/5 802.1x enable
vlan port mobile 1/6
vlan port 1/6 802.1x enable
vlan port mobile 1/7
vlan port 1/7 802.1x enable
vlan port mobile 1/8
vlan port 1/8 802.1x enable
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:
```

Figura 3. VLAN´s asignadas a un puerto móvil

Estas VLAN´s corresponden a un perfil, es decir, cuando un usuario ingrese a la red, ya sea por medio alámbrico o inalámbrico, dicho usuario será asignado a una VLAN de acuerdo a las credenciales entregadas por el servidor de autenticación. En la siguiente imagen se muestran los permisos que tienen cada una de las VLAN´s:



Role Name	Vlan	HIC	Policy List Name	Max Ingress-BW	Max Egress-BW	Max Default-Depth	Redirect URL
Almacen	4	No	Block-TELNET	-	-	-	-
Gerencia	1	No	N/A	-	-	-	-
Sistemas	3	No	N/A	-	-	-	-
Ventas	2	No	Block-FTP	-	-	-	-
VoIP	5	No	N/A	-	-	-	-

Figura 4. Asignación de Permisos por VLAN

En esta imagen no hay ningún usuario conectado a la red, por ello no se muestran los roles, anchos de banda asignados, entre otros. Sin embargo, se puede ver que cualquier usuario asignado a la VLAN Almacen, no podrá establecer ninguna sesión de Telnet, así como los usuarios asignados a la VLAN Ventas, no podrá hacer uso de FTP.

La importancia de esta demostración radica en proveer al cliente una red segura sin tener que invertir en otra cosa que no sea el conmutador de red, pues estas funcionalidades de perfilamiento y autenticación, están embebidas en el conmutador, sin necesidad de agregar licenciamiento alguno.

Esta demostración se enfoca en usuarios suplicantes que tengan habilitado en su dispositivo el protocolo 802.1x, sin embargo, pude suceder que el dispositivo de algún usuario no tenga ese método de autenticación. En este caso el conmutador de red lo tratará como un dispositivo no suplicante y aplicará algún otro método de autenticación, como se muestra en las siguientes imágenes:

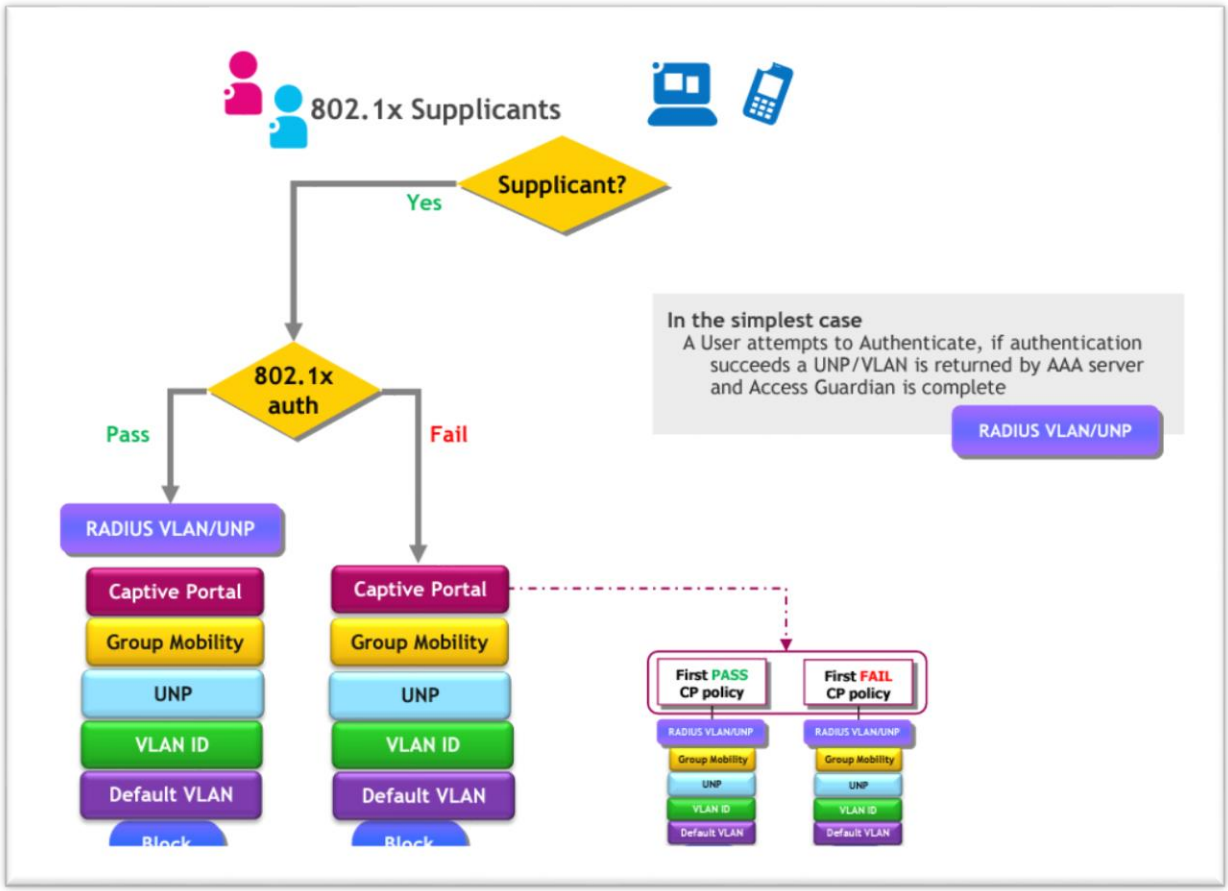


Figura 5. Asignación de Perfil para Usuarios Suplicantes

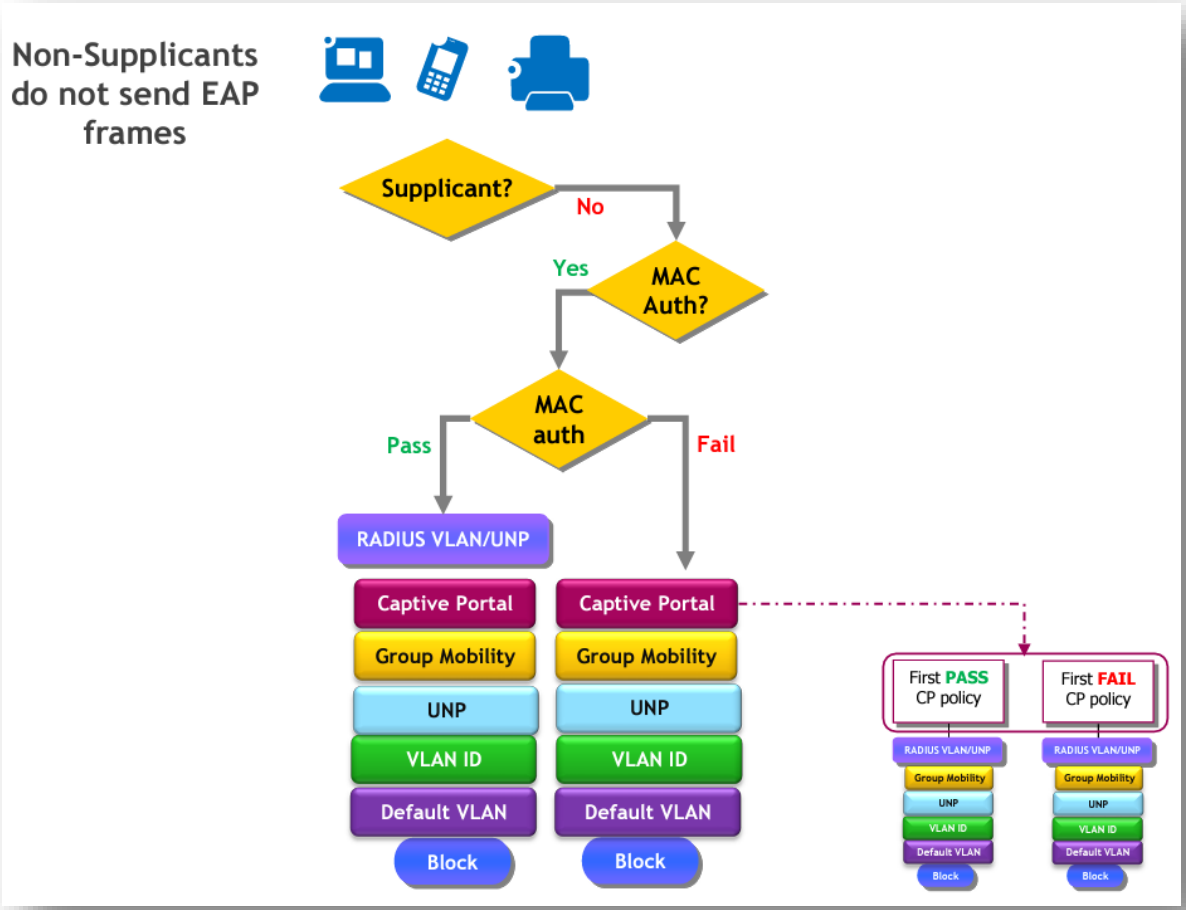


Figura 6. Asignación de Perfil para Usuarios No Suplicantes

Cuando la autenticación falla usando el protocolo 802.1x o bien cuando un usuario no suplicante intenta ingresar a la red, el conmutador de red tomará la decisión de dar acceso a ese usuario mediante un portal cautivo, el cual reside en el conmutador y puede ser personalizable de acuerdo a cada cliente.

Lo anterior se resume en la siguiente imagen:

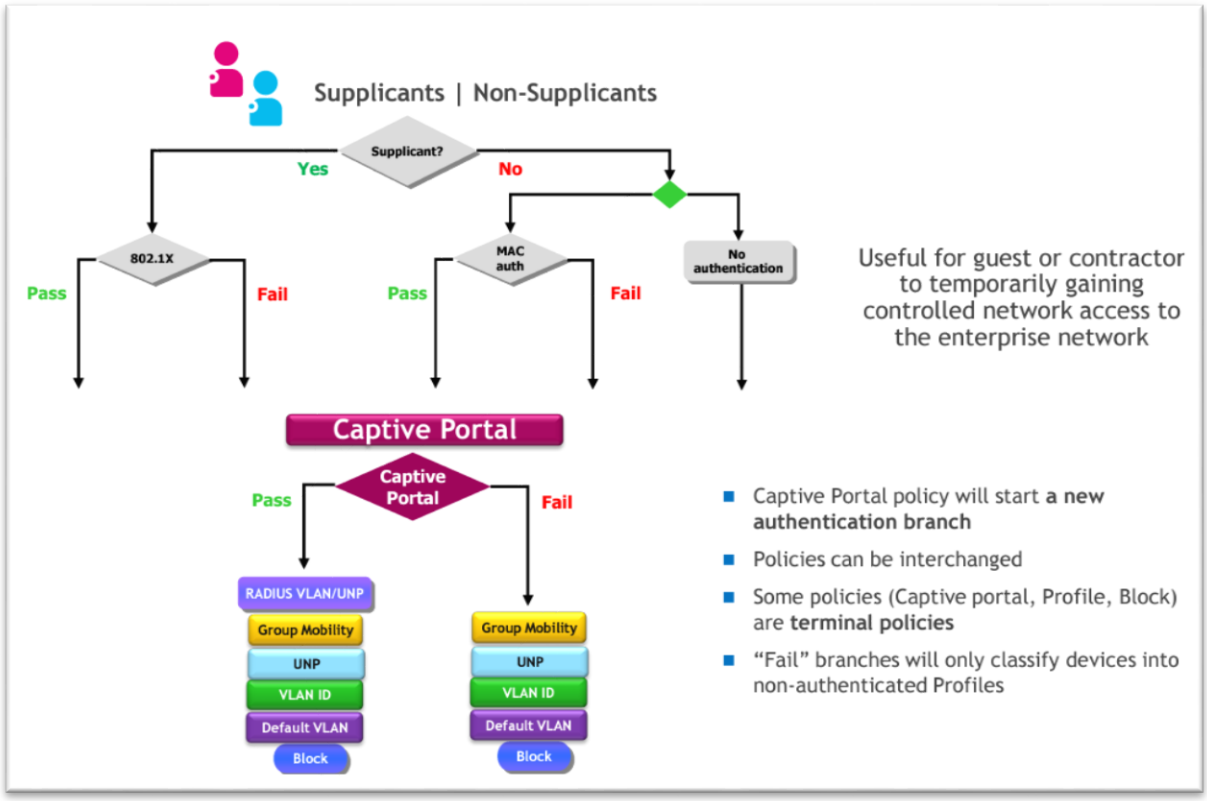


Figura 7. Autenticación Mediante Portal Cautivo

Como se muestra, en casa de falla de autenticación, el conmutador mandará al usuario a un portal cautivo para que pueda ingresar a la red por medio de unas credenciales provisionales que se asignan durante un periodo determinado de tiempo.

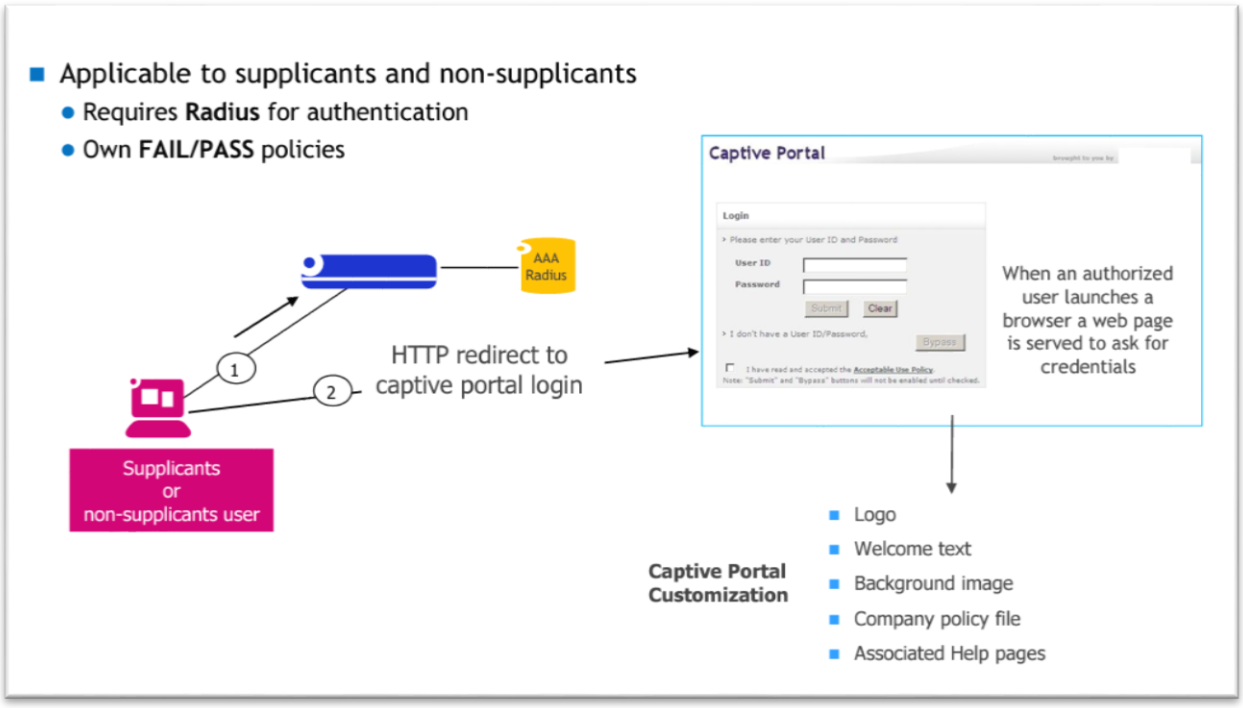


Figura 8. Portal Cautivo Dentro del Conmutador de Red

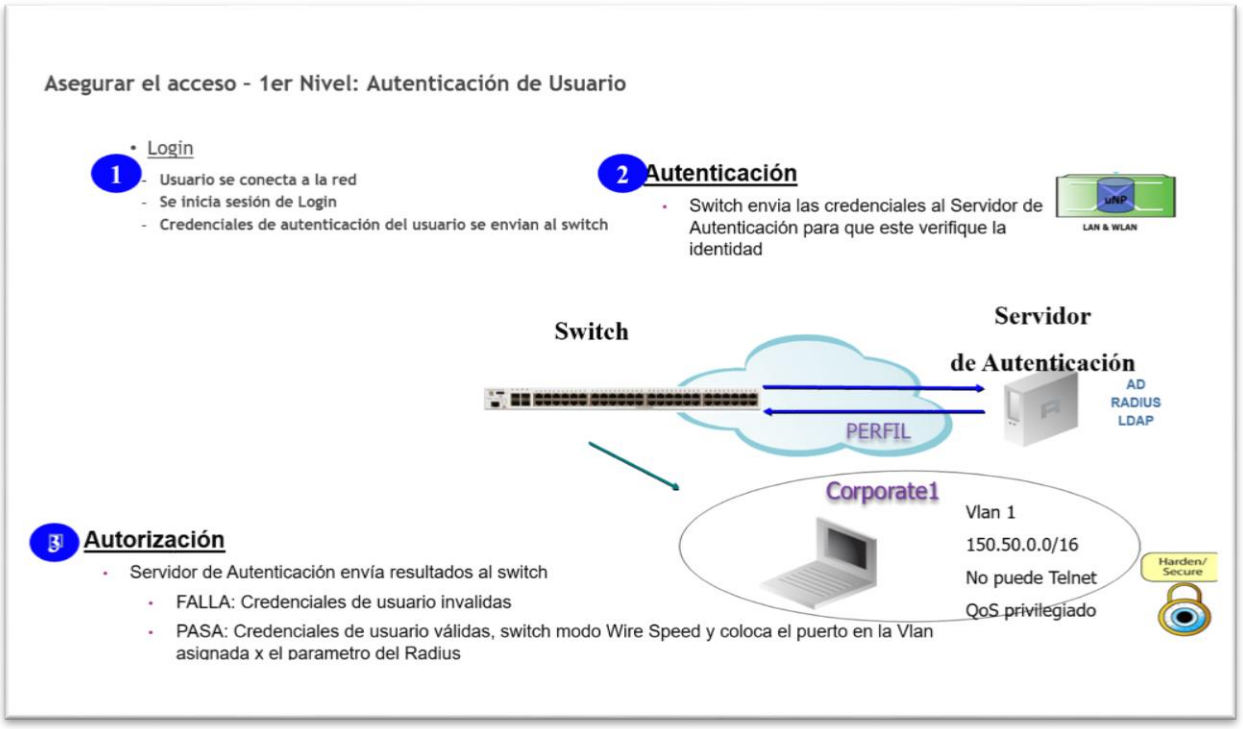


Figura 9. Esquema General de Autenticación

Otra facilidad que se le presentó al cliente fue el sistema de gestión de red. Este sistema, con ayuda de los conmutadores de red, principalmente los de acceso, ofrece muchas ventajas y facilita la administración de la red. Una de las ventajas es la visibilidad de las aplicaciones que se están ejecutando y que están consumiendo los recursos de red, así como los usuarios que están haciendo uso de dichas aplicaciones.

El sistema de gestión consta de varias herramientas, las cuales se muestran en la siguiente imagen:

Figura 10. Herramientas del Sistema de Gestión de Red

Cada una de estas herramientas cumple una función específica. Dashboard se refiere a la visualización de cada uno del resto de los componentes, tal como se muestra en la siguiente imagen:

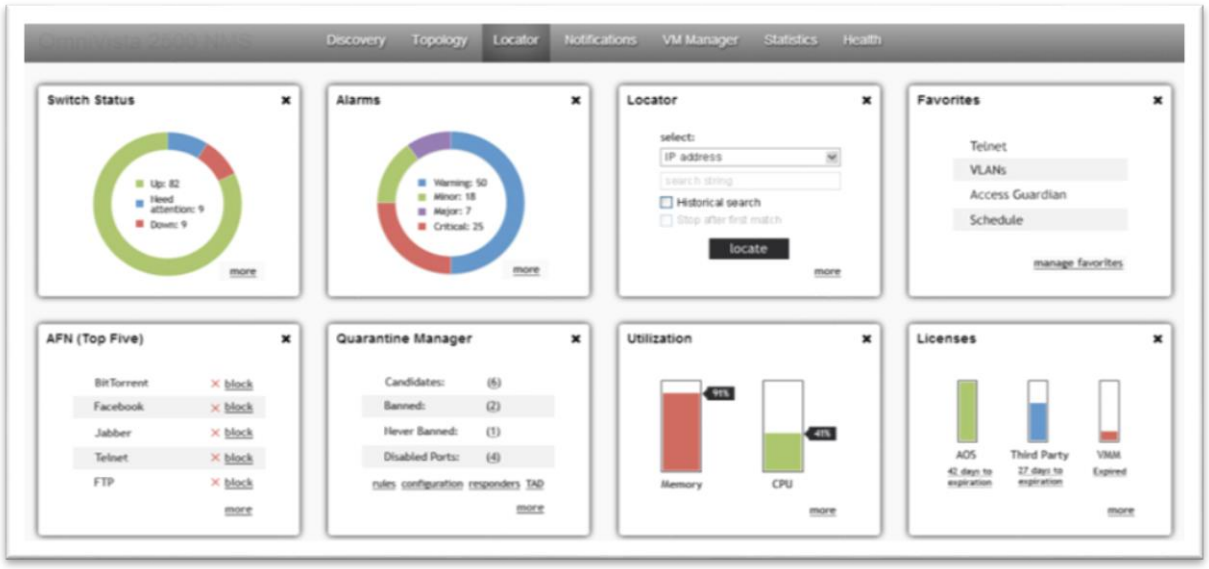


Figura 11. Visualización de Herramientas del Sistema de Gestión.

También se tiene la facilidad de observar a los usuarios que consumen mayormente los recursos de la red, como se muestra en la imagen:

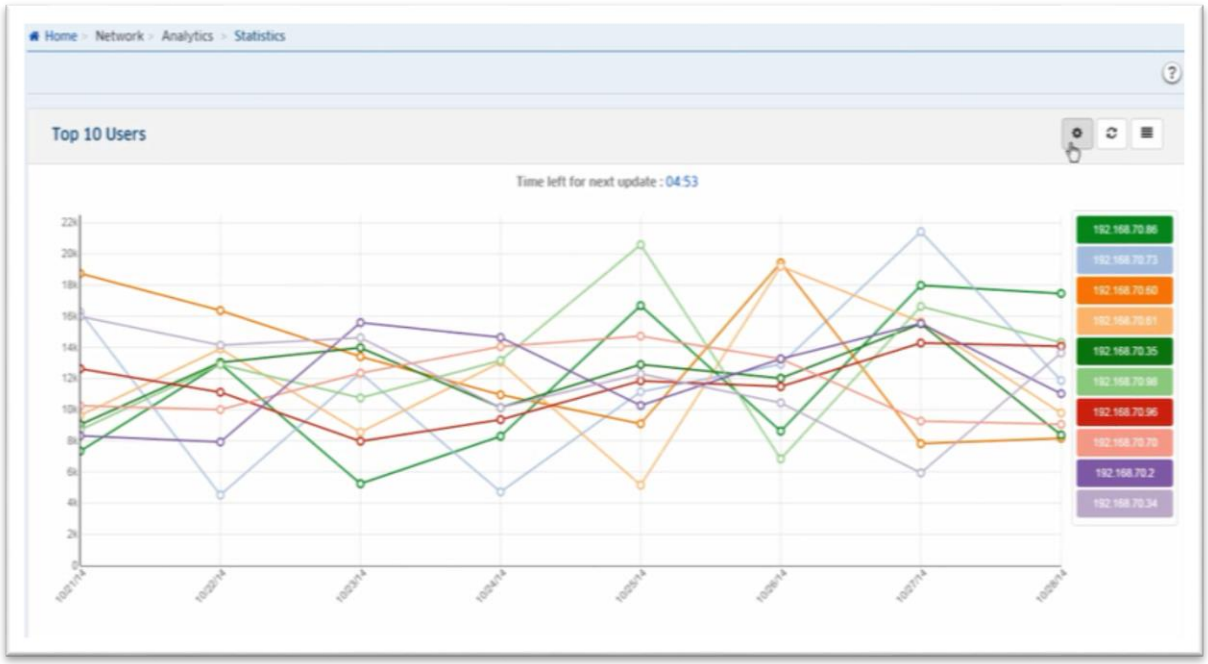


Figura 12. Visualización de los Usuarios que Demandan Más Recursos de la Red

El sistema de gestión también permite visualizar las aplicaciones que están consumiendo la mayor cantidad de recursos de la red. El administrador de red podrá tomar la decisión de qué aplicación controlar o en dado caso, bloquear.

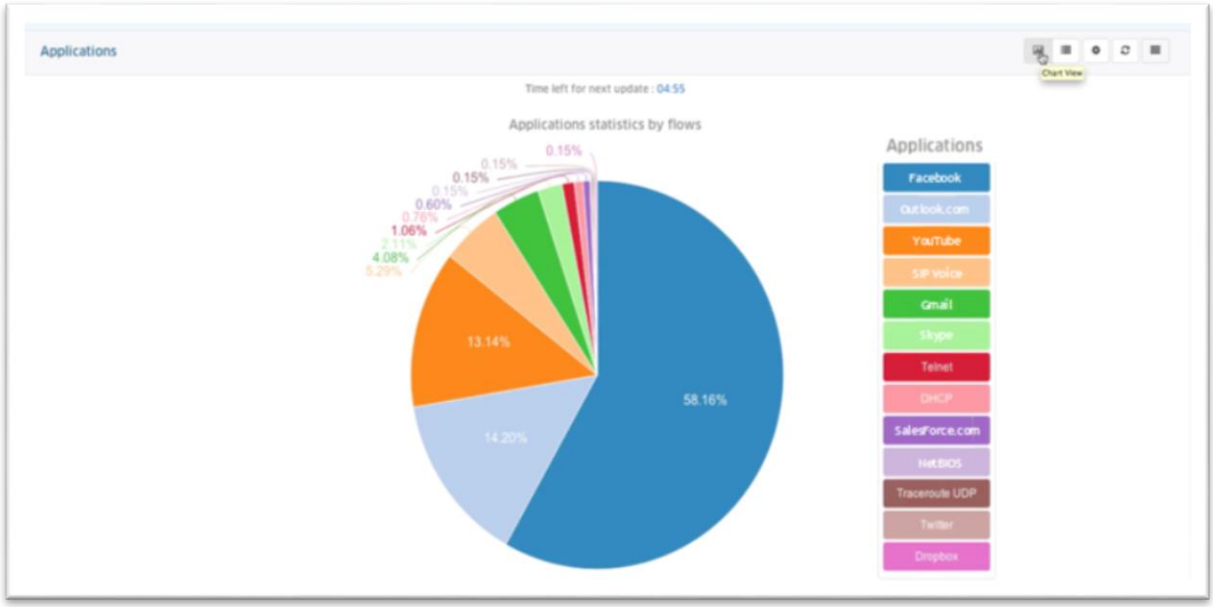


Figura 13. Visualización de Aplicaciones Ejecutándose en la Red

8. Glosario

1. **Latencia:** se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

2. **Troubleshooting:** se trata de una búsqueda sistemática y lógica para el origen de un problema con el fin de resolverlo, y hacer que el producto o el proceso operativo de nuevo.

3. **Sapnning Tree Protocol:** STP (del inglés Spanning Tree Protocol) es un protocolo de red de nivel 2 del modelo OSI (capa de enlace de datos). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

4. **Shortest Path Bridging**: Shortest Path Bridging (SPB), es un estándar especificado en la norma 802.1aq de IEEE 802.1aq. Es una tecnología de red destinada a simplificar la creación y configuración de redes de ordenadores al tiempo que permite el enrutamiento de trayectos múltiples.

   Shortest Path Bridging reemplaza el viejo protocolo Spanning tree. SPB permite tener todos los caminos activos con múltiples caminos de igual coste.

5. **Routing Information Protocol:** RIP es un protocolo de puerta de enlace interna o interior utilizado por los enrutadores de red para intercambiar información acerca de redes del Protocolo Internet a las que se encuentran conectados. Su algoritmo de enrutamiento está basado en el vector de distancia, ya que calcula la métrica o ruta más corta posible hasta el destino a partir del número de "saltos" o equipos intermedios que los paquetes IP deben atravesar. El límite máximo de saltos en RIP es de 15, de forma que al llegar a 16 se considera una ruta como inalcanzable o no deseable.

6. **File Transfer Protocol:** FTP es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

7. **Telnet:** Telnet es un protocolo de Internet estándar que permite conectar terminales y aplicaciones en Internet. El protocolo proporciona reglas básicas que permiten vincular a un cliente con un intérprete de comandos del lado del servidor. El protocolo Telnet se aplica en una conexión TCP para enviar datos en formato ASCII codificados en 8 bits, entre los cuales se encuentran secuencias de verificación Telnet.