UNIVERSIDAD CATÓLICA DE SANTA MARÍA

Facultad de Ciencias e Ingenierías Físicas y Formales

Programa Profesional de Ingeniería de Sistemas

MODELO DE IMPLEMENTACIÓN JERÁRQUICO DE LA RED DE DATOS IP DE LA UNIVERSIDAD CATÓLICA DE SANTA MARÍA UTILIZANDO LA METODOLOGÍA TOP DOWN Y EL ESTÁNDAR IEEE 802.3ae, IEEE 802.3an Y IEEE 802.3ab

Tesis presentada por el bachiller:

HUANAYQUE VILCA, CESAR

Para optar por el título de:

INGENIERO DE SISTEMAS

AREQUIPA – PERU

2013

PRESENTACIÓN

Sra. Directora del Programa Profesional de Ingeniería de Sistemas

Sres. Miembros del Jurado Examinador de Tesis

De conformidad con las disposiciones del Reglamento de Grados y Títulos del Programa Profesional de Ingeniería de Sistemas, remitimos a vuestra consideración el estudio de investigación titulado "MODELO DE IMPLEMENTACIÓN JERÁRQUICO DE LA RED DE DATOS IP DE LA UNIVERSIDAD CATÓLICA DE SANTA MARÍA UTILIZANDO LA METODOLOGÍA TOP DOWN Y EL ESTÁNDAR IEEE 802.3AE, IEEE 802.3AN Y IEEE 802.3AB", el mismo que de ser aprobado me permitirá optar por el título profesional de Ingeniero de Sistemas.

Arequipa, abril del 2013

_____

Cesar Huanayque Vilca

A mis padres.

AGRADECIMIENTOS

Agradezco a mis padres Cornelia y Agustín por siempre estar a mi lado y por siempre haberme brindado su apoyo incondicional.

Agradezco a la Ing. Karina Rosas por su valiosa orientación para la realización del presente proyecto.

Agradezco al Ing. Fredy Delgado por la confianza brindada y su valiosa orientación para la realización, elaboración e implementación del presente proyecto.

"En el reino de las ideas todo depende del entusiasmo, En el mundo real todo depende de la perseverancia"

Goethe

"Si primero pudiéramos saber en qué lugar estamos y hacia qué lugar estamos yendo, entonces podríamos juzgar que hacer y cómo hacerlo"

Abraham Lincoln

"El mundo que hemos hecho es el resultado del nivel de pensamiento, hemos creado problemas los cuales no podemos resolver al mismo nivel del que lo creamos"

Albert Einstein

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente trabajo de investigación se basa en la determinación de las mejores prácticas y recomendaciones para la modelación e implementación de una red de campus y enterprise en redes medianas o grandes teniendo como objetivo proporcionar el mejor modelo de red de acuerdo al core Bussiness y las necesidades de la organización en la que se aplique.

La necesidad de un modelo de implementación viene de los problemas que ocurren en una red IP diseñada sin tomar en cuenta requerimientos de negocio y técnicos y que luego de su implementación pueden tener problemas en escalabilidad, calidad de servicio, flexibilidad y seguridad.

Se establece la identificación de todos los requerimientos por parte de las actuales y futuras aplicaciones de la red, comunidades de usuario, identificación de data-stores, para luego tener una solución que se adapte a las necesidades actuales y futuras el cual se ve reflejada en el diseño jerárquico con zonas bien marcadas como red LAN de campus, granja de servidores, DMZ, accesos remotos y WAN.

Finalmente se comprobó las mejoras asociadas al uso del modelo teniendo como fundamento ancho de banda, velocidad de transmisión y la escalabilidad de la red, calidad de servicio según la aplicación, flexibilidad del diseño y seguridad.

ABSTRACT

The present research paper is based on the determination of the best practices and recommendations for the exemplified and implementation of a campus and enterprise network in a business network y medium and large networks having as an objective provide the best possible network model in accordance of core business and the needs of the organization where it is applied.

The need for an implementation model comes from the problems that occur in an IP network designed without taking into account business and technical requirements and after its implementation may have problems in scalability, quality of service, flexibility and security.

It establishes the identification of all the requirements from current and future network applications, user communities, identifying data-stores, and then have a solution that meets current and future needs which is reflected in hierarchical design with well-marked areas of campus LAN, server farm, DMZ, remote access and WAN.

Finally found improvements associated with the use of the model and are based upon bandwidth, transmission speed and network scalability, quality of service according to application, flexibility in the design and a secure network.

INTRODUCCION

Hoy en día las nuevas prácticas en las empresas y organizaciones están impulsando cambios en las redes empresariales. La mayoría de los servicios de las empresas y organizaciones se dan a través de las redes de datos Ethernet lo que conllevan a una red emergente donde servicios de data, video, voz conviven bajo una misma arquitectura.

Las redes convergentes conllevan a un mundo donde se tiene que tener claro el diseño de la red, teniendo en cuenta las tecnologías, protocolos y herramientas a utilizar para el buen funcionamiento de estas. Siendo indispensable contar con una red jerárquica la cual sea escalable, flexible y que aplique calidad de servicio y seguridad. Todos estos puntos motivaron el presente proyecto de investigación y es que resulta interesante el efecto que puede ocasionar no tener una red no jerárquica y las implicaciones que esta pueda tener con el crecimiento de la organización a nivel tecnológico.

El presente trabajo de investigación ha sido dividido en cinco capítulos:

El capítulo 1 contiene el planteamiento teórico que sustenta la utilización de un modelo. En él se encuentran el objetivo general, los objetivos específicos, el alcance y las limitaciones y la hipótesis con los indicadores para su validación.

El capítulo 2 presenta conceptos generales de redes convergentes incluyendo el modelo OSI que es el punto de referencia hacia el diseño de una red jerárquica, además de los estándares a utilizar de las ramas de 10Gigabit Ethernet.

El capítulo 3 contiene el modelo propuesto, plasmando su estructura y los pasos a realizar en cada una de sus 4 etapas.

El capítulo 4 presenta la implementación del modelo en la UCSM siguiendo los pasos del modelo presentado en el capítulo 3.

El capítulo 5 presenta la validación del modelo de acuerdo a los indicadores que dieron como resultado la implementación del modelo en la UCSM.

Capítulo 1

Planteamiento Teórico

1.1. Titulo descriptivo del proyecto de investigación

"Modelo de implementación jerárquico de la red de datos IP de la Universidad Católica de Santa María utilizando la metodología Top Down y el estándar IEEE 802.3ae, IEEE 802.3an y IEEE 802.3ab"

1.1.1. Descripción del problema

Actualmente las redes de datos tienen una carga mayor de tráfico debido al desarrollo de las tecnologías en lo que es aplicaciones, base de datos, sistemas integrados como ERP, voz y video, herramientas de data mining y su vez los mecanismos de seguridad que se utilizan como algoritmos de encriptación para proteger los datos que viajan a través de las redes de datos IP.

La norma 10Gbps (IEEE 802.3ae, IEEE 802.3an) no sólo dá a esta tecnología de una capacidad diez veces superior a 1Gbps (IEEE 802.3ab), sino que también le abre las puertas a otras áreas de aplicación diferentes de las LAN, como las MAN y las WAN, al cubrir distancias de hasta 40 kilómetros. Con Ethernet a 10 Gbps es posible transferir los contenidos de un disco duro de 10 Gigabytes en 8 segundos o hacer backup de un sistema de almacenamiento corporativo de 2 Terabytes en 27 minutos, y, aunque en principio su aplicación está más orientada a datos, podría transportar de una sola vez 833 señales de vídeo digital o 156.250 llamadas telefónicas.

Frente a otras alternativas de alta velocidad, la gran ventaja del estándar 10 Gigabit Ethernet, se basa en su gran compatibilidad con la base instalada de interfaces 802.3 y con los principios de gestión y operación de

red propios de Ethernet, así como en la preservación de las inversiones ya realizadas en investigación y desarrollo respecto de esta tecnología. Y todo ello tanto para entornos LAN como MAN y WAN. La tecnología 10 GE representa un salto sustancial en velocidad con las ventajas que proporciona la madurez, facilidad de gestión del entorno Ethernet, posibilidades de QoS integradas y coste asociado respecto de otras tecnologías como ATM.

La tecnología 10 GE está principalmente dirigida a cubrir las demandas de conectividad en entornos LAN: 10/100/1000 Mbps en el puesto del usuario, 10 Gbps en los servicios y 10 Gbps en conexión entre edificios en entornos de campus.

1.1.2. Justificación del estudio

La infraestructura de la red de datos de la Universidad Católica de Santa María actualmente a nivel de Core y Backbone utiliza la tecnología Gigabit Ethernet y en lo que concierne en el nivel de Distribución y Acceso utiliza Fast Ethernet y en algunos casos Ethernet (10Mbps) en una cuarta capa. El actual diseño de red el cual está compuesto por el diseño físico y lógico que se implantó en Octubre del 2002, el cual fue creciendo de manera no planificada y solo en función de las necesidades que se requirieron con el pasar de los años por lo tanto el diseño actual no cubre las requerimientos que se vienen presentando actualmente.

El modelo propuesto pretende reducir el efecto de algunas de las barreras citadas anteriormente en la implementación de red, teniendo como fin trazar un marco de referencia para la implementación de diseño jerárquico utilizando tecnologías 1Gbps y 10Gbps además de ser escalable a 40Gbps considerando diversas situaciones y recursos disponibles. Este modelo proporciona el conocimiento requerido para aplicar la metodología de diseño jerárquico Top Down permitiendo al

administrador de red evaluar y analizar la aplicación de las herramientas propuestas.

1.2. Objetivos

1.2.1. General

Diseñar e implementar un modelo de implantación jerárquico para la red de datos IP de la UCSM utilizando la metodología Top Down y el estándar IEEE 802.3ae, IEEE 802.3an y IEEE 802.3ab.

1.2.2. Específicos

- Diseñar un modelo que se adapte al Core Bussiness de la institución y que sea flexible a los cambios, decisiones y recursos.
- Diseñar un modelo que se adapte a los estándares planteados y que sea escalable con las tecnologías emergentes.
- Proponer un modelo que integre seguridad, calidad de servicio, convergencia, performance y accesibilidad.
- Analizar las arquitecturas de equipos de comunicaciones existentes que soporten los estándares de la norma IEEE 802.3ae, IEEE 802.3an, IEEE 802.3ab.

1.3. Limitaciones y alcances

1.3.1. Limitaciones

- En el planteamiento del modelo jerárquico no se tomara en cuenta el desarrollo e implementación de redes inalámbricas.
- En el planteamiento del modelo jerárquico no se tomara en cuenta las redes SAN.

- En la implementación del modelo solo se tomara en cuenta las capas de Core y Distribución dejándose la capa de Acceso. para una futura implementación.
- En el planteamiento del modelo se mencionara la red Enterprise como WAN y acceso remoto, pero en la en la implementación no se tomaran en cuenta.
- Limitaciones en cuanto a las características físicas de los equipos que soporten 10G.

1.3.2. Alcances

- Proyecto de renovación tecnológica en redes de datos IP a implementarse en la Universidad.
- Acceso sin restricciones a la red de datos IP física y lógica.
- Implementación general de la red de datos IP a realizarse en el último trimestre del año 2012.
- Implementación de un modelo optimizado a los requerimientos de la Universidad tomando como referencia la red de datos IP existente.

1.4. Hipótesis

Dado que los estándares IEEE 802.3ae, IEEE802.3an, IEEE 802.3ab establecen los procedimientos para el uso eficiente de anchos de banda superiores al IEEE 802.3u (Fast Ethernet), es probable que con la implementación de un modelo jerárquico Top Down y de los estándares IEEE 802.3an, IEEE 802.3ae, IEEE 802.3ab se pueda mejorar la calidad de servicio, velocidad y seguridad de la transmisión en la UCSM.

1.4.1. Variables

1.4.1.1. Independientes

- Red de datos IP alineado a los estándares IEEE 802.3ae, IEEE802.3an, IEEE 802.3ab.

1.4.1.2. Dependientes

- Modelo de implementación Jerárquico en la red de datos IP.

1.4.2. Indicadores

1.4.2.1. De la variable independiente

Calidad y continuidad de la transmisión y comunicación de datos determinada por:

- Throughput
- Latencia
- Priorización
- Convergencia

1.4.2.2. De la variable dependiente

- Escalabilidad
- Flexibilidad
- Calidad de Servicio
- Seguridad

1.5. Área científica

- **Área:** Redes y Telemática.
- **Línea:** Arquitectura de redes de datos.

1.6. Tipo y nivel de investigación

- **Tipo:** Aplicada
- **Nivel:** Experimental

1.7. Antecedentes de investigación

1.7.1. Optimización e implementación de la red LAN del Instituto de electricidad y electrónica UACH - Chile

1.7.1.1. Objetivo

Mejorar y optimizar los recursos existentes y también ser una herramienta para la docencia, investigación e incrementar el nivel educativo en el aprendizaje de los estudiantes de la carrera de Ing. Electrónica de la Universidad Austral de Chile.

1.7.1.2. Conclusiones

- Con el desarrollo de este trabajo ha quedado de manifiesto que Ethernet es una tecnología de gran flexibilidad, también ha evolucionado rápidamente de una tecnología local a una de área metropolitana, incluso extensa y que hoy domina el mundo ofreciendo conectividad alámbrica con un gran ancho de banda.

- El uso de modelos de referencia divididos en capas facilita el entendimiento de la comunicación entre dos computadores en una red y proporcionar de una gran ayuda a la detección y solución de problemas.

- La implementación de redes conmutadas permite un mayor aprovechamiento del ancho de banda disponible en una red, permitiendo crear pequeños dominios los que disminuyen el tráfico de broadcast.

- Clasificar el diseño de na red en niveles jerárquicos, como la propuesta en este trabajo de tesis, permite seleccionar el hardware apropiado para cada nivel que se traduce en eficiencia y por consiguiente un aumento del rendimiento de la red, por lo tanto disminuyen los cotos y tiempo de implementación.

- La propuesta de mejoramiento de la red del Instituto de Electricidad y Electrónica, presentada en el capítulo 3 del presente trabajo, recomienda en primera instancia reemplazar los dispositivos concentradores de capa 1 (Hubs) existentes por dispositivos de capa 2 (Switches), transformándose de esta manera la red en una red conmutada, con lo que se obtendrá un mayor aprovechamiento del ancho de banda disponible. Para tener funcionalidades de calidad de servicio (QoS), administración remota, seguridad y/o creación de redes virtuales, la elección del hardware debe poseer la misma tecnología existente en la Red UACh.

1.7.2. Red LAN para el centro local Amazonas Universidad Nacional Abierta – Venezuela

1.7.2.1. Objetivo

Desarrollar una red de área local LAN que facilite la comunicación en el centro local Amazonas de la Universidad Nacional Abierta.

1.7.2.2. Conclusiones

- Las redes al igual que las aplicaciones, deben moverse junto a las exigencias de los clientes, por lo cual, ambos deben ir al mismo ritmo de estos últimos. Instituciones educativas, como es el caso de centro local Una-Amazonas donde se toman decisiones importantes y en donde una compleja LAN los envuelve, deben soportar tráfico que por ella pasa y el flujo de la información debe ser tan rápido como las exigencias de los usuarios.

- El uso del cableado estructurado, plataforma de equipos switcheados y demás componentes que una red involucra, trae consigo a que se esté bien preparado para atender los requerimientos y la LAN soporte tráfico brusco en ciertas ocasiones.

- El desarrollo de la infraestructura de cableado representa el punto de partida para que, en un futuro no muy lejano, pueda seguirse con la instalación de equipos más poderosos que puedan soportar velocidades de hasta 1Gbps.

- Gracias al empleo de una efectiva metodología de investigación, se logró alcanzar el mejor desarrollo para realizar el análisis, diseño y se lograra la implementación del sistema de cableado y el reemplazo de concentradores existentes por switches. El análisis hizo posible diagnosticar y proponer una solución factible para satisfacer la problemática que existía en la institución el diseño permitió elaborar el sistema propuesto de acuerdo a los requerimientos de los usuarios involucrados; y la implementación se convertirá en la solución de todas las debilidades encontradas en el sistema actual y preparación para una posible emigración de toda la plataforma de switches de nueva generación y mayor capacidad

1.7.3. Estructuración lógica de una LAN correspondiente a los laboratorios de Informática de la UNSIJ – Universidad de la Sierra Juárez, México

1.7.3.1. Objetivo

Estructurar lógicamente la red de los laboratorios de informática y salas de cómputo mediante el uso de dispositivos de networking para optimizar el ancho de banda y mejorar la transferencia de paquetes de datos.

1.7.3.2. Conclusiones

- Mediante el desarrollo de este proyecto se pudo mostrar la segmentación lógica de una red como la principal solución para controlar el tráfico y así optimizar el ancho de banda. El uso de VLANs mejora su desempeño ya que permite dividirla en dominios de broadcast más pequeños, disminuyendo la saturación del canal de transmisión. La implementación de VLANs permite también que la red seguridad y flexibilidad dejando abierta la posibilidad de movimientos y cambios futuros.

- Otras técnicas utilizadas son las ACL, con las que además de indicar quienes acceden a la red también disminuye trafico al no permitir el acceso a ciertas aplicaciones o trafico proveniente de fuentes desconocidas.

- El uso de protocolos de enrutamiento generó una red con mayor escalabilidad, ya que permiten integrar con mayor facilidad nuevas redes, en este caso solo se utilizó el protocolo de enrutamiento RIP debido a que el tamaño de la red y los equipos con que se contaba. Sin embargo está planeado por la jefatura de la carrera informática adquirir más dispositivos de red para tener mejor equipos el laboratorio de redes y así, los

futuros tesistas y alumnos tengan la posibilidad de experimentar en una más óptima.

- El monitoreo del trafico también fue muy importante observando así el comportamiento de la red al elevar el tráfico generado por aplicaciones ejecutadas en los equipos de cómputo. Además de identificar las IPs que generaban mayor tráfico y como consecuencia la VLAN también se pudieron observar puertos, protocolos e IPs utilizados en el envío de paquetes los hosts de origen y destino. Toda esta información y mucha más se observó con el servidor dejando en claro que es indispensable la implementación de este tipo de herramientas de red.

1.7.4. Diseño e implementación de una red LAN y WLAN con sistema de control de acceso mediante servidores AAA – PUCP Perú.

1.7.4.1. Objetivo

Diseñar e implementar una red LAN y WLAN que sea capaz de evitar la suplantación de identidad; así como reducir la brecha entre una red cableada convencional y una red inalámbrica.

1.7.4.2. Conclusiones

- Se comprobó que los protocolos AAA RADIUS y TACACS+ tienen diferentes características en el manejo de autenticación y autorización. El protocolo RADIUS maneja ambos servicios de manera combinada, mientras que el protocolo TACACS+ los ofrece como servicios independientes. A pesar de ello fueron implementados en una misma red y coexisten para brindar una red con sistema de control de acceso robusto.

- Se demostró que con ayuda de adecuados protocolos y técnicas de red se puede optimizar el uso de recursos de la misma y hacer que esta sea más robusta frente a averías que pueda sufrir. En esta tesis usamos la técnica Etherchannel para implementar redundancia de enlace, demostrándose que el tiempo de respuesta ante una caída de enlace será menor a 1 ms. Asimismo se utilizó la técnica Etherchannel para balancear la carga entre los enlaces resultando en la ampliación del ancho de banda. También se usó el protocolo GLBP para implementar redundancia de equipos y balanceo de carga entre ellos.

- Al culminar con la implementación del presente proyecto se pudo concluir que, gracias al servidor RADIUS, un usuario inalámbrico puede autenticarse e ingresar a la red; asimismo, el servidor TACACS+, teniendo como base el nivel de privilegio del usuario, permite a este ingresar o no a los equipos de red para realizar configuraciones en los equipos.

- Se diseñó una solución teniendo en cuenta las características más valoradas por los usuarios finales: continuidad de servicio, rapidez en el intercambio de datos y seguridad de la información.

1.7.5. Estudio, análisis, diseño e implementación de una infraestructura de red común en un edificio de propósito general

1.7.5.1. Objetivo

El objetivo principal de este proyecto es que sirva como documento de análisis, donde se realize un exhaustivo estudio de las necesidades en cuanto a comunicaciones surgidas en una organización común, definido como un edificio de 3 plantas, y el resultado sea tratado como posible alternativa de solución y correcta implantación de la solución obtenida.

1.7.5.2. Conclusiones

- Diseñar una red es un gran desafío, el proceso no solo consiste en conectar computadoras. Una red precisa de muchas características que la hagan fiable, manejable y escalable. Para lograr estos objetivos, se deben conseguir que los componentes principales de una red tengan requerimientos de diseño diferentes. Si una red no está correctamente diseñada, aparecerán muchos problemas imprevistos que pueden poner en peligro su crecimiento.

- Para que una red sea eficaz y sirva a las necesidades de sus usuarios, debe estar diseñada e implementada de acuerdo a una serie de pasos sistemáticos planificados, entre los que se incluyen los siguientes: Estudio de viabilidad del sistema, Análisis de la solución propuesta, Diseño de la red, Implementación.

- Tras el estudio realizado, podemos garantizar que la solución adoptada ha sido la mejor entre las muchas posibilidades que nos brindan las redes de hoy en dias. Es decir, utilizando los conocimientos de Ingeniería de las tecnologías de la información y comunicación (TIC) hemos desarrollado la solución óptima, adecuada a los requerimientos relacionados, tratando de aprovechar de la mejor manera los recursos disponibles teniendo en cuenta la funcionalidad, escalabilidad, adaptabilidad y manejabilidad.

Capítulo 2

Marco Teórico

2.1. Modelo

Es un sistema de elementos que reproduce determinados aspectos, relaciones y funciones del objeto que se investiga; desarrollado en un nivel avanzado del conocimiento, en el que recopila las características generales del objeto investigado y las unifica en un concepto global, del cual se puede visualizar el objeto en un momento dado [1].

Un modelo es un arquetipo o punto de referencia para imitarlo o reproducirlo, otros usos de la palabra refieren a la representación en pequeño de alguna cosa; al esquema teórico de un sistema o de una realidad compleja. Los modelos enfocan ciertas partes importantes de un sistema (por lo menos, aquella que le interesan a un tipo de modelo específico), restándole importancia a otras [2].

Un modelo es por tanto una representación parcial o simplificada de la realidad que recoge aquellos aspectos de relevancia para las intenciones del modelador, y de la que se pretende extraer conclusiones de tipo predictivo. Se modela para comprender mejor o explicar mejor un proceso o unas observaciones [3].

2.2. Modelo OSI

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO) en el año 1984. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

Fue desarrollado en 1984 por la Organización Internacional de Estándares (ISO), una federación global de organizaciones que representa

aproximadamente a 130 países. El núcleo de este estándar es el modelo de referencia OSI, una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes.

Se trata de una normativa estandarizada útil debido a la existencia de muchas tecnologías, fabricantes y compañías dentro del mundo de las comunicaciones, y al estar en continua expansión, se tuvo que crear un método para que todos pudieran entenderse de algún modo, incluso cuando las tecnologías no coincidieran. De este modo, no importa la localización geográfica o el lenguaje utilizado. Todo el mundo debe atenerse a unas normas mínimas para poder comunicarse entre sí. Esto es sobre todo importante cuando hablamos de la red de redes, es decir, Internet.

Este modelo está dividido en siete capas:

Figura 2.2-1: Modelo OSI
Fuente: [CCN2007]

2.2.1. Capa 1

Es la que se encarga de las conexiones globales de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información [4].

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.

2.2.2. Capa 2

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo. Es uno de los aspectos más importantes a revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras así determinando el paso de tramas, verificando su integridad, y corrigiendo errores, por lo cual es importante mantener una excelente adecuación al medio físico, con el medio de red que redirecciona las conexiones mediante un router. Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el Switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios, dada esta situación se determina como el medio

que se encarga de la corrección de errores, manejo de tramas, protocolización de datos [4].

2.2.3. Capa 3

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)
- Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea son los routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final [4].

2.2.4. Capa 4

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión. Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP:Puerto.

2.2.5. Capa 5

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles [4].

2.2.6. Capa 6

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor [4].

2.2.7. Capa 7

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP), por UDP pueden viajar (DNS y Routing Information Protocol). Hay tantos

protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente [4].

2.3. Modelo de redes jerárquicas

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo [CCN2007].

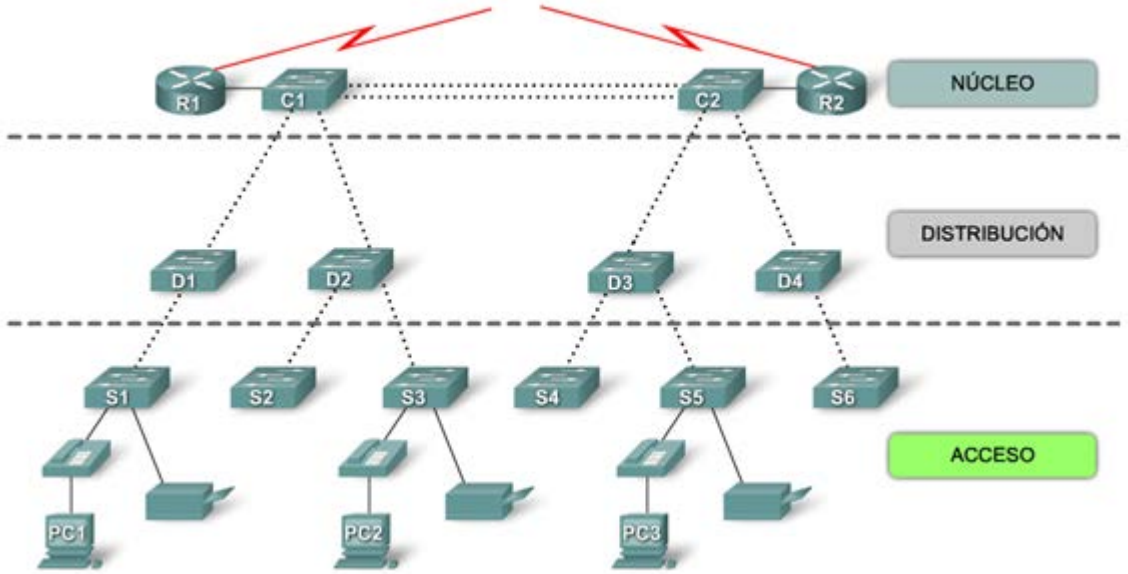

Figura 2.3-1: Redes Jerárquicas
Fuente: [CCN2007]

2.3.1. Capas del modelo jerárquico

2.3.1.1. Core

La capa núcleo del diseño jerárquico es la backbone de alta velocidad de la Internetwork. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente [CCN2007].

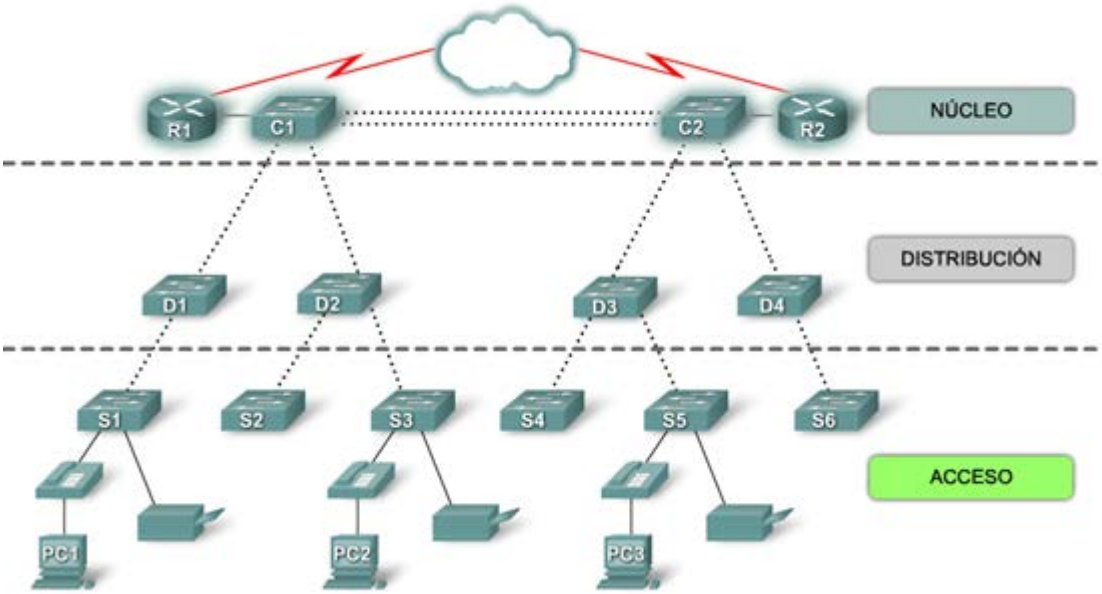

Figura 2.3-2: Capa de Core
Fuente: [CCN2007]

2.3.1.2. Distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario dividir en segmentos el tráfico sobre un switch en subredes separadas. Por ejemplo, en una universidad el usuario podría separar el tráfico según se trate de profesores, estudiantes y huéspedes. Normalmente, los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad [CCN2007].

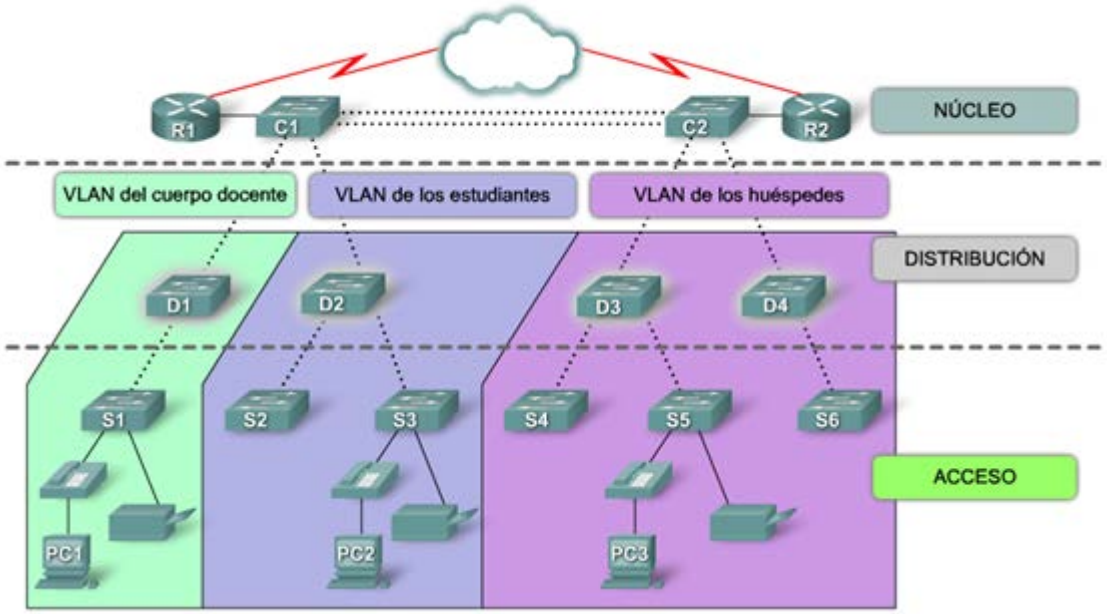

Figura 2.3-3: Capa de Distribución
Fuente: [CCN2007]

2.3.1.3. Acceso

La capa de acceso interactúa con dispositivos finales, como PC, impresoras y teléfonos IP, para proporcionar acceso al resto de la red. La capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos (AP). El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red [CCN2007].

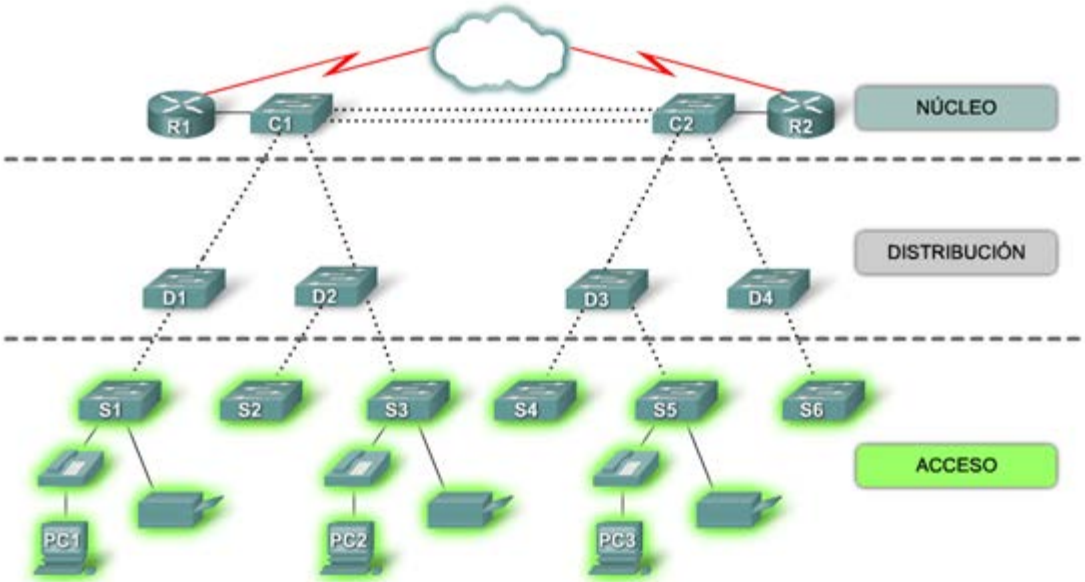

Figura 2.3-4: Capa de Acceso
Fuente: [CCN2007]

2.3.2. Beneficios

2.3.2.1. Escalabilidad

Las redes jerárquicas escalan muy bien. La modularidad del diseño le permite reproducir exactamente los elementos del mismo a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión. Por ejemplo, si el modelo del diseño consiste en dos switches de la capa de distribución por cada 10 switches de la capa de acceso, puede continuar agregando switches de la capa de acceso hasta tener 10 switches de la capa de acceso interconectados con los dos switches de la capa de distribución antes de que necesite agregar switches adicionales de la capa de distribución a la topología de la red. Además, a medida que se agregan más switches de la capa de distribución para adaptar la carga de los switches de la capa de

acceso, se pueden agregar switches adicionales de la capa núcleo para manejar la carga adicional en el núcleo.

2.3.2.2. Redundancia

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas. Los switches de la capa de acceso se conectan con dos switches diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los switches de la capa de distribución, el switch de la capa de acceso puede conmutar al otro switch de la capa de distribución. Adicionalmente, los switches de la capa de distribución se conectan con dos o más switches de la capa núcleo para asegurar la disponibilidad de la ruta si falla un switch del núcleo. La única capa en donde se limita la redundancia es la capa de acceso. Habitualmente, los dispositivos de nodo final, como PC, impresoras y teléfonos IP, no tienen la capacidad de conectarse con switches múltiples de la capa de acceso para redundancia. Si falla un switch de la capa de acceso, sólo se verían afectados por la interrupción los dispositivos conectados a ese switch en particular. El resto de la red continuaría funcionando sin alteraciones [CCN2007].

2.3.2.3. Rendimiento

El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de switches intermediarios de bajo rendimiento. Los datos se envían a través de enlaces del puerto del switch agregado desde la capa de acceso a la capa de distribución casi a la velocidad de cable en la mayoría de los casos. Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para

reenviar el tráfico hasta el núcleo, donde se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, hay menos contención para el ancho de banda de la red. Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos [CCN2007].

2.3.2.4. Seguridad

La seguridad mejora y es más fácil de administrar. Es posible configurar los switches de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y hacia dónde se les permite dirigirse. Por ejemplo, si desea limitar el uso de HTTP a una comunidad de usuarios específica conectada a la capa de acceso, podría aplicar una política que bloquee el tráfico de HTTP en la capa de distribución. La restricción del tráfico en base a protocolos de capas más elevadas, como IP y HTTP, requiere que sus switches puedan procesar las políticas en esa capa. Algunos switches de la capa de acceso admiten la funcionalidad de la Capa 3, pero en general es responsabilidad de los switches de la capa de distribución procesar los datos de la Capa 3 porque pueden procesarlos con mucha más eficacia [CCN2007].

2.3.2.5. Facilidad de administración

La facilidad de administración es relativamente simple en una red jerárquica. Cada capa del diseño jerárquico cumple funciones

específicas que son consistentes en toda esa capa. Por consiguiente, si necesita cambiar la funcionalidad de un switch de la capa de acceso, podría repetir ese cambio en todos los switches de la capa porque presumiblemente cumplen las mismas funciones. La implementación de switches nuevos también se simplifica porque se pueden copiar las configuraciones del switch entre los dispositivos con muy pocas modificaciones. La consistencia entre los switches en cada capa permite una recuperación rápida y la simplificación de la resolución de problemas. En algunas situaciones especiales, podrían observarse inconsistencias de configuración entre los dispositivos, por eso debe asegurarse de que las configuraciones se encuentren bien documentadas, de manera que pueda compararlas antes de la implementación [CCN2007].

2.3.2.6. Facilidad de mantenimiento

Debido a que las redes jerárquicas son modulares en naturaleza y escalan con mucha facilidad, son fáciles de mantener. Con otros diseños de topología de la red, la administración se torna altamente complicada a medida que la red crece. También, en algunos modelos de diseños de red, existe un límite en cuanto a la extensión del crecimiento de la red antes de que se torne demasiado complicada y costosa de mantener. En el modelo del diseño jerárquico se definen las funciones de los switches en cada capa haciendo que la selección del switch correcto resulte más fácil. La adición de switches a una capa no necesariamente significa que se evitará un cuello de botella u otra limitación en otra capa. Para que una topología de red de malla complete alcance el rendimiento máximo, es necesario que todos los switches sean de alto rendimiento porque es fundamental que cada switch pueda cumplir todas las funciones en la red. En el modelo jerárquico, las funciones de los switches son diferentes en

cada capa. Se puede ahorrar dinero con el uso de switches de la capa de acceso menos costosos en la capa inferior y gastar más en los switches de la capa de distribución y la capa núcleo para lograr un rendimiento alto en la red [CCN2007].

2.3.3. Principios

Sólo porque aparentemente una red presenta un diseño jerárquico, no significa que la red esté bien diseñada.

2.3.3.1. Diámetro

Al diseñar una topología de red jerárquica, lo primero que debe considerarse es el diámetro de la red. Con frecuencia, el diámetro es una medida de distancia pero en este caso se utiliza el término para medir el número de dispositivos. El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro de la red asegura una latencia baja y predecible entre los dispositivos [CCN2007].

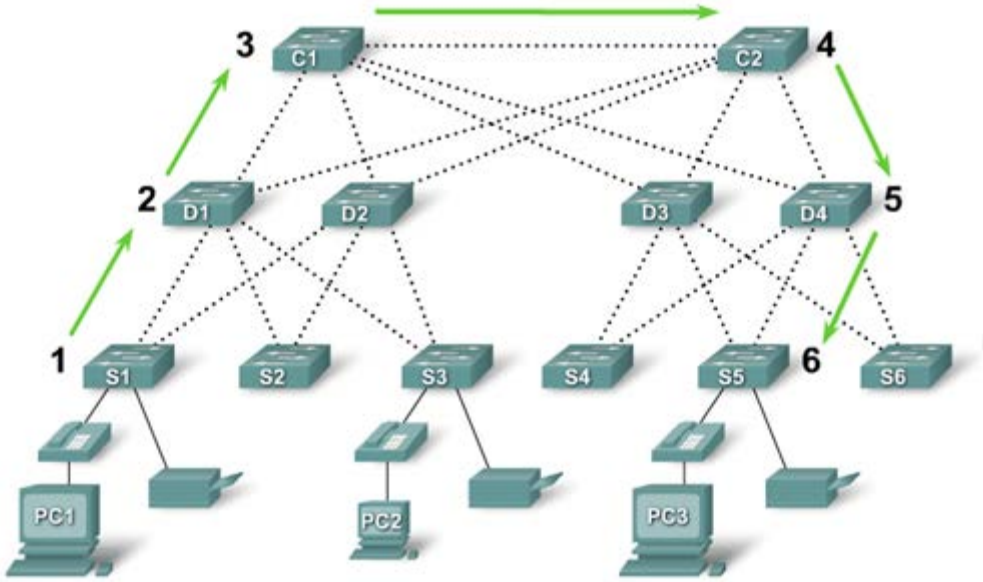

Figura 2.3-5: Diámetro de la red
Fuente: [CCN2007]

En la figura 2.3-5, la PC1 se comunica con la PC3. Es posible que existan hasta seis switches interconectados entre la PC1 y la PC3. En este caso, el diámetro de la red es 6. Cada switch en la ruta introduce cierto grado de latencia. La latencia del dispositivo de red es el tiempo que transcurre mientras un dispositivo procesa un paquete o una trama. Cada switch debe determinar la dirección MAC de destino de la trama, verificar la tabla de la dirección MAC y enviar la trama al puerto apropiado. Aunque el proceso completo se produce en una fracción de segundo, el tiempo se incrementa cuando la trama debe cruzar varios switches.

En el modelo jerárquico de tres capas, la segmentación de la Capa 2 en la capa de distribución prácticamente elimina el diámetro de la red como consecuencia. En una red jerárquica, el diámetro de la red siempre va a ser un número predecible de saltos entre el dispositivo origen y el dispositivo destino [CCN2007].

2.3.3.2. Agregado de ancho de banda

Cada capa en el modelo de redes jerárquicas es una candidata posible para el agregado de ancho de banda. Este agregado es la práctica de considerar los requisitos de ancho de banda específicos de cada parte de la jerarquía. Después de que se conocen dichos requisitos de la red, se pueden agregar enlaces entre switches específicos, lo que recibe el nombre de agregado de enlaces. El agregado de enlaces permite que se combinen los enlaces de puerto de los switches múltiples a fin de lograr un rendimiento superior entre los switches [CCN2007].

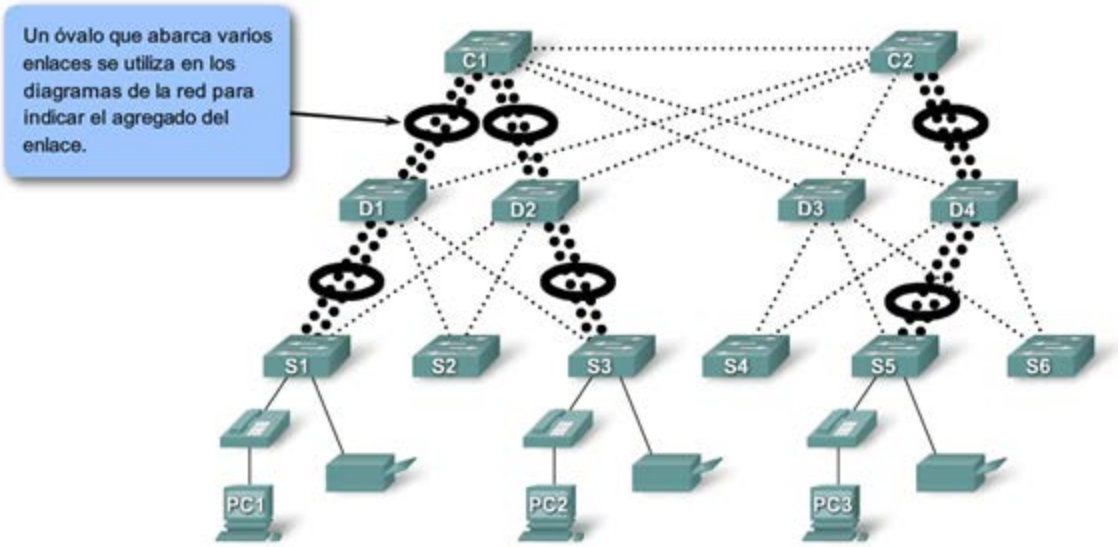

Figura 2.3-6: Agregado de Ancho de Banda
Fuente: [CCN2007]

En la figura 2.3-6, las computadoras PC1 y PC3 requieren una cantidad significativa de ancho de banda porque se utilizan para desarrollar simulaciones de condiciones climáticas. El administrador de la red determina que los switches S1, S3 y S5 de la capa de acceso requieren un aumento del ancho de banda. Estos switches de la capa de acceso respetan la jerarquía y se conectan con los switches de distribución D1, D2 y D4. Los switches de distribución se conectan con los switches C1 y C2 de la capa núcleo. Observe cómo los enlaces específicos en puertos específicos se agregan en cada switch. De esta manera, se suministra un aumento del ancho de banda para una parte específica seleccionada de la red. Observe que en esta figura se indican los enlaces agregados por medio de dos líneas de puntos con un óvalo que las relaciona. En otras figuras, los enlaces agregados están representados por una línea de puntos única con un óvalo.

2.3.3.3. Redundancia

La redundancia es una parte de la creación de una red altamente disponible. Se puede proveer redundancia de varias maneras. Por ejemplo, se pueden duplicar las conexiones de red entre los dispositivos o se pueden duplicar los propios dispositivos.

La implementación de los enlaces redundantes puede ser costosa. Imagine que cada switch en cada capa de la jerarquía de la red tiene una conexión con cada switch de la capa siguiente. Es improbable que sea capaz de implementar la redundancia en la capa de acceso debido al costo y a las características limitadas en los dispositivos finales, pero puede crear redundancia en las capas de distribución y núcleo de la red.

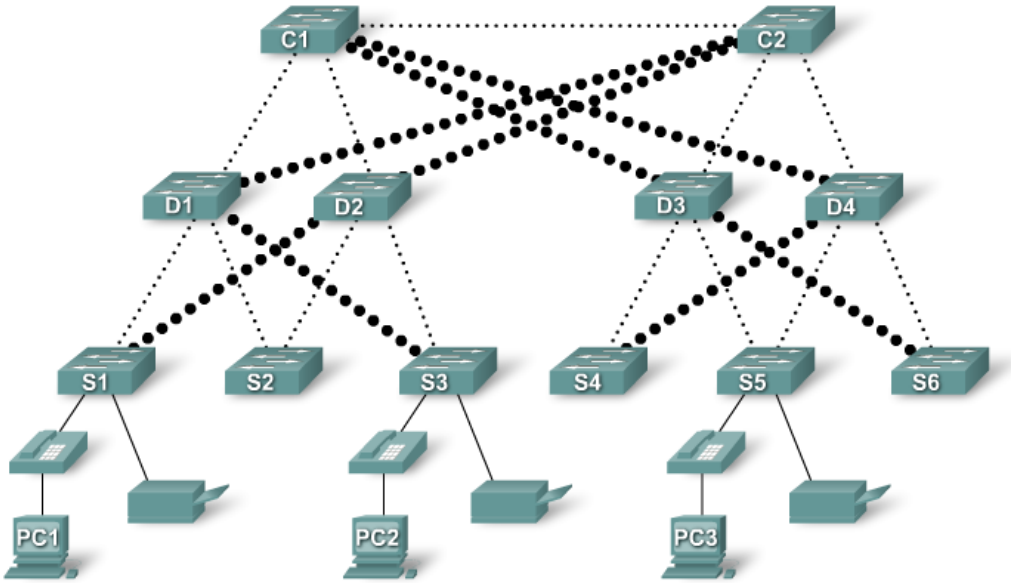

Figura 2.3-7: Redundancia en la red
Fuente: [CCN2007]

En la figura, los enlaces redundantes se observan en la capa de distribución y en la capa núcleo. En la capa de distribución existen dos switches, el mínimo requerido para admitir redundancia en esta capa. Los switches de la capa de acceso, S1, S3, S4 y S6, se encuentran interconectados con los switches de la capa de

distribución. Esto protege su red si falla uno de los switches de distribución. En caso de falla, el switch de la capa de acceso ajusta su ruta de transmisión y reenvía el tráfico a través del otro switch de distribución.

Ciertas situaciones de falla de la red nunca pueden impedirse, por ejemplo si la energía eléctrica se interrumpe en la ciudad entera o el edifico completo se derrumba debido a un terremoto. La redundancia no intenta abordar estos tipos de desastres [CCN2007].

2.4. IEEE Tecnologías LAN

Como resultado de la investigación realizada por Xerox Corporation a principios de los años 70, Ethernet se consagró como un protocolo ampliamente reconocido aplicado a las capas físicas y de enlace. Posteriormente apareció Fast Ethernet que incrementó la velocidad de 10 a 100 megabits por segundo (Mbit/s). Gigabit Ethernet fue la siguiente evolución, incrementando en este caso la velocidad hasta 1000 Mbit/s (1 Gbit/s). La idea de obtener velocidades de 1 Gbit/s sobre Ethernet se gestó durante 1995, una vez aprobado y ratificado el estándar Fast Ethernet, y prosiguió hasta su aprobación en junio de 1998 por el IEEE como el estándar 802.3z (z, por ser la última letra del alfabeto, y pensar que sería la última de la familia Ethernet), comúnmente conocido como 1000BASE-X.

IEEE 802.3ab, ratificada en 1999, define el funcionamiento de Gigabit Ethernet sobre cables de cobre del tipo UTP y categoría 5, 5e o 6 y por supuesto sobre fibra óptica. De esta forma, pasó a denominarse 1000BASE-T. Se decidió que esta ampliación sería idéntica al Ethernet normal desde la capa de enlace de datos hasta los niveles superiores, permitiendo el aprovechamiento de las posibilidades de la fibra óptica para conseguir una gran capacidad de transmisión sin tener que cambiar la infraestructura de las redes actuales.

Inicialmente, Gigabit Ethernet fue muy utilizado sobre redes de gran capacidad, como por ejemplo, redes de comunicación de universidades. En 2000, Apple's Power Mac G4 y PowerBook G4 fueron las primeras máquinas en utilizar la conexión 1000BASE-T, a las que siguieron posteriormente Macintoshes y PC´s.

En 2002, IEEE ratificó una nueva evolución del estándar Ethernet, 10 Gigabit Ethernet, con un tasa de transferencia de 10 000 megabits por segundo (10 veces mayor a Gigabit Ethernet).

2.4.1. Gigabit Ethernet

Gigabit Ethernet, también conocida como GigaE, es una ampliación del estándar Ethernet IEEE 802.3ab y IEEE 802.3z que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet o 100BASE-TX.

Gigabit Ethernet surge como consecuencia de la presión competitiva de ATM por conquistar el mercado LAN y como una extensión natural de las normas Ethernet 802.3 de 10 y 100 Mbit/s. que prometen tanto en modo semi-dúplex como dúplex, un ancho de banda de 1 Gbit/s. En modo semi-dúplex, el estándar Gigabit Ethernet conserva con mínimos cambios el método de acceso CSMA/CD.

En cuanto a las dimensiones de red, no hay límites respecto a extensión física o número de nodos. Al igual que sus predecesores, Gigabit Ethernet soporta diferentes medios físicos, con distintos valores máximos de distancia. Es una tecnología aplicada a los mejores montajes de las redes LAN a nivel mundial.

El gran interés por la propuesta Gigabit Ethernet se debe a su simplicidad, fiabilidad, compatibilidad hacia atrás y costes.

2.4.1.1. IEEE 802.3az

- 1000BASE-SX: Fibra Multimodo (MMF), laser 850 nm, distancia < 550 m.
- 1000BASE-LX: Fibra SMF, laser 1310 nm, Distancia < 10 km.
- 1000BASE-EX: Fibra SMF, laser 1310 nm, distancia < 40 km.
- 1000BASE-ZX: Fibra SMF, laser 1550 nm, distancia < 80 km.
- 1000BASE-CX: Cable STP (2 pares), distancia < 25 m.

2.4.1.2. IEEE 802.3ab

- 1000BASE-T
  - Cable UTP-5e (125 MHz) con 4 pares.
  - Codificación PAM-5.
  - Distancia < 100 m.
  - Full-Duplex (FDX) dual.

2.4.2. 10 Gigabit Ethernet

10-gigabit Ethernet (XGbE o 10GbE) actualmente es el estándar que se está aplicando hacia la LAN/MAN/WAN, fue presentado en el año 2002 y más rápido de los estándares Ethernet después de 40GbE y 100 GbE. IEEE 802.3ae define una versión de Ethernet con una velocidad nominal de 10 Gbit/s, diez veces más rápido que gigabit Ethernet.

El estándar 10-gigabit Ethernet contiene siete tipos de medios para LAN, MAN y WAN. Ha sido especificado en el estándar suplementario IEEE 802.3ae, y está incluido en las librerías del estándar IEEE 802.3.

2.4.2.1. IEEE 802.3ae

- 10GBASE-SR - ("short range") -- Diseñada para funcionar en distancias cortas sobre cableado de fibra óptica multi-modo, permite una distancia entre 26 y 82 m dependiendo del tipo de

cable. También admite una distancia de 300 m sobre una nueva fibra óptica multi-modo de 2000 MHz·km (usando longitud de onda de 850nm).

- 10GBASE-LR ("long range")-- Este estándar permite distancias de hasta 10 km sobre fibra mono-modo (usando 1310nm).
- 10GBASE-ER ("extended range")-- Este estándar permite distancias de hasta 40 km sobre fibra mono-modo (usando 1550nm). Recientemente varios fabricantes han introducido interfaces de hasta 80-km.

2.4.2.2. IEEE 802.3an

- 10GBASE-T: Diseñada para funcionar bajo cableado LAN UTP, en categorías 6, 6a, 7, hasta una máxima distancia de 100 m, codificación PAM-16.

2.5. Redes Convergentes

2.5.1. Redes múltiples de múltiples servicios

El teléfono tradicional, la radio, la televisión y las redes de datos informáticos tienen su propia versión individual de los cuatro elementos básicos de la red. En el pasado, cada uno de estos servicios requería una tecnología diferente para emitir su señal de comunicación particular. Además, cada servicio tiene su propio conjunto de reglas y estándares para garantizar la comunicación exitosa de su señal a través de un medio específico [CCN2007].

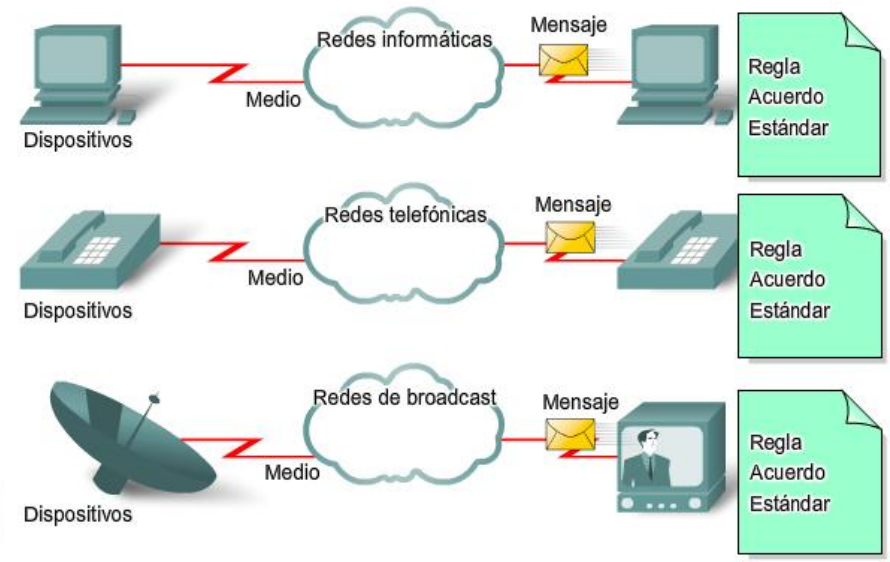

Figura 2.4-1: Redes tradicionales
Fuente: [CCN2007]

2.5.2. Redes convergentes

Los avances de la tecnología nos permiten consolidar esas redes dispersas en una única plataforma: una plataforma definida como una red convergente. El flujo de voz, vídeo y datos que viajan a través de la misma red elimina la necesidad de crear y mantener redes separadas. En una red convergente todavía hay muchos puntos de contacto y muchos dispositivos especializados (por ejemplo: computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas) pero una sola infraestructura de red común [CCN2007].

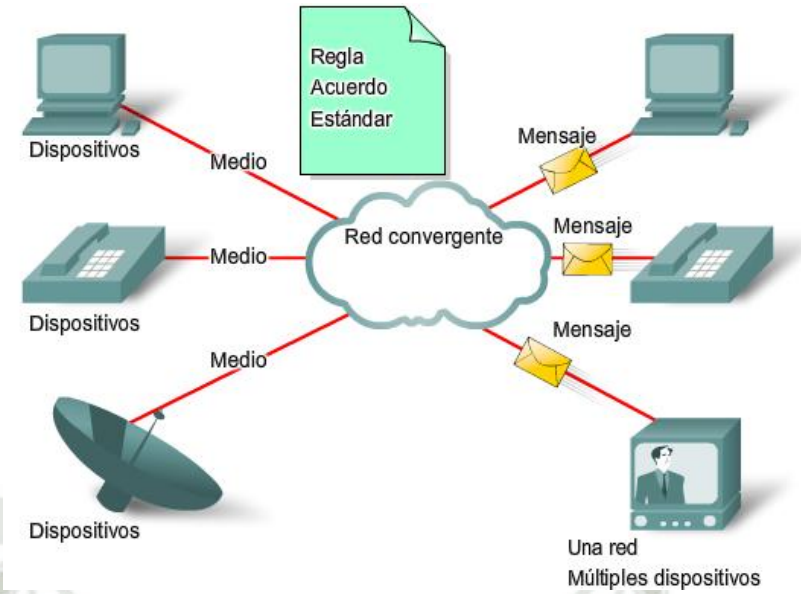

Figura 2.4-2: Redes Convergentes
Fuente: [CCN2007]

2.5.3. Redes de información inteligentes

La función de la red está evolucionando. La plataforma de comunicaciones inteligentes del futuro ofrecerá mucho más que conectividad básica y acceso a las aplicaciones. La convergencia de los diferentes tipos de redes de comunicación en una plataforma representa la primera fase en la creación de la red inteligente de información. En la actualidad nos encontramos en esta fase de evolución de la red. La próxima fase será consolidar no sólo los diferentes tipos de mensajes en una única red, sino también consolidar las aplicaciones que generan, transmiten y aseguran los mensajes en los dispositivos de red integrados. No sólo la voz y el video se transmitirán mediante la misma red, sino que los dispositivos que realizan la conmutación de teléfonos y el broadcasting de videos serán los mismos dispositivos que enrutan los mensajes en la red. La plataforma de comunicaciones resultante proporcionará funcionalidad de aplicaciones de alta calidad a un costo reducido [CCN2007].

2.6. Calidad de servicio QoS

2.6.1. Qué es QoS

"Conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo" (Recomendación IETF RFC 2386) [EPA2005].

"Calidad de servicio es un conjunto de herramientas disponibles para los administradores de red para asegurar que un mínimo nivel de servicio sea proporcionado a cierto tipo de tráfico" [MEF2001].

La calidad de servicio está dada por la capacidad de soportar diferentes tipos de tráfico a través de una misma estructura, satisfaciendo la necesidad de ciertos requerimientos que cada tipo de tráfico presente.

La Calidad de Servicio (QoS) es el efecto global de la calidad de funcionamiento de un servicio que determina el grado de satisfacción de un usuario de un servicio.

2.6.2. Finalidad de QoS

Satisfacer en la medida de lo posible las expectativas del usuario con respecto a un determinado servicio prestado.

Calidad de servicio puede ser implementada para:

- Dar prioridad a las aplicaciones de misión crítica en la red.
- Maximizar el uso de la inversión actual en infraestructura de red.
- Mejorar el rendimiento para las aplicaciones sensibles al retardo como son las aplicaciones de voz y video.
- Responder adecuadamente ante los cambios en los flujos de tráfico en la red.

2.6.3. Factores que afectan la QoS

La calidad de servicio suele ser muy variable dependiendo no solo de los requerimientos de los flujos de datos de las aplicaciones sino también debido a ciertos factores que pueden llevar a su degradación total o parcial.

2.6.3.1. Retardo o Latencia

Diferencia existente entre el momento en que una señal es transmitida y el momento en que la misma llega a su destino. Existen dos tipos de fuentes de retardo:

a. Retardo Constante:

Se consideran dentro de este tipo a aquellas fuentes que siempre generan la misma cantidad de retardo entre ellas tenemos:

- **Retardo de paquetización**: Retardo generado al convertirse en paquetes IP.
- **Retardo de serializacion**: Retardo generado debido a la colocación de los paquetes en las interfaces por las cuales serán enviados.
- **Propagación**: Retardo generado debido al paso de los paquetes por los diferentes medios de transporte (cables, fibra óptica, aire) hasta llegar a su destino.

b. Retardo Variable

Dentro de esta categoría se tiene:

- **Encolamiento**: Retardo generado por el tiempo de espera para ser transmitido en las colas de los

dispositivos. Es calculado como el retardo de serializacion de los paquetes que se transmitirán antes en la cola.

Para el retardo de serializacion se puede tomar en cuenta el peor de los casos que es cuando se transmiten paquetes con el tamaño de la MTU.

- **Retardo de procesamiento o de reenvío:** Retardo producido al recibir una trama procesar y decidir su reenvío colocándola en la cola de egreso. Este retardo no considera el retardo de encolado. Es variable dependiendo del trabajo que estén realizando los equipos. El retardo es sin duda uno de los principales retos que tiene la transmisión de paquetes en redes convergente donde exista data, video y voz a través de la red IP; ya que estos tienen un tiempo máximo para ser transmitido desde el origen a su destino.

2.6.3.2. Jitter

Variación en el retardo de paquetes de un mismo flujo de información. El Jitter es considerado como la diferencia entre el tiempo real y el tiempo esperado de llegada de un paquete a su destino.

A diferencia de las transmisiones de datos, las transmisiones de tráfico de voz y video suelen ser muy propensas a sufrir serias afecciones debido al jitter. Un retardo excesivo entre el envío de paquetes y su recepción puede tener como resultado una recepción de video y comunicación de voz deficiente.

El jitter es usado por aquellas aplicaciones que dependen de alguna forma de garantía de que los paquetes se procesen en períodos de tiempos específicos, frente a este inconveniente se ha desarrollado los buffer jitter que consisten en regular la velocidad de audio durante una

transmisión manteniendo una velocidad constante, para ello es necesario que los paquetes lleguen con cierta frecuencia en caso contrario el buffer no podrá controlarlos y los perderá, y, si esta pérdida es superior al 1% de la totalidad de paquetes será percibida por los usuarios [OWE2005].

2.6.3.3. Pérdida de Paquetes

Las comunicaciones de Data, Video y Voz sobre las Redes IP son susceptibles a las pérdidas de paquetes considerando que para el transporte de los paquetes de data por lo general es utilizando el protocolo TCP el cual tiene mecanismos de reenvío de paquetes perdidos, y en cuanto a video y voz utilizamos el protocolo UDP y que éste último no implementa mecanismos de control de recuperación de pérdidas.

2.6.4. Principios de QoS

2.6.4.1. Clasificación y marcado

La clasificación consiste en la diferenciación de tráfico y tratamiento del mismo asociado a diferentes clases de servicio; el marcado de paquetes implica la configuración de algunos bits en las cabeceras de enlace de datos y/o de red con el fin de distinguir el tráfico.

Para el marcado de paquetes se puede determinar condiciones de coincidencia en una ACL o directamente en una clase de servicio.

2.6.4.2. Eficiencia

Consiste en el uso y la distribución eficaz de los recursos de la Red. Supongamos que el flujo de VoIP tiene asignado 1 Mb como máximo y el flujo de datos tiene 0.5 Mb; una vez que se ha preestablecido

esta distribución se procede al envío de ambos flujos, resultando que el flujo de datos se envía en 10 segundos mientras el de VoIP en 45. Existe 35 segundos durante la transmisión en que sólo se usa el 66.67 % del total del canal desperdiciándose el 33.33 %. Se debe implementar mecanismos que permitan la asignación dinámica de recursos a los diferentes flujos de datos.

2.6.4.3. Límite de Recursos

Ahora bien, que sucede si llega un tercer flujo de datos con un requerimiento de 1 Mb durante la transmisión del flujo de VoIP de 1 Mbps y el flujo de datos de 0.5 Mb, considerando que el canal solo dispone de 1.5 Mbps de capacidad total; en este caso la red podrá bloquear al nuevo flujo de datos solicitante ya que no puede cubrir su requerimiento. Por lo tanto la red sólo podrá satisfacer requerimientos hasta cubrir el máximo de capacidad del enlace en caso contrario deberá bloquear las nuevas peticiones.

2.6.5. Arquitectura de QoS

2.6.5.1. Best-Effort

Servicio Best-Effort o servicio de “Mejor Esfuerzo” se caracteriza por no brindar garantías de Calidad de Servicio (QoS) en las transmisiones. La redes best-effort tratan todos los paquetes como si fueran iguales y trabajan muy bien en entornos donde de disposición de recursos es muy alta y no se tiene limitaciones de CPU, memoria y el ancho de banda es lo suficientemente grande para manejar y servir los paquetes apenas estos lleguen; sin embargo, encontrar una red bajo estas condiciones no es muy común [MEF2001].

Las transmisiones VoIP son sensibles al retardo y al jitter debido a esto el uso del servicio Best-Effort no es recomendable.

2.6.5.2. DiffServ

DiffServ (Servicios Diferenciados) especificado en el RFC 2475, se caracteriza por manejar la información de clase de servicio en cada paquete independiente del número de flujos presentes en la red. DiffServ "añade" el campo DS a los paquetes IP (RFC 2474), en realidad ocupa el campo denominado ToS.

La estructura del campo DS está dividido en dos bloques:

- DSCP: Valor de 6 bits que permiten generar hasta 64 posibles categorías de tráfico (codepoints)

2.6.6. Herramientas de clasificación y marcado de paquetes

La clasificación es la primera función QoS que se aplica antes de cualquier otra política. Para clasificar tráfico los paquetes deben de coincidir con un "patrón" establecido como podrían ser ACLs, valores de campos de encabezados, interfaces de salida, direcciones MAC, entre otros [OWE2005].

El marcado es el mecanismo consiste en configurar determinados bits en las cabeceras de los paquetes basados de acuerdo a la clasificación, valores de mapeos, valores por default, entre otros.

El marcado determina la prioridad entre paquetes y el modo en que estos deben ser tratados, por ejemplo si se desea enviar un paquete de VoIP este deberá ser marcado con prioridad alta y será enviado con mayor rapidez que otros paquetes, así mismo no es candidato a ser eliminado en algún punto de la ruta.

El marcado de paquetes además determina el límite de confianza; es decir, hasta que dispositivo se puede confiar los valores de marcado y la diferenciación de tráfico de tal manera que se pueden dar los siguientes casos cuando un paquete entra a un dispositivo:

- Los paquetes no están marcados.
- Los paquetes están marcados pero el marcado es diferente.
- Los paquetes están marcados y guardan relación con los marcados establecidos.

En los dos primeros casos es recomendable remarcar los paquetes.

a. Marcado de paquetes a nivel LAN/WAN

LAN		WAN	
Campo	**Localización**	**Campo**	**Localización**
IP Precedence	Cabecera IP	Discard Elegible (DE)	Cabecera frame relay
IP DSCP	Cabecera IP	MPLS Experimental values	Cabecera MPLS
DS	Cabecera IP		
ToS	Cabecera IP	Cell Loss Priority (CLP)	Cabecera de la celda ATM
ToS	Cabecera IP		
CoS	ISL and 802.1Q/P		

Tabla 2.6-1: Ejemplos de marcado de paquetes en LAN y WAN
Fuente: [TSZ2004]

b. IP precedence y DSCP

A nivel de capa 3 las herramientas más utilizadas son: IP precedence y DSCP que utilizan los bits del campo ToS del encabezado IP.

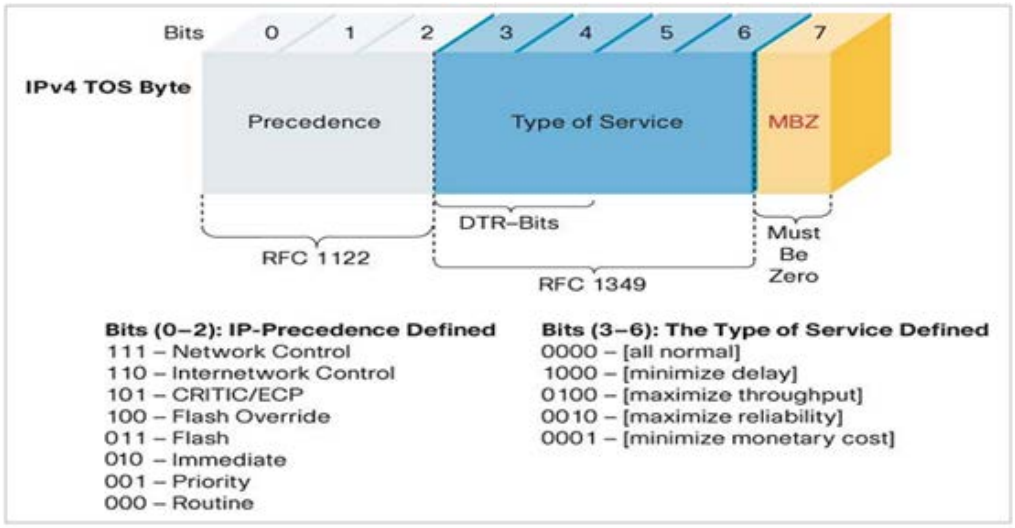

Figura 2.6-2: Campo ToS - IP precedence
Fuente: [5]

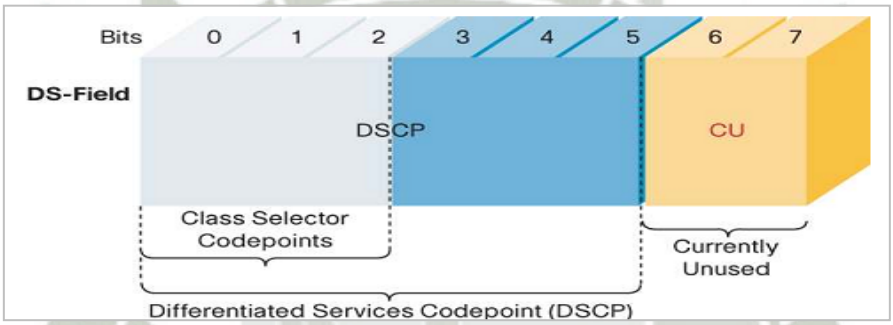

Figura 2.6-3: Campo ToS – DSCP
Fuente: [5]

c. Ethernet 802.1Q y ISL

A nivel de capa 2 en redes LAN la tecnología más utilizadas es Ethernet por lo cual la herramienta de clasificación más usada es Ethernet CoS dentro de encabezados ISL o 802.1Q.

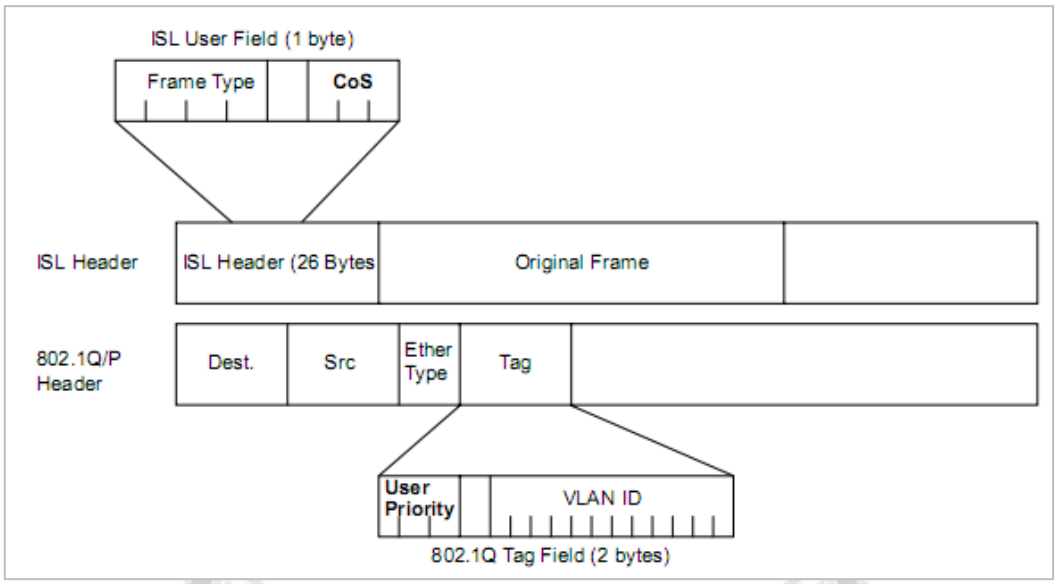

Figura 2.6-4: CoS en ISL y 802.1Q
Fuente: [5]

Capítulo 3

Metodología de Implementación de Red de datos de campus y Enterprise

3.1. Objetivo

Proponer un modelo de implementación de red jerárquica IP analizando la elección y utilización de diferentes tecnologías de red lógicas, físicas y demostrando como éstas mejoran el rendimiento de una red.

3.1.1. Necesidad de un modelo de implementación

El plan de diseño de red jerárquico depende de los servicios y aplicaciones proporcionadas y utilizadas, los recursos disponibles y el soporte de la red para su implementación y desarrollo; debido a esto no podemos considerar una "fórmula general" que vaya a proporcionar buenos resultados para todo tipo de organización de acuerdo a su Core Bussiness, mas sí podemos seguir una serie de pasos y realizar evaluaciones que puedan concluir en un modelo flexible que pueda adecuarse al tipo de organización que lo requiere.

Se considera necesario un modelo de implementación debido a que frecuentemente los problemas de diseño y del de rendimiento de una red se muestran cuando cambian o se agregan servicios y aplicaciones o las reglas de red que se tienen varían.

Otro motivo de contar con un modelo de implementación, es que éste debe considerar la implementación desde las capas superiores hasta la inferior, es decir, se debe tener control de todas las aplicaciones que se brindan en capa 7 y definir todos sus requerimientos de la aplicación pasando por las diversas capas hasta la capa 1 en forma descendente.

3.2. Estructura del modelo

La metodología presentada está dividida en cuatro partes:

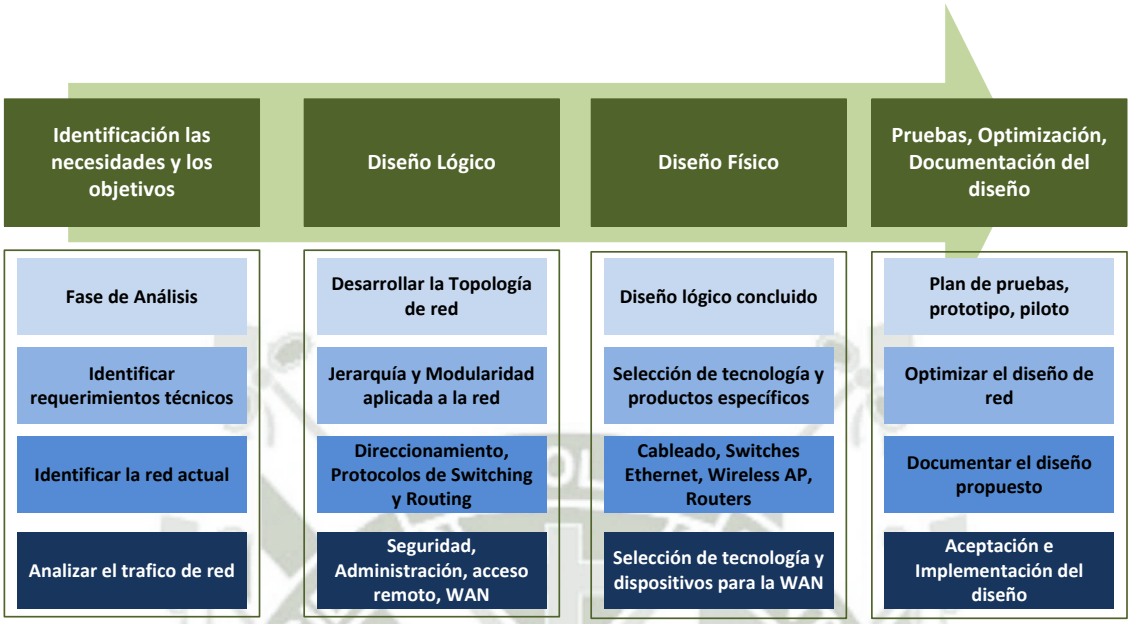

Figura 3.2-1: Estructura del modelo
Fuente: Elaboración Propia

Identificación las necesidades y objetivos

En la primera parte se cubrirán análisis de requerimientos. Empezará identificando metas y requerimientos, labores de identificación de la red actual incluyendo arquitectura y performance de los principales segmentos y dispositivos. Luego se analizará el tráfico de red incluyendo carga y flujo de tráfico, comportamiento de protocolos y calidad de servicio QoS.

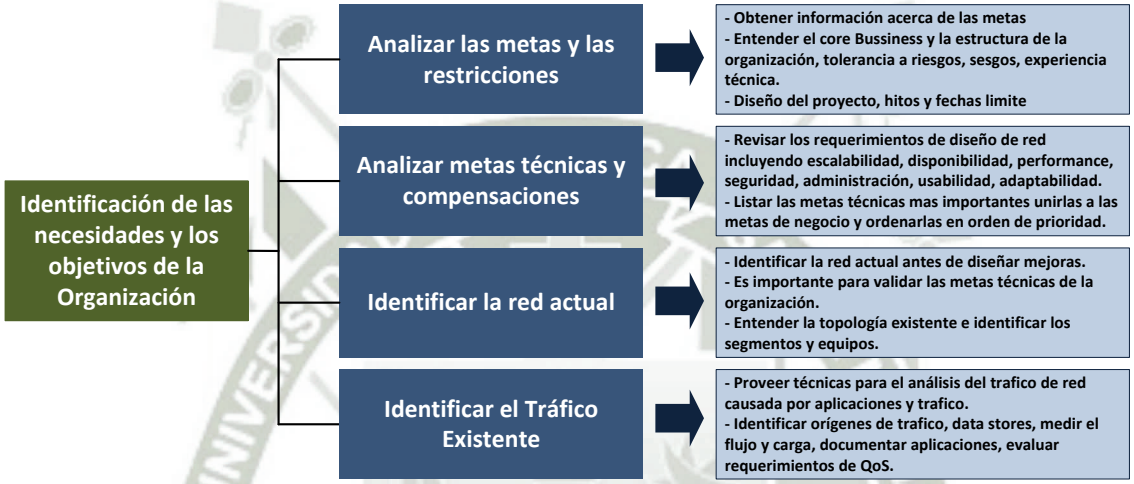

Figura 3.2-2: Estructura del modelo Parte I
Fuente: Elaboración Propia

Diseño de red Lógico

Durante la fase de diseño lógico, se desarrollará la topología de red. Dependiendo del tamaño de la red e identificación del tráfico, la topología puede ser desde simple a compleja, requiriendo jerarquía y modularidad. En esta parte el diseñador de la red elaborará el modelo de direccionamiento y seleccionará protocolos de switching y enrutamiento. El diseño lógico también incluye plan de seguridad, administración, e investigación inicial de proveedores WAN.

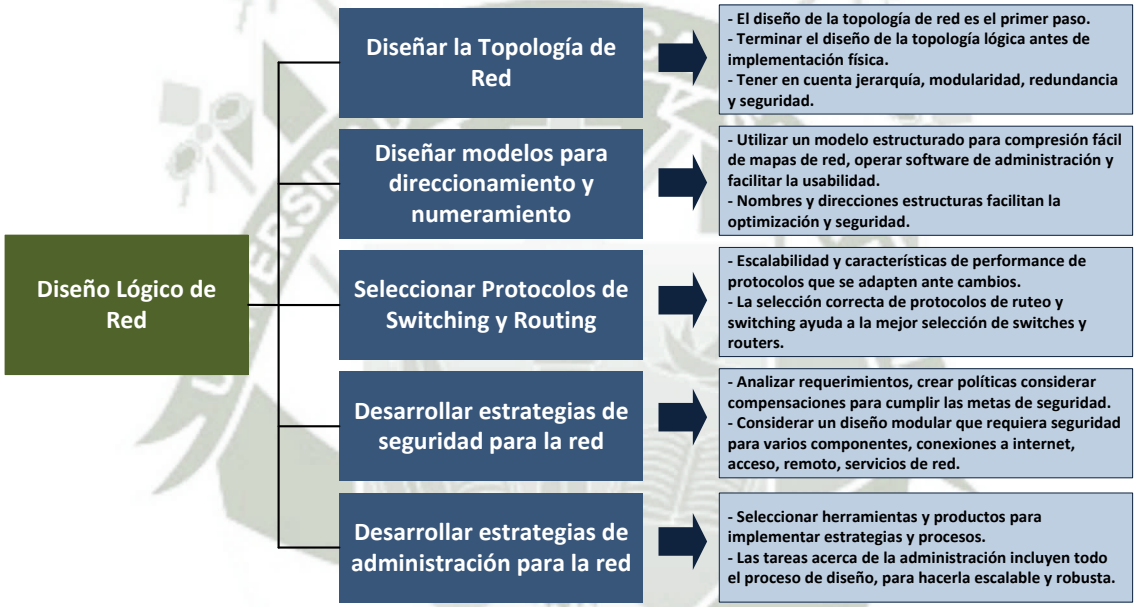

Figura 3.2-3: Estructura del modelo II
Fuente: Elaboración Propia

Diseño de red Físico

Durante la fase de diseño físico, tecnologías específicas y productos que cumplan con el diseño lógico serán elegidas. Empieza con la selección de tecnologías y dispositivos para redes de campus incluyendo cableado y switches Ethernet, Access points, bridges inalámbricos y routers. Selección de dispositivos de acceso remoto y necesidades de WAN. Además la investigación de los proveedores WAN, debe estar completa en esta fase.

Figura 3.2-4: Estructura del modelo III
Fuente: Elaboración Propia

Pruebas, Optimización, Documentación del diseño

Los pasos finales en diseño de red son escribir e implementar un plan de pruebas, construir un piloto, optimizar el diseño de red, y documentar la red. Si las pruebas indican problemas de performance se debe actualizar el diseño e incluir características de traffic shaping y mecanismos avanzados de switching y routing.

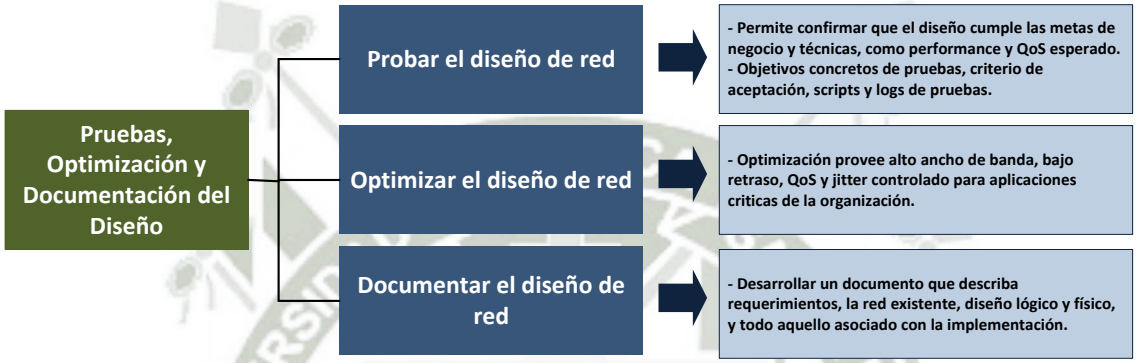

Figura 3.2-5: Estructura del modelo IV
Fuente: Elaboración Propia

IDENTIFICACIÓN DE LAS NECESIDADES Y LOS OBJETIVOS

3.3. Analizar las metas y restricciones de la organización

3.3.1. Utilizar la metodología Top Down

- El punto de partida de esta metodología es iniciar en la capas superiores del modelo OSI y luego ir descendido a las capas inferiores. Además de explorar la estructura de la organización y a los grupos a quienes se dará el servicio de red, de donde el diseñador de la red obtendrá información valiosa para que el diseño sea exitoso.
- Este diseño es iterativo y para no quedarse estancado en detalles muy rápidamente, lo primero que se debe hacer es tener todos los requerimientos de la organización.

3.3.1.1. Utilizar el proceso de Diseño de red estructurado

- La meta principal es hacer el análisis más preciso enfocado en las necesidades del usuario final. Otra meta es hacer el proyecto manejable dividiéndolo en módulos que pueden ser más sencillos de mantener o cambiar.

- El análisis de los sistemas estructurados siguen las siguientes pautas:
  - El sistema de red está diseñado utilizando la secuencia top-down.
  - Durante el diseño del proyecto se pueden utilizar muchas técnicas para identificar la red existente, nuevos requerimientos de usuario y proponer una estructura para el futuro sistema de red.
  - Enfocarse en flujo de data, tipos de data, procesos que accedan o cambian la data.

- Enfocarse en comprender y entender la ubicación, necesidades de las comunidades de usuario que acceden o cambian la data.
- El modelo lógico es desarrollado antes del modelo físico. El modelo lógico representa bloques básicos de la organización, divididos por función y la estructura del sistema. El modelo físico representa equipos y tecnologías específicas e implementaciones.
- Las especificaciones derivan de los requerimientos obtenidas al inicio de la secuencia top-down.

3.3.1.2. Ciclo de vida de desarrollo de sistemas de red

- Típicamente los sistemas de red son desarrollados y existen por un periodo de tiempo.
- En la metodología se seguirán las cuatro fases principales:

- Análisis de requerimientos
  - Analizar las metas y restricciones de la empresa y su rubro de negocio.
  - Analizar las metas técnicas y compensaciones.
  - Identificar la red existente.
  - Identificar el tráfico de red.

- Desarrollo del diseño lógico
  - Diseñar la topología de red.
  - Diseñar modelos para direccionamiento y nombramiento.
  - Seleccionar protocolos de conmutación y enrutamiento.
  - Desarrollar estrategias de seguridad de red.
  - Desarrollar estrategias de manejo de red.

- Desarrollo del diseño físico
  - Seleccionar tecnologías y dispositivos para redes de campus.
  - Seleccionar tecnologías y dispositivos para redes empresariales.

- Pruebas, Optimización y documentación del diseño.
  - Probar el diseño de red
  - Optimizar el diseño de red
  - Documentar el diseño de red

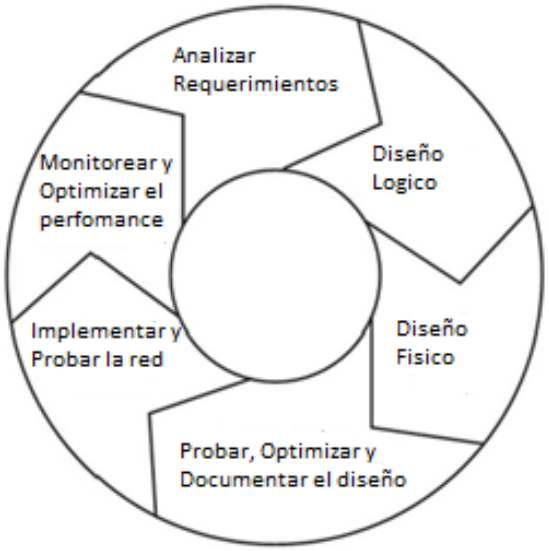

Figura 3.3-1: Ciclo de vida de sistemas de red
Fuente: [POP2011]

3.3.2. Analizar las metas de la organización

- Basado en los objetivos usted puede armar un diseño que cumpla con las expectativas de la organización.

3.3.2.1. Trabajar con el usuario

- Tener en claro la estructura organizacional de la compañía.
- Probablemente el diseño final reflejara la estructura de la compañía, entonces es importante tener información de la estructura de la compañía, departamentos, línea de negocio, vendors, partners, campo y oficinas remotas.
- Pregunte a la organización la meta final del proyecto de diseño de red. ¿Para qué se está haciendo el nuevo proyecto de diseño de red? ¿Para qué se utilizara la red? ¿Cómo la red ayudara a la organización para la satisfacción de sus clientes, usuarios?
- Se debe tener en claro las consecuencias del éxito del proyecto o del fracaso del mismo.

3.3.2.1.1. Cambios en la red Enterprise

- La red que es utilizada solo por los usuarios internos ya no es una norma en muchas compañías.
- El diseñador de la red debe considerar cuidadosamente los requerimientos para extender la red a usuarios externos.

3.3.2.1.2. La necesidad de soportar usuarios móviles

- Los usuarios deben tener acceso seguro y confiable para acceder a herramientas y la data desde donde se encuentren.
- Los desafíos son hacer que la data se transporte por varios medios sin que se ve comprometida.
- El diseñador tiene el desafío de desarrollar soluciones seguras, resistentes y administrables que habiliten al usuario de realizar su trabajo segura y eficientemente desde donde se encuentren.

3.3.2.1.3. La importancia de la seguridad y resistencia en la red

- En el caso de que algún problema de seguridad y operacional suceda, las redes deben recuperarse rápidamente.
- Las redes deben mantenerse operativas durante y después de algún desastre.
- En el mercado actual, seguridad y recuperación ante desastres deben ser consideradas en cada opción de diseño y el diseñador debe proponer soluciones que provean resistencia y seguridad.

3.3.2.2. Metas típicas del diseño de red en organizaciones

- Incremento de ganancias y competitividad
- Incremento de cuota de mercado
- Expansión en otros mercados
- Incrementar ventajas competitivas sobre otras compañías
- Reducir costos
- Incrementar la productividad
- Ofrecer nuevos servicios
- Ofrecer mejor soporte al cliente y usuario
- Evitar interrupción del servicio causado por problemas de seguridad
- Evitar interrupción del servicio causado por desastres
- Modernizar la tecnología
- Reducir costos de telecomunicaciones y de red, incluyendo sobrecarga de voz, video, datos

3.3.2.3. Identificar el ámbito del proyecto de diseño de red

- Uno de los primeros pasos en el diseño de red es identificar el ámbito.

- ¿Pequeño en ámbito? Permitir que la gente de ventas, u otros que ingresen a la red interna vía VPN?
- ¿Amplio en ámbito? Rediseño de toda la red empresarial
- Explique a la organización si tiene alguna preocupación acerca del ámbito del proyecto ya sea técnica o de negocio.
- Utilice el modelo OSI para aclarar las dudas en cuanto al ámbito del proyecto.

3.3.2.4. Identificar las aplicaciones de la red

- Preguntar al responsable de la organización acerca de las aplicaciones

Nombre de la aplicación	Tipo de aplicación	Aplicación nueva (si o no)	Critica	Comentarios

Tabla 3.3-1: Identificar aplicaciones
Fuente: Elaboración Propia

- En nombre de aplicación, utilizar un nombre simple como Exchange o el nombre de la aplicación que sea identificado por la organización.

- En tipo de aplicación, puede utilizar el texto que describa a la aplicación:
  - Email
  - FTP
  - WEB
  - Base de datos
  - Terminal remoto
  - Video Conferencia
  - Video en demanda

- Video multicast
- Telefonía IP local
- File server
- ERP

De ser requerido indicar si existe aplicaciones de sistema

- Autenticación y autorización de usuarios
- DNS
- DHCP
- Boot remoto
- Configuración remota
- Active Directory
- Backup de red
- Administración de red
- Distribución de software
- Configuración de aplicaciones

- En la columna de “critica”
  - 1. Extremadamente critica
  - 2. Algo critica
  - 3. No critica

- En la columna de “comentarios” añadir observaciones relevantes al diseño de red.

3.3.3. Analizar metas y restricciones

3.3.3.1. Política y Políticas

- En el caso de política de oficina es mejor escuchar antes de hablar. La meta es obtener agendas escondidas, peleas, sesgos, relaciones

entre grupos o historias detrás del proyecto que puedan causar su falla.

- Prestar atención a problemas personales que puedan afectar al proyecto. Quienes son sus defensores y quienes sus oponentes.
- Estar seguro si el proyecto causara si algún puesto de trabajo será eliminado.
- Se tiene que conversar con la organización acerca de las pruebas que se realizaran, que nuevas políticas acerca de protocolos, estándares y vendors.
- En el apuro de obtener requerimientos técnicos los diseñadores de red a veces ignoran algunos problemas técnicos. Muchos proyectos brillantes de red pueden ser rechazados porque se basaron en las capas bajas del modelo OSI y no tomaron en cuenta la política de la compañía.

3.3.3.2. Restricciones de presupuesto y personal

- Tener en cuenta que el diseño incluirá en compra de equipamiento, licencias de software, acuerdos de mantenimiento y soporte, pruebas, entrenamiento y personal. Además de consultoría y otros.
- A lo largo del proyecto trabaje con la organización para identificar requerimientos de nuevo personal como administradores de red adicionales.
- Analizar las habilidades del personal actual, para recomendar si se necesitara entrenamiento o se deberá contratar outsourcing para la administración.
- Considerar que las tecnologías y protocolos que se incluyan en el diseño elevara el grado de experiencia y conocimiento del actual personal.

3.3.3.3. Programación del proyecto

- Preguntar acerca del tiempo que se tiene estimado para el desarrollo e implementación del proyecto de diseño de red. ¿Cuándo es la fecha final y cuáles son los principales hitos?
- Incluir hitos intermedios en la programación del proyecto ya que estos le dan la opción de revisar si hay tropiezos en la implementación.
- Tener en cuenta el estado del cableado de los edificios, si son de categorías bajas no soportaran nuevas aplicaciones. Si el cableado necesita ser reemplazado, eso influirá en la programación del proyecto.

3.3.4. Revisión de objetivos

- A este punto ya se debe tener claro los objetivos y preocupaciones de la organización. Tener en cuenta de haber realizado lo siguiente:

  - Investigar el core Bussiness y la competencia de la organización.
  - Entender la estructura de la organización.
  - Cumplido con la lista de metas de negocio.
  - Identificado las operaciones de misión crítica.
  - Entendido los criterios de éxito o fracaso del proyecto.
  - Entendido el ámbito del proyecto.
  - Identificado las aplicaciones de red.
  - Identificado soluciones propietarias y abiertas.
  - Presupuesto del proyecto.
  - Entendido la programación del proyecto.
  - Identificado las habilidades del personal.
  - Conversado el plan de capacitación.
  - Analizado la política y relaciones del personal dentro de la organización.

3.4. Analizar las metas técnicas y compensaciones

Las metas técnicas típicas incluyen: escalabilidad, disponibilidad, performance de la red, seguridad, capacidad de administración, usabilidad, adaptabilidad, asequibilidad.

3.4.1. Escalabilidad

- Se refiere a la habilidad de cuanto crecimiento puede soportar la red. Para algunas organizaciones la escalabilidad es una meta principal en algunos otros casos se añade usuarios, aplicaciones, lugares adicionales, y conexiones externas de la red a una tasa rápida.

3.4.1.1. Plan de expansión

- Tener en cuenta la expansión a uno, dos o cinco años de acuerdo al requerimiento de la organización.
- Las siguientes preguntas pueden ayudar a analizar la expansión:
  - ¿Cuántos sitios adicionales serán agregados en los próximos 1, 2, 5 años?
  - ¿Cuán extensivas serán las redes por cada sitio?
  - ¿Cuántos usuarios adicionales se incorporaran a la red en los próximos 1, 2, 5?
  - ¿Cuántos servidores adicionales se incorporan a la red en los próximos 1, 2, 5?

3.4.1.2. Expandir acceso a la data

- La meta de negocio de hacer la data disponible hacia los usuarios resulta en las siguientes metas técnicas para el escalamiento y la actualización de la redes:

- Conectar LAN departamentales separas en una red corporativa.
- Solucionar problemas de cuellos de botella LAN/WAN causados por el incremento de tráfico en la red.
- Proporcione servidores centralizados que residan en el data center.
- Hacer que la data sea accesible a la red IP corporativa.
- Añada nuevos sitios para soportar sucursales y sus trabajadores.
- Añada nuevos sitios y servicios para soportar comunicaciones seguras con clientes, proveedores, partners.

3.4.2. Disponibilidad

- La disponibilidad puede ser expresado en un porcentaje de tiempo de actividad por año, mes, semana, dio u hora comparado con un periodo de tiempo y es expresado en porcentajes.
- La disponibilidad es vinculada a la confiablidad, redundancia y resistencia.

3.4.2.1. Recuperación ante desastres

- Tener en cuenta que muchas organizaciones han reconocido la necesidad de tener un plan to sostener la continuidad del negocio en caso de desastres naturales y no naturales.
- El plan de recuperación ante desastres incluye el proceso de mantener la data con sus backups en otros lugares que no sean afectadas por el desastre.
- Tener en cuenta que se debe reconocer que partes de la red son críticas y necesitan tener su backup. Para un buen entendimiento se debe saber que dispositivos, enlaces, aplicaciones y personal son

críticos. Además debe hacer pruebas con todos los factores mencionados anteriormente.

3.4.2.2. Especificar requerimientos de disponibilidad

- Tener los requerimientos de disponibilidad con precisión.
- Deben ser especificados en tiempo de actividad por años, meses, semanas, días y horas.
- Las metas de disponibilidad deben ser basadas en el resultado del primero paso del diseño donde se identificó las aplicaciones de los usuarios.

3.4.2.2.1. Cinco nueves de disponibilidad

- Algunas organizaciones que no toleren tiempo de inactividad altos en su requerimiento solicitaran tiempo de servicio en 99.999 que son los cinco nueves de disponibilidad.
- Este requerimiento es difícil de alcanzar, debido a que se necesitara redundancia en equipos y enlaces, personal adicional y hardware y software confiable.
- Las potenciales fallas a considerar son falla en carriers, falla de software en routers o switches, incremento inesperado en el uso de ancho de banda, problemas de configuración, errores humanos, falla de energía, brechas de seguridad y fallas de software en aplicaciones de red.

3.4.2.2.2. El costo de estar fuera de servicio

- La disponibilidad de aplicaciones de misión crítica ejecutándose sin problemas con poco o nada de inoperatividad, es una meta general.

- Explicar a la organización el costo que tiene estar fuera de servicio.
- Para cada aplicación documentar cuánto dinero perderá la organización por hora de inoperatividad.

3.4.2.2.3. Tiempo medio entre fallas y tiempo para la reparación

- Además de expresar la disponibilidad como un porcentaje de tiempo de actividad, se puede definir la disponibilidad como tiempo medio entre fallas "MTBF – Mean time between failure" y tiempo para la reparación "MTTR – Mean time to repair"
- MTBF es el tiempo promedio en el cual cualquier dispositivo puede fallar.
- MTTR es el tiempo promedio que tomar reparar la falla.

$$\text{Disponibilidad} = \text{MTBF} / (\text{MTBF}+\text{MTTR})$$

Ecuación: Disponibilidad
Fuente: [POP2011]

- Se tiene que tener en cuenta que deben a ver varios valores de acuerdo a las diferentes partes de la red.

3.4.3. Performance de la red

- Tener en cuenta los siguientes factores: throughput, precisión, eficiencia, latencia y variación de latencia.
- Las metas de performance están ligadas al análisis de la red actual así como también a la escalabilidad.
- Antes de revisar factores de performance se debe tener en claro en crecimiento.

3.4.3.1. Definición de performance de red

La siguiente lista puede ayudar al análisis de requerimientos en cuanto a performance:

- Capacidad (ancho de banda)
- Utilización, Utilización óptima
- Throughput
- Carga ofrecida
- Precisión
- Eficiencia
- Latencia
- Variación de la latencia
- Tiempo de respuesta

3.4.3.2. Utilización óptima de red

- La utilización de la red se mide en cuanto ancho de banda es utilizado durante un periodo de tiempo.
- Se tiene que tener cuanto será la máxima utilización promedio de ancho de banda en un segmento.
- Si se tiene que un segmento utiliza más que su umbral máximo permitido se tiene que desdoblar en múltiples segmentos o aumentar ancho de banda en el enlace.
- En promedio el 70% es un óptimo porcentaje de utilización. Si este umbral se supera se tiene que tener planificado el aumento de ancho de banda del enlace.
- Tener en cuenta que las LAN tienen mucho más ancho de banda que las WANs.

3.4.3.3. Throughput

- Throughput es la cantidad de datara libre de errores que es transmitida por unidad de tiempo.
- Idealmente throughput es lo mismo que capacidad, la capacidad depende de las tecnologías de la capa física.
- La capacidad de la red debe ser adecuada para manejar la carga ofrecida, a pesar de que haya picos de tráfico.

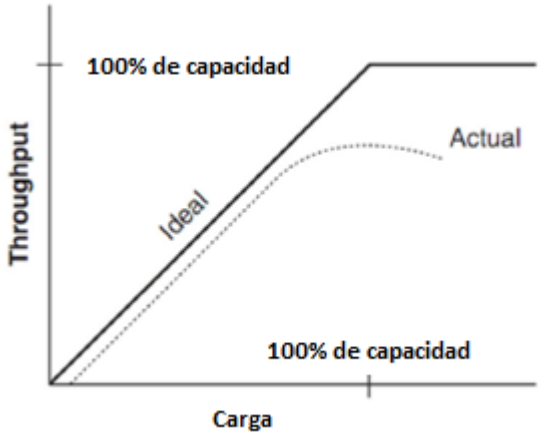

Figura 3.4-1: Carga Ofrecida y Throughput
Fuente: [POP2011]

3.4.3.3.1. Throughput para los dispositivos de red

- Se mide en paquetes por segundo (pps).
- Para dispositivos de red throughput es la máxima tasa que el dispositivo pueda reenviar paquetes sin descartar alguno.
- Varios dispositivos pueden reenviar paquetes al máximo teórico, lo que se conoce como “wire speed”.

3.4.3.3.2. Throughput para la capa de aplicación

Algunos factores que restringen el throughput en capa de aplicación son:

- Tasas de error de punto a punto
- Funciones de protocolo como handshaking, windows o acknoledgments
- Parámetros de protocolos como tamaño de frame y temporizadores de retransmisión
- Los pps de los dispositivos de interconexión
- Paquetes perdidos en dispositivos de interconexión

Factores de estaciones de trabajo y servidores

- Velocidad de acceso a disco
- Tamaño de la cache del disco
- Performance del controlador de dispositivo
- Performance del bus de computador
- Performance del procesador, memoria
- Ineficiencias del sistema operativo, aplicación o bugs.

3.4.3.4. Precisión

- La meta principal es que la data recibida debe ser igual a la data que envió el origen.
- Las causas típicas del error en data incluyen: subidas de tensión o picos, problemas de mismatch, conexiones físicas pobres, fallas en dispositivos y el ruido causado por la maquinaria.
- Tener en cuenta las colisiones y errores de CRC.

3.4.3.5. Eficiencia

- Este punto especifica cuanto gasto se requiere para enviar tráfico, si el gasto es causado por colisiones, reporte de errores, re-enrutamiento, acknoledgments, cabeceras de frame largas, un mal diseño de red u otros.

- ¿Cuán largo los paquetes pueden ser? Largos más eficientes. Pero muy largos puede significar mucha perdida de data si es que un paquete está dañado.

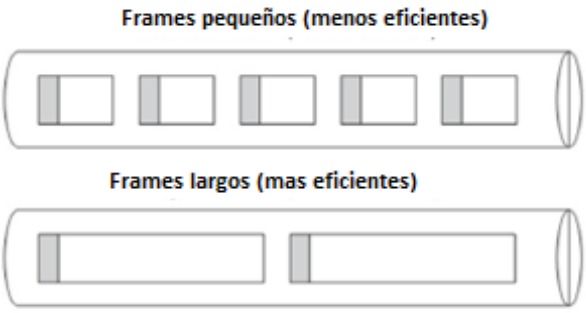

Figura 3.4-2: Utilización de ancho de banda eficiente
Fuente: Elaboración Propia

3.4.3.6. Latencia y variación de latencia

- Los usuarios esperan un retraso mínimo. Así como las aplicaciones de voz y video además de una mínima variación del retraso en el envío de paquetes.
- Las variaciones del retraso o jitter causan interrupciones en comunicaciones de voz y transmisión de video.
- Tener en cuenta que cuando se apliquen mecanismos de seguridad, estos incrementaran o variaran la latencia.

3.4.3.7. Tiempo de respuesta

- En general el umbral de 100 ms es usualmente utilizado como un temporizador para protocolos que ofrecen transporte de data seguro.
- 100 ms es el umbral para tiempo de respuesta para aplicaciones interactivas.

3.4.4. Seguridad

- Es uno de los puntos más importantes en el diseño de red empresarial.
- La primera tarea en el diseño de seguridad es el planeamiento. Esto incluye identificar activos de red, analizar riesgos y desarrollar requerimientos. Todos estos puntos se detallaran más en el punto "3.10 Desarrollar estrategias de seguridad de la red".

3.4.4.1. Identificar activos de la red

- Identificar los activos que deben ser protegidos, su valor y el costo asociado a la pérdida del mismo. Esto incluye hardware, software, aplicaciones y data
- Identificar los activos críticos de la red con los responsables de la organización.

3.4.4.2. Analizar riesgos de seguridad

- Un paso importante en el planeamiento de seguridad es analizar amenazas potenciales y entender su probabilidad y el impacto en la organización.
- Análisis de riesgos y la consecuente construcción de las políticas de seguridad y asegurar el diseño de red es un proceso continuo debido a que los riesgos cambian en severidad, probabilidad con el transcurrir del tiempo.
- Incluir el riesgo del peligro de no tomar ninguna acción de seguridad.
- Además de ver los potenciales atacantes que pueden ser externos y en muchos casos internos.

3.4.4.3. Desarrollar requerimientos de seguridad

Algunos requerimientos generales de seguridad se detallan:

- Confidencialidad de la data, solo usuarios autorizados pueden revisar información sensible.
- Integridad de la data solo usuarios autorizados pueden modificar información sensible.
- Disponibilidad de la data y del sistema, proveer acceso ininterrumpido a la data.

Algunos requerimientos más específicos de seguridad pueden incluir las siguientes metas:

- Autorizar y autenticar oficinas remotas y usuarios móviles.
- Detectar intrusos y aislar el daño que causaron.
- Autenticar actualizaciones de tabla de ruteo.
- Proteger data transmitida a sitios remotos mediante VPN.
- Asegurar físicamente dispositivos de red en cuartos con llave.
- Asegurar lógicamente hosts y dispositivos de red con cuentas de usuario y acceso solo para lo que tienen privilegios.
- Proteger aplicaciones y data de virus.

3.4.5. Capacidad de Administración

En el punto "3.11 Desarrollar Estrategias de Administración de red", inicialmente tener en cuenta los requerimientos de la organización, además los siguientes puntos:

- Administración de fallas: Detectar, aislar y corregir problemas, reportar problemas al usuario final, analizar tópicos acerca de problemas similares.
- Administración de la configuración: Controlar, operar, identificar y recolectar data de dispositivos administrables.

- Administración de la contabilidad: Contabilizar el uso de la red para asignar costos a los usuarios y planificar para cambios en la capacidad y requerimientos.
- Administración del performance: Analizar tráfico y comportamiento de las aplicaciones para optimizar una red que cumpla niveles de servicio contratado "SLA" y planificar una expansión.
- Administración de la seguridad: Monitorear y probar la seguridad y las políticas de protección, manteniendo y distribuyendo passwords y otra información de autenticación y autorización manejando llaves de encriptación y auditando la adherencia de las políticas de seguridad.

3.4.6. Usabilidad

- La facilidad de uso por la cual los usuarios puede acceder a la red y a servicios. Si la administración hace el trabajo del administrador fácil, la usabilidad hace el trabajo del usuario más fácil.
- Tener en claro los requerimientos de la organización en cuanto a usabilidad, debido a que algunos componentes del diseño pueden generar un impacto negativo en la usabilidad por ejemplo políticas de seguridad.

3.4.7. Adaptabilidad

- Un buen diseño de red puede adaptarse a nuevas tecnologías y cambios.
- Cuando se diseñe la red, se tiene que evitar incorporar a la red elementos que pueden hacer difícil el trabajo de implementar nuevas tecnologías en el futuro.
- Un diseño flexible puede adaptarse a cambio de patrones de tráfico y requerimientos de calidad de servicio.

3.4.8. Asequibilidad

- Todo depende de lo que se realizó en el punto 3.1 donde se revisó las metas de negocio. Es común que los enlaces a la WAN son los más costosos en redes amplias, para lo que se tiene consolidad enlaces, minimizar tráfico hacia la WAN, utilizar compresión, eliminar enlaces no utilizados.

- En general para reducir costos operacionales tener en cuenta lo siguiente:

    - Seleccionar dispositivos de red que sean fáciles de configurar, operar, mantener y administrar.
    - Seleccionar el diseño de red que sea fácil de entender y de solucionar problemas.
    - Desarrollar una buena documentación de red que ayude a reducir el tiempo de solución de problemas.
    - Seleccionar aplicaciones de red y protocolos que sean fáciles de usar de tal manera que los usuarios puedan darse auto ayuda en algún momento.

3.4.9. Hacer compensaciones en el diseño de red

- Para cumplir altos requerimientos de disponibilidad, componentes de redundancia son necesarios lo cual genera costo a la implementación, para cumplir requerimientos de performance circuitos y equipos son necesarios, para reforzar políticas de seguridad, alto monitoreo debe ser proveído y los usuarios deben abstenerse de facilidad de uso, para implementar escalamiento, la disponibilidad puede sufrir debido a que nuevos usuarios y lugares son añadidos, falta de personal calificado puede incurrir en el desuso de algunas características. Entonces el diseño de red que se desarrolle debe tener estas compensaciones en consideración.

- El proceso de diseño de red es usualmente progresivo, esto quiere decir que equipos heredados deben coexistir con los nuevos equipos.
- Un ejemplo de cómo realizar estas compensaciones se detalla:

Escalabilidad	→ 20%
Disponibilidad	→ 30%
Performance	→ 15%
Seguridad	→ 5%
Administración	→ 5%
Usabilidad	→ 5%
Adaptabilidad	→ 5%
Asequibilidad	→ 15%
Total	→ 100% (La sumatoria debe ser hasta 100)

Tabla 3.4-1: Compensaciones del diseño
Fuente: Elaboración Propia

3.4.10. Revisión de metas técnicas

Al final de este punto se tiene que haber realizado los siguientes puntos:

- Haber documentado los planes de expansión de la organización en cuanto a usuarios, sitios, servidores en los próximos 1, 2, 5 años.
- Haber documentado si se planea mover servidores departamentales a un sitio central.
- Haber documentado planes para la implementación de extranet con otras organizaciones.
- Haber documentado la disponibilidad de la red en porcentajes y/o en MTBF y MTTR.
- Haber documentado metas para el promedio máximo de utilización de red.
- Haber documentado metas para el throughput de la red y de los dispositivos de red en pps.

- Haber identificado aplicaciones que requieran un tiempo de respuesta menor a 100ms
- Haber documento los riesgos de seguridad y los requerimientos de seguridad de la organización.
- Haber obtenido información acerca de requerimientos de administración, metas de performance, fallas, configuración, seguridad y contabilización.

Nombre de la aplicación	Tipo de aplicación	Aplicación nueva (Si o No)	Criticidad	Costo de estar fuera de servicio	MTBF Aceptable

Tabla 3.4-2: Identificar aplicaciones y requerimientos técnicos
Fuente: Elaboración Propia

MTBF Aceptable	Throughput Objetivo	Retraso debe ser menos de	Variación del retraso debe ser menos de	Comentarios

Tabla 3.4-3: Identificar disponibilidad y latencia
Fuente: Elaboración Propia

3.5. Identificar la red existente

3.5.1. Identificar la infraestructura de red

- Desarrollar un conjunto de mapas de redes y entender la ubicación las principales ubicaciones de los dispositivos y segmentos de red.
- También documentar los nombres y direcciones de los principales dispositivos y segmentos e identificar algún método o estándar para el direccionamiento y nombramiento.
- Documentar los tipos y longitudes del cableado e investigar las restricciones de arquitectura y del entorno.

3.5.1.1. Desarrollar un mapa de red

- A este punto en el proceso de diseño la meta es obtener el mapa o conjunto de mapas de la red actual, para lo cual se requiere buenas herramientas de dibujo.

3.5.1.1.1. Identificar redes amplias

- Un solo mapa puede no ser suficiente para redes amplias. Para esto se puede desarrollar varios mapas, uno para cada ubicación. Otro método puede ser dibujar mapas de acuerdo al nivel jerárquico.

- Empiece con el mapa o conjunto de mapas que muestren la siguiente información:
  - Información geográfica, como país, provincia, ciudad, campus.
  - Conexiones WAN entre las ubicaciones.
  - Conexiones WAN o LAN entre edificios o campus.

- Para cada red, puede dibujar mapas que muestres información más detallada como:
    - Edificios o pisos y posiblemente cuartos o cubículos
    - La ubicación de los principales servidores o granja de servidores
    - La ubicación de routers o switches.
    - La ubicación de firewalls, dispositivos NAT, IDS e IPS.
    - Ubicación de mainframes
    - Ubicación de las principales estaciones de administración de red.
    - Ubicación y alcance de LANs y VLANs.
    - Alguna indicación de donde residen las estaciones de trabajo.

- Luego localice los servicios de red como servidores RADIUS, TACACS, DHCP, DNS, SNMP, VPN.
- El mapa de dispositivos de capa 3 y su topología.
- El conjunto de mapas que muestren información detallada acerca de enlaces de capa 2 y dispositivos son útiles, este mapa muestra dispositivos LAN conectadas a LAN o WAN, entre otros debe incluir la siguiente información:
    - Nombre de proveedores WAN
    - ID del circuito WAN
    - La ubicación y alto nivel de configuración de switches LAN.
    - La ubicación y alance de VLANs
    - La ubicación y alto nivel de configuración de trunks entre switches LAN
    - La ubicación y alto nivel de configuración de firewalls de capa 2.

3.5.1.1.2. Identificar la arquitectura lógica

- Mientras documente la infraestructura de red, revise los diagramas y trate de identificar la topología lógica de la red y los componentes físicos.
- Identifique bombas de tiempo, como dominios STP largos, problemas de enrutamiento.
- En el punto "3.5 Diseñar la topología de red" se detallara más fondo este tema.

3.5.1.1.3. Desarrollar un diagrama de bloques modular

- Además de desarrollar un conjunto es útil dibujar un diagrama de red en bloques para identificar las partes de la red.

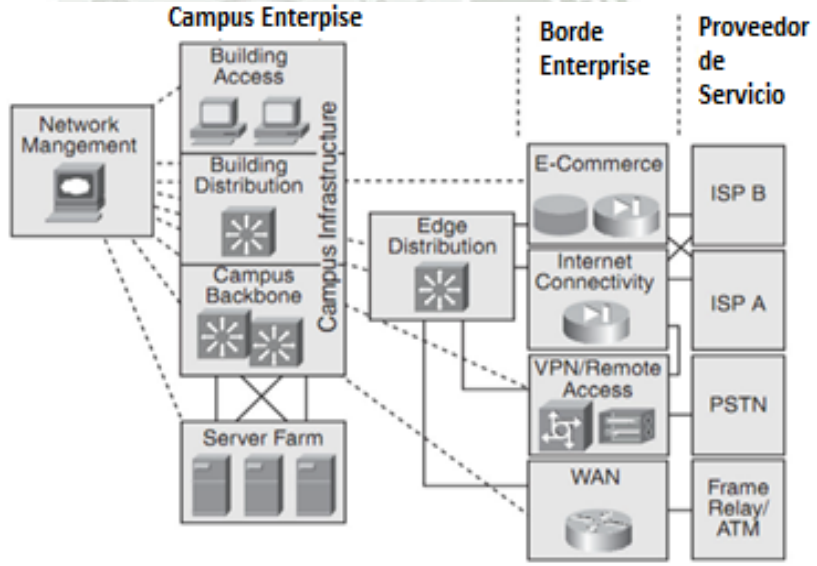

Figura 3.5-1: Topología de red modular
Fuente: [POP2011]

3.5.1.2. Identificar direccionamiento de red y nombramiento

- En los dibujos de red que realice identificar los nombres de los sitios principales, routers, switches, segmentos de red y servidores.
- Identificar las máscaras de red, resumen de rutas, subredes.
- En la Parte II de la metodología se describe este tema con mayor detalle.

3.5.1.3. Identificar el medio y cableado

- Es importante para cumplir las metas de disponibilidad y escalabilidad. La identificación del cableado actual es importante para identificar problemas potenciales.
- Identificar que el cableado este etiquetado. Incluir información de distancia entre edificios, tipo de medio cableado o inalámbrico, tipo de cableado utp, stp y su categoría.
- En los edificios localizar gabinetes y ductos de cableado, laboratorios además del cableado vertical, horizontal y de área de trabajo.
- Solicitar a la organización certificaciones de cableado en los enlaces principales de cobre o de fibra óptica.

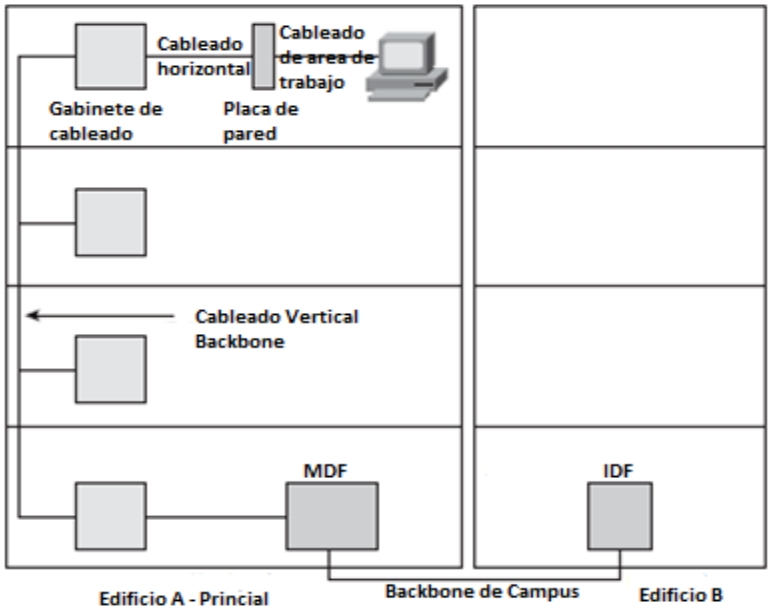

Figura 3.5-2: Cableado de red de campus
Fuente: Elaboración Propia

Nombre del edificio						
Ubicación de los gabinetes de						
Ubicación de cuartos y demarcación de redes externas						
Topología de cableado lógica						
Cableado vertical						
	Coaxial	Fibra	STP	Categoría 3 UTP	Categoría 5,6 UTP	Otro
Conexión vertical 1						
Conexión vertical 2						
Conexión vertical n						
Cableado Horizontal						
	Coaxial	Fibra	STP	Categoría 3 UTP	Categoría 5,6 UTP	Otro
Piso 1						
Piso 2						
Piso 3						
Piso n						
Cableado de Área de Trabajo						
	Coaxial	Fibra	STP	Categoría 3 UTP	Categoría 5,6 UTP	Otro
Piso 1						
Piso 2						
Piso 3						
Piso n						

Tabla 3.5-1: Cableado de edificio
Fuente: Elaboración Propia

3.5.1.4. Revisar restricciones de arquitectura y del entorno

- Asegúrese de que los siguientes elementos de arquitectura sean suficientes para soportar su diseño:
  - Aire Acondicionado
  - Calor
  - Ventilación
  - Energía
  - Protección de interferencia electromagnética
  - Puertas en buen estado.

- Asegúrese de que exista espacio para:
  - Vías de cableado
  - Patch Panel
  - Equipamiento de rack
  - Área de trabajo para técnicos en labores de instalación y troubleshooting

3.5.2. Revisar la salud de la red actual

- Tener en cuenta los resultados obtenidos del punto "3.2 Analizar metas técnicas y compensaciones" ya que el performance de los segmentos de red actuales afectaran afectan al performance total, se necesita estudiar el performance actual para cumplir con las metas del performance de la red completa.
- Al analizar la red actual se va reconocer que sistemas se heredaran y tienen que ser considerados en el nuevo diseño.

3.5.2.1. Desarrollar una base de línea de la red actual

- Se tiene que emplear bastante tiempo y seleccionar adecuadamente cuando realizar el análisis. Además el análisis no

debe incluir problemas atípicos ocasionados por carga de tráfico excepcional.

- En general, los errores, paquetes y latencia se incrementa con la carga de red. Para obtener la medición de típico retraso, precisión realice sus mediciones en periodos de tráfico normal.

3.5.2.2. Analizar la disponibilidad de la red

- Converse con los ingenieros de red y técnicos acerca de la raíz de los más recientes periodos de caída de red.
- Realice cuadros de MTTR y MTBF para validar los análisis.

	MTBF	MTTR	Fecha y duración de la última caída	Causa de la última caída mayor	Reparación para la última caída mayor
Enterprise					
Segmento 1					
Segmento 2					
Segmento 3					
Segmento n					

Tabla 3.5-2: Identificar disponibilidad de la red actual
Fuente: Elaboración Propia

3.5.2.3. Analizar la utilización de la red

- Medida de la cantidad de ancho de banda que se utiliza durante un periodo especifico de tiempo, especificada como un porcentaje de la capacidad.
- En general se debe guardar los datos de utilización de la red con suficiente granularidad en tiempo para analizar picos de tráfico y de esta manera realizar requerimientos de capacidad de dispositivos y segmentos.

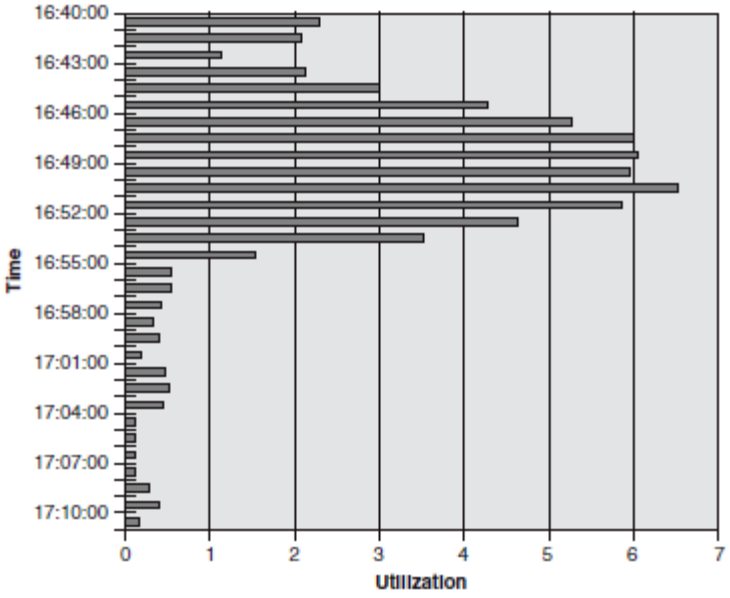

Figura 3.5-3: Utilización de la red en intervalo de minutos
Fuente: [POP2011]

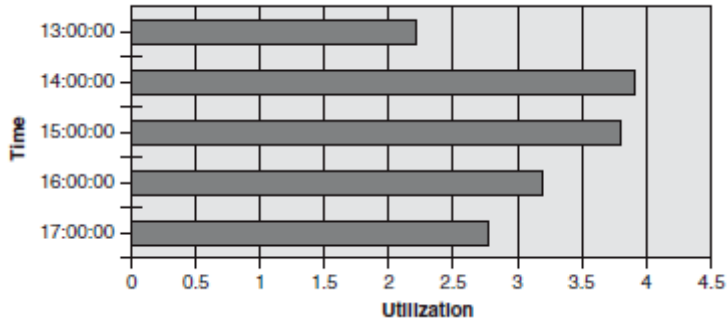

Figura 3.5-4: Utilización de la red en intervalo de horas
Fuente: [POP2011]

3.5.2.4. Analizar la precisión de la red

- Tener en cuenta los valores de "BER bit-error-rate", CRC con testeadores y analizadores de protocolo.
- La precisión también mide la perdida de paquetes, se puede medir perdida de paquetes mientras se mide el tiempo de respuesta.

3.5.2.5. Analizar la eficiencia de la red

- El incremento del tamaño de frame y window de recepción en clientes y servidores puede resultar en una mejorada eficiencia.
- El incremento del MTU es necesario en algunas interfaces de routers que usan túneles.
- Para determinar resultados verdaderos se requiere analizar el tamaño del frame con un analizador de protocolos.
- El análisis del tamaño de frames también puede ayudar a entender la salud de la red, un excesivo número de frames menores a 64 bytes puede indicar muchas colisiones en un segmento Ethernet compartido.

3.5.2.6. Analizar el retraso y tiempo de respuesta

- Para cumplir con requerimientos de diseño se necesita medir el tiempo de respuesta entre dispositivos significativos de la red antes y después de que la red este implementada. Para esto se puede utilizar un analizador de protocolos o con el envío de paquetes ping y medir el tiempo de ida y vuelta “RTT round-trip time”.
- También medir el tiempo de respuesta desde el punto de vista del usuario con las aplicaciones comunes que realice.
- Adicionalmente medir el tiempo que una estación de trabajo toma para arrancar, algunas sistemas operativos demoran un largo tiempo debido a la cantidad de tráfico que envían y reciben mientras arrancan, esto antes y después de la implementación.

	Node A	Node B	Node C	Node D
Node A	X			
Node B		X		
Node C			X	
Node D				X

Tabla 3.5-3: Medidas del tiempo de respuesta
Fuente: Fuente: [POP2011]

3.5.2.7. Revisar el estado de los dispositivos principales entre switches, routers y firewalls

- Revisión buffer
- Revisión entorno
- Revisión interfaces
- Revisión memoria
- Revisión de procesos
- Revisión de actual configuración
- Revisión de versión

3.5.3. Lista de revisión de la salud de la red

- La topología de red física y lógica deben estar bien documentadas.
- Las direcciones de red y nombres deben estar asignados de una manera estructurada y bien documentada
- El cableado de red debe estar testeado y certificado.
- El cableado de red entre closet de comunicación y estación de trabajo finales no deben superar los 100 metros.
- La disponibilidad de la red debe satisfacer las metas del cliente.
- La seguridad de la red debe satisfacer las metas del cliente.
- Ningún segmento de LAN o WAN deben estar saturadas.
- El tamaño de los frames deben ser optimizados para que sean lo más largo posible para la capa 2.

- Trafico de broadcast debe ser menos del 20% de todo el tráfico de cada segmento de red.
- El tamaño de los frames debe ser optimizados para que se lo mas largo posible en capa 2.
- Ningún Router debe ser sobreutilizado.
- En promedio, routers no deben descartar más del 1% de paquetes.
- Actualizar routers, switches y demás dispositivos las configuraciones deben ser recolectadas, archivadas y analizadas como parte del diseño de estudio.
- El tiempo de respuesta entre clientes y host debe ser menos de 100ms.

3.6. Identificar el tráfico de red

3.6.1. Identificar el flujo de trafico

- Incluye identificar orígenes y destinos del tráfico de red analizando la dirección y simetría de la data que viaja entre el origen y destino.

3.6.1.1. Identificar los principales fuentes de tráfico y data-stores

- Primero se debe identificar las comunidades de usuario y data-stores.
- Las comunidades de usuario es el conjunto de trabajadores que utilizan el mismo conjunto de aplicaciones.

Nombre de la Comunidad de usuario	Tamaño de la Comunidad	Ubicaciones de la Comunidad	Aplicaciones utilizadas por la Comunidad

Tabla 3.6-1: Comunidades de usuario
Fuente: Elaboración Propia

- Los data-stores es el área donde las aplicaciones residen. Pueden ser servidores, SAN, mainframe, backup, librerías de video, o cualquier dispositivo que contenga cantidades amplias de data almacenada.

Data Store	Ubicación	Aplicaciones	Utilizadas x Comunidad(es) de Usuario(s)

Tabla 3.6-2: Data-Stores
Fuente: Elaboración Propia

3.6.1.2. Documentar el flujo de tráfico en la red actual

- Documentar el flujo de tráfico incluye identificar flujos de tráfico individuales entre origen y stores, esto contiene dirección, simetría, vía de ruteo, numero de paquetes, numero de bytes, direcciones cada final de flujo.

- Medir el comportamiento de trafico puede ayudar al diseñador de la red para realizar lo siguiente:

  - Identificar el comportamiento de las redes existentes.
  - Planes para el desarrollo y expansión de la red.
  - Cuantificar el performance de red.
  - Verificar la calidad de los servicios de red.
  - Atribuir el uso de red a usuarios y aplicaciones.

- El método más simple es medir los MBps entre las entidades de la conexión.

	Destino 1		Destino 2		Destino 3		Destino n	
	MBps	Path	MBps	Path	MBps	Path	MBps	Path
Origen 1								
Origen 2								
Origen 3								
Origen n								

Tabla 3.6-3: Flujo de tráfico
Fuente: Elaboración Propia

3.6.1.3. Identificar los tipos de flujo de tráfico para nuevas aplicaciones de red

- Terminal/host: el tráfico es usualmente asimétrico. La terminal envía pocos paquetes y el host envía varios paquetes “Telnet”.

- Cliente/Servidor: El flujo es bidireccional y asimétrico. FTP y HTTP son protocolos cliente/servidor y son probablemente los protocolos más usados de este tipo.
- Cliente Thin: Un caso especial de la arquitectura cliente/servidor. La mayor parte de la carga se realiza en el servidor. Las aplicaciones de usuario se originan y ejecutan en el servidor central.
- Peer to Peer: El flujo es usualmente bidireccional y simétrico. Cada host actúa como cliente y servidor. “Torrents”.
- Servidor/Servidor: El tráfico incluye transmisión entre servidores y transmisión entre servidores y aplicaciones de administración. El flujo por lo general es bidireccional.
- Cómputo Distribuido: Se refiere a las aplicaciones que requieren múltiples nodos de cómputo que trabajan juntos para completar una tarea.
- Voz sobre IP: trabaja con dos tipos de tráfico. El flujo para transmitir la voz digital es peer-to-peer es separado del flujo asociado con establecimiento de llamada con la terminación de llamada.

3.6.1.4. Documentar el flujo de tráfico para aplicaciones existentes y nuevas de red

- Para identificar el flujo de tráfico para aplicaciones nuevas y existentes de la red, identifique el tipo de flujo por cada aplicación, comunidad de usuario y data-stores que está asociada.

Nombre de la Aplicación	Tipo de flujo de tráfico	Protocolos usados por la aplicación	Comunidades de usuarios que utilizan la aplicación	Data Stores (Servidores, Host, entre otros)	Requerimiento de ancho de banda aproximado para la aplicación	Requerimientos de QoS

Tabla 3.6-4: Identificación de tráfico en aplicaciones de red
Fuente: Elaboración Propia

3.6.2. Identificar la carga de trafico

- Es importante identificar el flujo y la carga de tráfico.
- La meta es identificar evitar un diseño que tenga algún cuello de botella. Para esto se puede investigar patrones de uso por aplicación, tiempos ociosos entre paquetes y sesiones, tamaño de frames.
- Otro enfoque para evitar cuellos de botella es simplemente lanzar largas cantidades de ancho de banda, sobre-provisionar. Actualmente el ancho de banda en LAN es más barato, se puede utilizar desde Fast Ethernet o mejor, en todas las estaciones de trabajo y switches. En WAN es caro aun.
- Si usted reconoce que el ancho de banda no será una restricción en su diseño entonces puede obviar este punto.

3.6.3. Identificar el comportamiento del trafico

3.6.3.1. Comportamiento broadcast

- Tener en cuanto que algunos dispositivos envían broadcast entre ellos para descubrirse unos a otros, el reenvío de estos puede resultar en un problema de escalabilidad para redes amplias planas con solo switches o bridges.
- Routers no reenvían broadcast y multicast, otro punto para reducir broadcast es implementando VLANs.

- Muchos frames broadcast pueden abrumar estaciones, switches y routers.

3.6.3.2. Eficiencia de red

- Tamaño del frame
- Control de flujo y windowing
- Mecanismos de recuperación de errores

3.6.4. Identificar requerimientos de calidad de servicio

- Solo saber los requerimientos de carga (ancho de banda) de aplicaciones no es suficiente, además debe saber si es el requerimiento es flexible o no, algunas aplicaciones pueden funcionar cuando el ancho de banda no es suficiente, otras aplicaciones como voz y video no son flexibles si el ancho de banda no es el adecuado.

- La IETF dispone las siguientes especificaciones para los servicios integrados de grupo de trabajo “Integrated Service working group”:
  - Carga de servicio controlada: Provee flujo de la data de cliente con QoS casi aproximada que el mismo flujo que en una red no cargada.
  - Servicio Garantizado: Provee límites de retraso en comunicaciones de extremo a extremo.

- La IETF dispone las siguientes especificaciones para los servicios diferenciados de grupo de trabajo “Integrated Service working group” - RFC 2475:
  - Los paquetes IP pueden ser marcados con servicios diferenciados de punto de código “differenciated services codepoint” DSCP para influenciar en las decisiones de las colas y descarte de paquetes para datagramas IP en interfaces de salida de routers o switches.

3.6.5. Lista de revisión de tráfico de red

- Haber identificado la mayoría de los orígenes de tráfico y almacenamiento de estos y documentar el flujo de tráfico entre estos.
- Haber categorizado el flujo de tráfico para cada aplicación como un terminal/host, cliente/servidor, peer-to-peer, server/server o computo distribuido.
- Haber estimado el ancho de banda de cada aplicación.
- Haber estimado los requerimientos de ancho de banda para protocolos de enrutamiento.
- Haber identificado el tráfico de red en términos de ratios de broadcast/multicast, tamaño de frames, windowing y control de flujo y mecanismos de recuperación de errores.
- Haber categorizado los requerimientos de QoS de cada aplicación.
- Haber analizado los retos asociados con la implementación de QoS punto a punto y la necesidad de los dispositivos en toda la red.

DISEÑO DE RED LÓGICO

3.7. Diseñar la topología de red

3.7.1. Diseño de red jerárquico

- El modelo ayuda al desarrollo de la topología en capas discretas, cada una de estas se enfoca en funciones específicas, permitiéndole elegir los sistemas y características para cada capa.
- La topología jerárquica típica comprende: core, distribución y acceso.

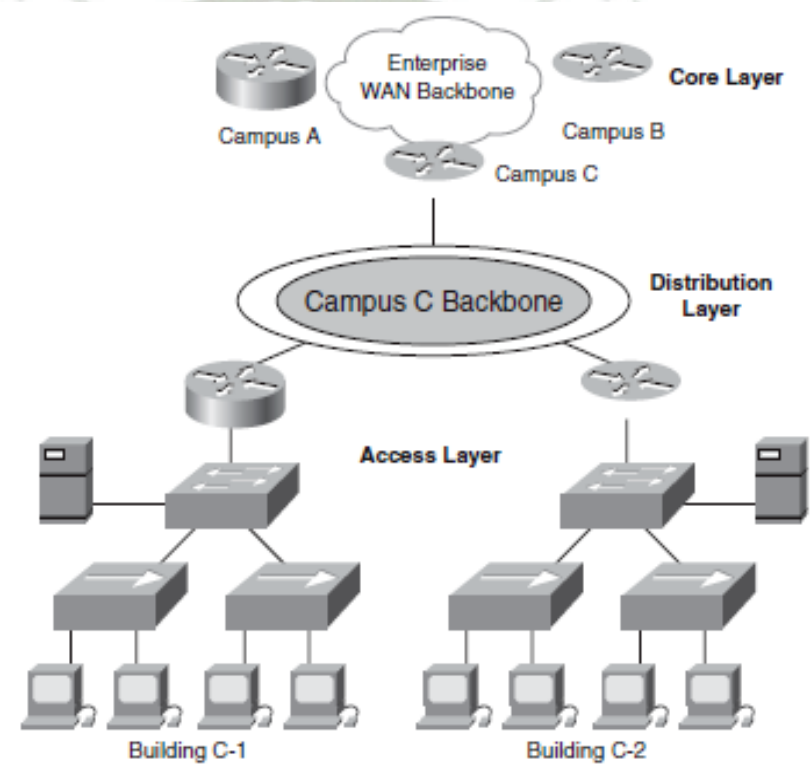

Figura 3.7-1: Topología Jerárquica
Fuente: [POP2011]

3.7.1.1. ¿Por qué utilizar el diseño de red jerárquico?

- Minimizar costos, saber cuál es el equipo apropiado para cada capa, además del planeamiento de capacidad por cada capa.

- La modularidad del diseño habilita la facilidad de entendimiento, esto minimiza la capacitación exhaustiva del personal, las pruebas son más sencillas, y el aislamiento de problemas ese reduce. Además facilita el cambio ya que es más sencillo crecer o hacer mejoraras.

3.7.1.2. Modelo jerárquico de tres capas

- **Capa de Core:**
  - La capa de núcleo de switches y routers de altas prestaciones las cuales son optimizadas para la disponibilidad y velocidad.
  - La función de esta capa es proveer el transporte de data de manera rápida y eficiente:
    - Altas velocidades de backbone con servicios de transportes de servicio rápido.
    - Provee redundancia y tolerancia a fallos.
    - Ofrece buena administración.
    - Evita la manipulación de paquetes lentos causados por filtros y u otros procesos.
  - Además conecta a la organización con otras por medio de extranet o internet.

- **Capa de distribución**
  - Capa de routers y switches las cuales implementan políticas y segmentan el tráfico.
  - Provee switching multicapa entre las capas de acceso y Core.

- Suma ancho de banda al concentrar varios enlaces lentos en uno solo “linkagregattion”. Además provee conexiones redundantes para el acceso de dispositivos.
- Implementa políticas basadas en decisiones: filtro por origen y destino, filtra por puerto de entrada y salida, esconde números internos de red por filtro de ruteo, ruteo estático, seguridad, calidad de servicio QoS.

- **Capa de acceso**

  - Puede incluir routers, switches, Access points.
  - Por lo general son switches de capa 2 los que van a este nivel en redes de campus.

3.7.1.3. Guía para el diseño de red jerárquico

- Primero tener en claro las tres capas: core, distribución y acceso.
- Controlar el perímetro de la red, esto ayuda a predecir caminos de enrutamiento, flujo de tráfico y requerimientos de capacidad.
- Evitar conectar dispositivos como otro switch debajo de la capa de acceso o cadenas.
- Evitar puertas traseras que es un dispositivo adicional como switches o routers conectadas a dos redes.
- Finalmente, se debe empezar el diseño desde la capa de acceso luego la capa de distribución y finalmente la capa de core. De esta manera se puede tener precisión en el planeamiento de la capacidad, además de las técnicas de optimización en las capas de distribución y core.

3.7.2. Topologías de diseño de red redundantes

- Permite cumplir requerimientos para la disponibilidad de la red duplicando elementos en la red.
- El objetivo es duplicar cualquier componente que su posible falla cause caída de aplicaciones críticas. El componente puede ser un equipo de Core, un switch, un enlace entre dos switches, una fuente de poder, entre otros.
- Si se va implementar redundancia tener en cuenta el costo, y el manejo de la topología y protocolos que la manejen con extremo cuidado.

- Rutas de Acceso "Path" de Backup
    - Considerar dos aspectos del ruta de acceso de backup
        - Cuanta capacidad soportara
        - Tiempo que tomara la red para usar este backup
        - Es normal que el backup tenga menos capacidad que el acceso primario debido a tecnología diferente, costo elevado.
    - Automático vs Manual
        - Manual: la reconexión y reconfiguración de usuarios mostrara el corte lo cual no es aceptable para aplicaciones de misión crítica.
        - Debe ser probado antes de ponerse en línea.
    - Algunas veces usado para el balanceo de carga además de backup.

- Balanceo de Carga
    - El primer objetivo de la redundancia es cumplir con la disponibilidad.
    - El segundo objetivo es mejorar el performance con el balanceo de carga a través de enlaces paralelos.
    - Debe ser planificado.

3.7.3. Diseño de red Modular

- Los conceptos de jerarquía y redundancia son importantes para este diseño.
- Un concepto fundamental de jerarquía es la modularidad.
- Las redes amplias en general consisten en general de diferentes áreas o módulos, cada una de estas deben ser diseñados con simetría y diseño de arriba abajo, aplicando jerarquía y redundancia donde sea necesario.
- El modelado modular los siguiente:
    - Core
    - Data Center
    - Campus
    - Administración
    - Borde WAN
    - Borde Internet
    - Ramas
    - Extranet
    - Sitios de partner

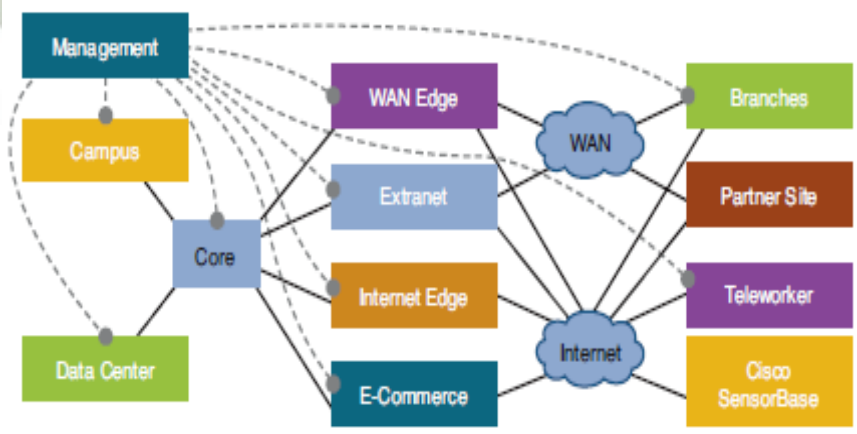

Figura 3.7-2: Diseño Modular
Fuente: [POP2011]

3.7.4. Diseño de red de campus

- Utilizar en modelo jerárquico o modular.
- Tener claro en cuenta las tres capas: Core, distribución y acceso.
- Minimizar el conjunto de equipos que compartan un mismo enlace y el mismo ancho de banda.
- Minimizar el tamaño de dominios de broadcast.
- Debe cumplir los requisitos de disponibilidad, performance, mantenibilidad y escalabilidad.
- Tener en cuenta los protocolos :
    - Capa 2:
        - STP, RSTP, MSTP
        - VLAN, IEEE802.1q
- Si se va incluir redes inalámbricas WLAN
    - Por lo general se implementan como otra VLAN.
    - Facilitar el roaming.
    - Proteger la red cableada de la inalámbrica.
- Proveer redundancia
    - Redundancia y balanceo de carga entre VLANs cableadas
    - Redundancia a nivel de servidores.
    - Redundancia de estación de trabajo hacia router con múltiples gateways.

3.7.5. Diseño de borde de red Enterprise

3.7.5.1. Segmentos WAN redundantes

- Los enlaces WAN son críticos, los enlaces de backup redundante son incluidos en la red Enterprise
- Topologías Full-Mesh proveen redundancia completa

- Full-Mesh es costosa de implementar, mantener, actualizar y de solucionar errores

3.7.5.2. Multihoming de conexiones a internet

- El significado genérico de multihoming es “proveer más de una conexión al sistema para acceder y ofrecer servicios de red”.

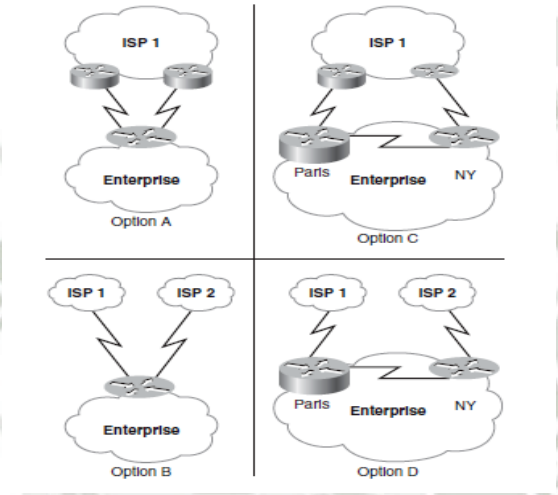

Figura 3.7-3: Opciones de conexión a internet
Fuente: [POP2011]

3.7.5.3. VPN

- Permite al usuario conectarse a la red interna utilizando la red pública convencional empleando mecanismos de seguridad tales como: SSL, IP-Sec, entre otras.
- También puede ser utilizada para conectar la intranet Enterprise a para que llegue a una extranet fuera de la organización.
- Provee la habilidad de conectar geográficamente oficinas dispersadas a través del proveedor de servicio.

3.7.6. Diseño de topologías de red segura

3.7.6.1. Plan para la seguridad física

- Instalar equipamiento donde personas ajenas a la red tengan acceso físico.
- La seguridad física no tiene que ver directamente con la topología lógica, pero si la seguridad física es expuesta la topología lógica puede tener impacto.

3.7.6.2. Cumplir requerimientos de seguridad mediante topologías de firewall

- Un firewall es un sistema o la combinación de sistemas que refuerza los límites entre dos o más redes.
- Los firewalls son importantes en los límites de la red Enterprise y el internet.
- El firewall debe ser puesto en la topología de red entonces todo el tráfico que provenga desde el exterior debe pasar por este.
- Para la publicación de servicios como Web, FTP, SMTP se debe contar con una zona espacial llamada DMZ “Demilitarized zone”, todos los servicios publicados se albergan allí.

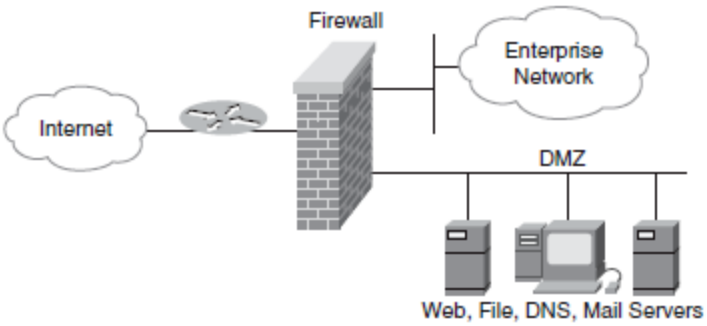

Figura 3.7-4: Topología DMZ
Fuente: [POP2011]

3.7.7. ¿Cómo saber si es un buen diseño?

- Cuando ya se sabe cómo añadir un nuevo edificio, piso, enlace WAN, sitio remoto.
- Cuando nuevas adiciones solo causan cambio para los dispositivos directamente conectados.
- Cuando su red se puede crecer en el doble o triple en tamaño sin mayores cambios.
- Cuando la solución de problemas es sencilla debido que no existen interacciones de protocolos complejos.

3.8. Diseñar modelos para direccionamiento y numeramiento

3.8.1. Guía de diseño para la asignación de direcciones de capa 3

Tener en cuenta lo siguiente:

- Diseñar el modelo estructurado antes de asignar direcciones.
- Dejar espacio si se planea crecer.
- Asignar bloques de direcciones en estilo jerárquico para fomentar escalamiento y ser disponibilidad.
- Asignar bloques de direcciones basadas en la red física pero no en membresía para evitar problemas cuando haya movimiento de usuarios.
- Si el nivel de experiencia de administración de las redes en sucursales es alto se puede delegar autoridad para nombramiento y direccionamiento.
- Para maximizar flexibilidad utilice direccionamiento dinámico.
- Para maximizar seguridad y adaptabilidad utilice direcciones privadas con NAT en entornos IP.

3.8.1.1. Utilizar un modelo estructurado para el direccionamiento

- El modelo estructurado para direccionamiento significa que las direcciones son significativas, jerárquicas y planificadas. Las direcciones que incluyan parte prefijo y host son estructuradas.
- Facilita la administración y solución de errores, hace más fácil leer mapas de red, operar software de administración de red, reconocer dispositivos en un analizador de protocolos.
- Además facilita la optimización de la red y seguridad porque hace la implementación de filtros más sencillos en firewalls, switches, routers.

3.8.1.2. Administración de direccionamiento por una Autoridad Central

- Identificar números de red para Core y bloques de subredes para las capas de distribución y de acceso.
- Tener en cuenta el direccionamiento público y privado.
- En el proceso se deben responder las siguientes preguntas:

  - ¿Se requerirán direcciones públicas, privadas o ambas?
  - ¿Cuántos sistemas finales necesitan acceder a la red privada?, ¿Cuántos sistemas finales necesitan ser visibles para la red pública?
  - ¿Cómo ocurrirá la transición entre direcciones privadas y públicas?
  - ¿Dónde existirán los límites entre direcciones privadas y públicas?

3.8.1.3. Direccionamiento estático y dinámico

- El direccionamiento dinámico evita la complejidad de la red y la hace más flexible.
- El direccionamiento estático son utilizadas por lo general para servidores, servicios de borde a internet y para dispositivos administrados.
- Muchas redes utilizan combinaciones de direccionamiento estático y dinámico.
- Algunos aspectos que se deben tomar en cuenta antes de elegir el tipo de direccionamiento.

  - Número de estaciones finales: en entornos extensos es más sencillo utilizar direccionamiento dinámico.

- Renombramiento: en entornos dinámicos es más sencillo. En direcciones públicas si se cambia de ISP se tendría que hacer el renombramiento.
- Alta disponibilidad: las direcciones estáticas están disponibles siempre porque no requieren de un servidor que les asigne una dirección.
- Seguridad: las direcciones estáticas son más seguras debido a que un sistema final antes tiene que ser configurado para tener acceso a la red.
- Seguimiento: en direcciones estáticas es más sencillo hacer este proceso.

3.8.1.4. Utilice direccionamiento privado en entornos IP

- En entornos locales el administrador asigna direcciones.
- En entornos de direcciones públicas el ISP asigna direcciones públicas.
- El direccionamiento privado no se publica directamente hacia internet.
- En caso de cambio de ISP, no afecta directamente a las direcciones privadas solo a las públicas.

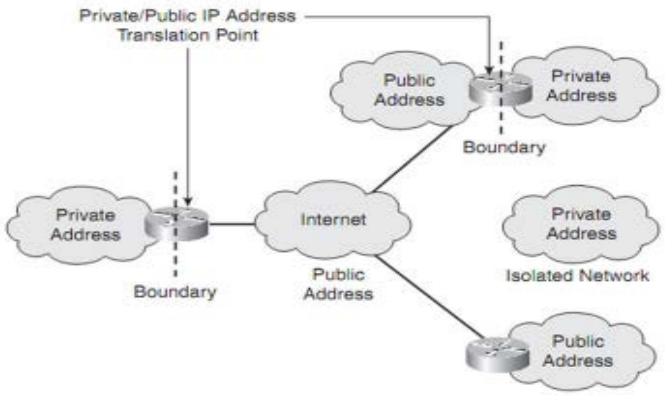

Figura 3.8-1: Direccionamiento privado
Fuente: [POP2011]

- **Traducción de direcciones de red "NAT"**

  - Es el mecanismo IP el cual es utilizado para la conversión de direcciones de la red interna hacia la externa y viceversa.
  - El administrador de NAT configura un pool de direcciones externas o públicas que se pueden ser usadas para la traducción.
  - Algunos productos ofrecen la traducción de traducción de puertos PAT o NAT overload.

3.8.2. Utilizar el modelo jerárquico para el asignar direcciones

- El modelo jerárquico es que aplica estructura a las direcciones, los números en la parte izquierda se refiere a bloques largos de redes o nodos y los números en la parte derecha se refiere a redes individuales o nodos.

- Tiene las siguientes ventajas:
  - Soporte para fácil manejo de errores, actualizaciones y administración.
  - Performance optimizado.
  - Convergencia de ruteo rápido.
  - Escalabilidad
  - Estabilidad
  - Pocos recursos necesitados (CPU, memoria, buffer, ancho de banda)

- Tener los conceptos claros y precisos de:
  - Ruteo con clase
  - Ruteo sin clase
  - Resumen de rutas
  - Redes discontiguas
  - Mascaras de subred de longitud variable – "VLSM"

3.8.3. Diseñar el modelo para el nombramiento

- Los nombres juegan un rol esencial en los objetivos de la red.
- Considerar las siguientes pautas:
  - ¿Qué tipos de entidades necesitaran nombres? Servidores, routers, impresoras.
  - ¿Los sistemas finales necesitan nombres?
  - ¿Cuál es la estructura de nombres? ¿Qué parte identifica al tipo de dispositivo?
  - ¿Quién asigna los nombres?
  - ¿Si las direcciones son dinámicas, entonces los nombres serán dinámicos?
  - ¿Cómo el nombre seleccionado afectara el tráfico de red y/o seguridad?

3.8.3.1. Pasos para asignar nombres

- Para maximizar la usabilidad los nombres deben ser:
  - Cortos
  - Significantes
  - No ambiguos
  - Distintos
  - No discriminativos en mayúsculas y minúsculas
  - No incluir espacios

- Una buena práctica es añadir caracteres para identificar al dispositivo.
- Los nombres pueden contener un código de ubicación.
- Evitar nombres con caracteres no usuales.

  - Guiones, sub-guion, asteriscos, símbolos, asteriscos entre otros.

- Los nombres deben ser de nueve a ocho o menos caracteres.
- Si algún dispositivo tiene más de una interfaz o dirección solo se debe asignar un solo nombre.
- Tener en cuenta de dispositivos clave asignar nombre complejos, en otras palabras se debe compensar el nombre entre usabilidad y seguridad.

3.8.3.2. Asignar nombres en un entorno IP

- Asignar nombres en un entorno IP es logrado mediante la configuración de host, servidores DNS o NIS.
- DNS es muy utilizado en el internet y muy recomendado para la administración de redes empresariales.

3.8.3.2.1. Servidor DNS

- DNS es una base de datos distribuida que provee un sistema de asignación de nombres jerárquicos.
- Tiene dos partes:
  - Nombre de host.
  - Nombre de dominio
- La arquitectura DNS distribuye el conocimiento de nombres por eso ningún sistema DNS solo necesita saber todos los nombres.
- DNS utiliza el modelo cliente/servidor.
- El software que resuelve la petición en la máquina del cliente envía una consulta al DNS Server y si el servidor DNS encuentra la petición envía la dirección IP asignada a este nombre.

3.9. Seleccionar Protocolos de Switching y Routing

3.9.1. Tomar decisiones como parte del diseño

- Los objetivos deben ser establecidos.
- Se deben explorar varias opciones.
- Las consecuencias de las decisiones deben ser investigadas.
- Planes de contingencia deben ser realizados.

3.9.2. Seleccionar protocolos de switching

Antes de seleccionar los protocolos tomar en cuenta lo siguiente:

- Tabla de dirección MAC
- Describir las ventajas de switch redundantes.
- Describir los problemas asociados con tormentas de broadcast, transmisiones de múltiple frames e inestabilidad de Tabla de dirección MAC.
- Describir cómo evitar la presencia de bucles y como resolver problemas de topología con switch redundante.
- Explicar cómo implementar STP u otros protocoles como EAPS para la resolución de problemas asociados a topologías de switches redundantes.

3.9.2.1. Puenteo Transparente (Bridging)

- Tener en cuenta lo siguiente:
  - Reenviar frames de manera transparente
  - Aprender que puerto es utilizado por cada MAC
  - Inundar cuando la dirección de destino no ha sido aprendido.
  - Filtrar frames de puertos de salida que no incluyen direcciones de destino.
  - Inundar broadcast y multicast.

3.9.2.2. Spanning Tree

- Provee una red redundante libre de bucle.

3.9.2.3. Prevención de bucles

- Varios vendors ofrecen protocolos propietarios para la prevención de bucles.
- El objetivo de estos protocolos es proveer protección adicional en contra de bucles causados por bloqueo de puertos de manera errónea.

3.9.2.4. Protocolos de transporte de VLAN

- Cuando las VLAN son implementadas en la red, los switches deben tener algún método para que la comunicación y tráfico entre-VLANs se realice por las interfaces correctas.

3.9.2.4.1. IEEE 802.1Q

- Es el estándar para etiquetar frames con ID de la VLAN.
- La etiqueta de VLAN es agregado en el frame Ethernet.

3.9.3. Seleccionar protocolos de routing

A tener en cuenta:

- Describir las ventajas de operación de ruteo estático.
- Describir las ventajas de operación de protocolos de ruteo dinámico, incluyendo RIP, IGRP, EIGRP y OSPF.
- Entender las diferencias entre ruteo estático y ruteo dinámico.
- Identificar las clases de los protocolos de ruteo.

3.9.3.1. Identificar los protocolos de ruteo

3.9.3.1.1. Protocolos de vector-distancia

- Los protocolos de vector-distancia:
  - RIP 1, 2
  - Interior Gateway Routing Protocol – IGRP
  - Enhaced IGRP – EIGRP
  - Border Gateway Protocol – BGP

3.9.3.1.2. Protocolos de estado de enlace

- Los protocolos de estado de enlace son:
  - OSPF
  - IS-IS

3.9.3.1.3. Elegir entre protocolos entre vector-distancia y estado de enlace

- Elegir protocolos de vector-distancia cuando:
  - La red utiliza una topología simple y plana y no requiere un diseño jerárquico.
  - La red utiliza un topología simple hub-and-spoke.
  - Los administradores no tienen mucho conocimiento de cómo operar y corregir errores con protocolos de estado de enlace.
  - En el peor de los casos cuando el tiempo de convergencia no es una preocupación.

- Elegir protocolos de estado de enlace cuando:

- El diseño de red es jerárquico por lo general enredes amplias.
- Los administradores tienen conocimiento acerca de protocolos de estado de enlace.

3.9.3.1.4. Métricas para protocolos de enrutamiento

- Utilizan métricas para saber que ruta de acceso utilizar.
- Varían de acuerdo al tipo de métrica soportada.
- Protocolos tradicionales de vector distancia utilizan contador de saltos.
- Protocolos actuales también utilizan retraso, ancho de banda, confiabilidad.
- Las métricas pueden afectar la escalabilidad y performance.

3.9.3.1.5. Protocolos de ruteo jerárquico vs. no jerárquico

- Algunos protocolos no soportan jerarquía, todos los routers son compañeros de todos los demás routers.
- Los protocolos que soportan jerarquía en cambio asignan diferentes tareas a cada router.

3.9.3.1.6. Protocolos Interiores y Exteriores

- Protocolos de ruteo interior como RIP, OSPF, y EIGRP son utilizados en routers dentro de la misma organización o sistemas autónomos.
- Protocolos de ruteo exterior como BGP, realizan ruteo entre múltiples sistemas autónomos. BGP es utilizado en internet.

3.9.3.1.7. Protocolos de ruteo con clase vs. sin clase

- Los protocolos de ruteo con clase resumen subredes automáticamente, esto quiere decir que subredes discontiguas no son visibles una con otra y VLSM no son soportados.
- Los protocolos de ruteo sin clase transmitan longitud de prefijo de red o mascara de subred con la dirección IP, esto quiere decir que subredes discontiguas y VLSM son soportados.

3.9.3.1.8. Protocolos dinámicos vs estático

- Rutas estáticas
  - Son manualmente configuradas y no confían en actualizaciones de algún protocolo de ruteo. En algunos casos no es necesario utilizar algún protocolo de ruteo.
  - Por lo general son utilizadas para conectar a una red "stub" la cual reside en el borde de la red.
  - La desventaja con el ruteo estático es la cantidad de administración requerida especialmente en redes amplias.
  - Las rutas por defecto por lo general son estáticas.

3.9.3.1.9. Restricciones de escalamiento en ruteo

Antes de seleccionar un protocolo de ruteo, analice los objetivos que se requieren cubrir.

- ¿Hay algún límite en alguna métrica?
- ¿Velocidad de convergencia del protocolo de ruteo?
- ¿Cuán a menudo se realizan actualizaciones de rutas?

- ¿Cuánta data es transmitida en una actualización de ruta?
- ¿Cuánto ancho de banda es requerido para enviar las actualizaciones de rutas?
- ¿Cuánto uso de CPU es requerido para procesar actualizaciones de rutas?
- ¿Rutas estáticas soportadas?
- ¿Resumen de rutas soportas?

3.9.3.1.10. Convergencia de protocolos de ruteo

- La convergencia es el tiempo que toma en llegar a un entendimiento de la topología de red cuando un cambio ocurrió, el cambio puede ser caída de un segmento de red o falla en algún router o alguna nueva ruta añadida a la red.
- El tiempo de convergencia debe ser de pocos segundos para aplicaciones de voz sobre IP y Aplicaciones de Arquitectura de Red. En este caso se debería usar OSPF por su rápida convergencia.

3.9.3.2. Ruteo IP

3.9.3.2.1. RIP

- Vector-distancia y como métrica contador de saltos
- Cada 30 segundos publica su tabla de ruteo, 25 rutas por paquete, en redes amplias se requieren muchos paquetes.
- El ancho de banda es un problema en redes amplias que utilicen el protocolo RIP.
- Utiliza el camino más corto a pesar de que existan otras rutas con mayor ancho de banda.
- RIP1 es protocolo con clase y RIP2 es protocolo sin clase.

3.9.3.2.2. EIGRP

- Protocolo propietario de Cisco, solo puede ser utilizado en dispositivos Cisco.
- Utiliza los siguientes factores para su métrica:
  - Ancho de banda
  - Retraso
  - Confiabilidad
  - Carga

3.9.3.2.3. OSPF

- Las principales ventajas de OSPF
  - Estándar abierto soportado por muchos vendors.
  - Converge rápidamente.
  - Autentica el protocolo para cumplir con objetivos de seguridad
  - Soporta subredes discontiguas y VLSM
  - Envía frames multicast en vez de broadcast
  - Encaja en el diseño jerárquico mediante áreas lo que reduce CPU y memoria
  - No utiliza mucho ancho de banda.

3.9.3.2.4. IS-IS

- Protocolo de estado de enlace dinámico.
- Protocolo de ruteo sin clase.
- Pueden ser implementados en niveles jerárquicos:
  - Nivel 1: routers rutean entre la misma área.
  - Nivel 2: routers rutean entre áreas

- Nivel 1 y 2: routers participan en nivel 1 en el área de red interna y nivel 2 ruteo interarea.

3.9.3.2.5. BGP

- Dividido en dos:
  - iBGP: puede ser utilizado en una organización grande para el ruteo entre dominios.
  - eBGP: es utilizado en una organización grande para el ruteo de la organización además también participa en el ruteo del internet.

- Debe ser configurado por ingenieros con experiencia en este tipo de ruteo.
- Debe ser configurado en dispositivos con bastante memoria y CPU y un alto ancho de banda hacia internet.

3.9.3.3. Si va a utilizar varios protocolos en la red

- El criterio varía de acuerdo a las diferentes partes de la red.
- El diseño de la red debería enfocarse para las capas de Core y distribución y la necesidad de operar con la actual capa de acceso

3.9.3.3.1. Protocolos de ruteo y el diseño Jerárquico

- Protocolos de ruteo para la capa de Core
  - Debe incorporar enlaces redundantes y distribución de la carga entre enlaces del mismo costo.
  - Debe proveer respuesta inmediata si algún enlace falla.
  - Los protocolos de ruteo que cumplen con los objetivos antes mencionados son: OSPF, EIGRP, IS-IS.

La decisión para utilizar estos protocolos se basa en topología, direccionamiento IP, preferencias de vendors y metas técnicas y de negocio.

- Protocolos de ruteo para la capa de Distribución
  - Los protocolos para esta capa incluyen: RIPv2, EIGRP, OSPF y IS-IS.

- Protocolos de ruteo para la capa de Acceso
  - Los protocolos para esta capa están OSPF, RIPv2 y EIGRP.
  - Ruteo estático es también una posibilidad.
  - De ser necesario el uso de OSPF tener en cuenta el procesamiento y memoria que pueda requerir en los dispositivos de acceso.

3.9.3.3.2. Redistribución entre protocolo de ruteo

- La redistribución permite a los routers ejecutar más de un protocolo de ruteo y compartir rutas a través de estos.
- Al implementar redistribución tiene que ser cuidadoso debido a que cada protocolo se comporta distinto a otros y no pueden intercambiar información directamente además de que puede conllevar a bucles de ruteo.
- A pesar de los problemas que puede generar la redistribución es deseable para conectar capas del diseño jerárquico.
- Otro punto a tomar en cuenta es redistribución en una vía o en dos.
- En la mayoría de diseños jerárquicos se utiliza la redistribución en una vía.

- Resolviendo métricas incompatibles
  - Las métricas de un protocolo de ruteo no pueden ser convertidas fácilmente a otro protocolo de ruteo.
  - En vez de hacer la conversión, debería tomar la decisión de que métrica debería aplicarse a determinado protocolo de ruteo.

- Distancias administrativas
  - Todos los protocolos de ruteo y cada vendor manejan este punto de varias formas.

3.10. Desarrollar Estrategias de Seguridad de la Red

3.10.1. Diseño de seguridad de la red

Tener en cuenta los siguientes pasos que ayudaran a la elaboración de una estrategia de seguridad.

- Identificar activos de la red
- Analizar riesgos de seguridad
- Analizar requerimientos de seguridad
- Desarrollar un plan de seguridad
- Definir una política de seguridad
- Desarrollar procedimientos para la aplicación de políticas de seguridad
- Desarrollar un implementación técnica de seguridad
- Lograr un acuerdo de soporte para usuarios, managers y staff técnico.
- Entrenar usuarios, managers y staff técnico
- Implementar estrategias técnicas y procedimientos de seguridad
- Testear y actualizar la seguridad algún problema es encontrado

3.10.1.1. Identificar activos de la red

- La identificación de los activos y los riesgos que puedan sufrir como sabotaje o acceso inapropiado. Además de evaluar la consecuencia de estos riesgos.
- Tener en cuenta los activos de la red como hosts, sistemas operativos y data. Dispositivos de la red como routers, switches y la data que opera a través de estos.

3.10.1.2. Analizar riesgos de seguridad

- Intrusos externos pueden ganar acceso mediante de usuarios poco entrenados para la descarga de aplicaciones que contengan virus y

a causa de esto robar data, o denegar el servicio a usuarios legítimos.

- Los ataques de DoS se fueron incrementando en los últimos años.

3.10.1.3. Analizar requerimientos de seguridad y compensaciones

- Confidencialidad de la data, solo usuarios autorizados pueden ver información sensible.
- Integridad de la data, solo usuarios autorizados pueden cambiar información sensible.
- Sistemas y la disponibilidad de la data, los usuarios tienen acceso ininterrumpido a recursos.
- Tener en cuenta que al lograr objetivos de seguridad se tiene que compensar con la asequibilidad, usabilidad, performance, redundancia y equilibrio de carga.
- Además agrega una cantidad al trabajo de administración debido a IDs de usuario, logins, y registros auditables deben ser guardados.

3.10.1.4. Desarrollar un plan de seguridad

- El plan especifica tiempo, personas, y otros requerimientos que serán incluidos en el plan.
- El plan debe basarse en las metas de la red.
- Debe referenciar la topología de red y servicios a ser publicados.
- Evitar servicios no necesarios ya que incurren en nuevos filtros o firewalls.
- Evitar estrategias de seguridad complejas ya que se puede llegar a una autodestrucción.
- Las estrategias de seguridad complejas son difíciles de implementar correctamente sin añadir huecos de seguridad.
- Tener en cuenta si:

- ¿Administradores de seguridad experimentados serán contratados?
- ¿Cómo los usuarios finales y managers serán involucrados?
- ¿Cómo serán entrenados los usuarios, managers y staff de técnicos?

3.10.1.5. Desarrollando una política de seguridad

- Las políticas de seguridad informan a los usuarios, managers y staff de técnicos de sus obligaciones para la protección de la tecnología y de activos de información.
- La política debe especificar de cómo se deben cumplir las obligaciones.
- La política debe ser aceptada por los empleados, managers, ejecutivos y personal técnico.
- Las políticas de seguridad son un documento viviente, el cual debe ser actualizado a medida que cambien los requerimientos del negocio y objetivos técnicos.
- Los componentes de la política de seguridad:
  - Política de acceso
  - Política de contabilización
  - Política de autenticación
  - Política de privacidad

3.10.1.6. Desarrollar procedimientos de seguridad

- Los procedimientos definen configuración, login, auditoria y mantenimiento del proceso.
- Deben ser escritos para usuarios finales, administradores de red, administradores de seguridad de la información.
- Deben especificar como manejar incidentes.

3.10.1.7. Dar mantenimiento de seguridad

- Se le debe dar mantenimiento mediante auditoria en periodos de tiempo determinados a través de logs, reporte de incidentes, performance, pruebas de seguridad, entrenamiento a administradores de seguridad.
- Los riesgos cambian en el tiempo entonces la seguridad también.

3.10.2. Mecanismos de Seguridad

3.10.2.1. Seguridad Física

- Limitar acceso a recursos clave de red detrás de una puerta con llave protegidos de desastres naturales y humanos.
- La seguridad física deben ser instalada para proteger equipos de Core, puntos de demarcación, servidores, almacenamiento de backup, hosts.
- Tener en cuenta donde se instalaran equipos de networking para que estén físicamente seguros.

3.10.2.2. Autenticación

- La autenticación identifica a quien solicita un recurso de red puede ser un usuario, un dispositivo o un proceso de software.
- La autenticación tradicionalmente se basa en una de tres pruebas:
  - Algo que el usuario sabe: usualmente incluye el conocimiento de una palabra secreta que es compartida por ambas partes de la autenticación.
  - Algo que el usuario tiene: usualmente incluye posición física de un ítem que es único para el usuario: password, token, tarjeta de seguridad.

- Algo que el usuario es: Incluye verificación de una característica física única del usuario como huella digital, patrón de retina, voz o cara.

3.10.2.3. Autorización

- Quien puede acceder a que recursos y brindar privilegios a procesos y usuarios.
- ACL – Listas de Acceso en firewalls, gateways, routers, servers, estaciones de trabajo.
- Expertos de la seguridad recomiendan utilizar el "principio de menos privilegios" en la implementación, esto quiere decir que se debe dar el menor privilegio posible a cada usuario para completar alguna labor.

3.10.2.4. Auditaría Contabilización

- Para analizar efectivamente la seguridad de la red se debe recolectar información de la red para su revisión.
- Para redes con políticas de seguridad estrictas, auditoria debe ser lograda revisando todo intento de autenticación y autorización por cada usuario.
  - Incluir usuario, nombre de host, fecha y hora.
  - No se debe recolectar passwords.
- La evaluación de la seguridad y examinación de la red debe ser realizar por profesionales de la seguridad entrenados para descubrir vulnerabilidades explotados por intrusos.

3.10.2.5. Encriptación de la data

- Proceso que codifica la data para ser protegida de cualquier usuario que no sea el destinatario correcto.

- Se tiene que hacer compensaciones entre performance y latencia que genera la encriptación.
- Revisar algoritmos con llave simétrica y asimétrica.

3.10.2.6. Filtros de paquete

- Establecer en routers o switches para aceptar o denegar paquetes de direcciones o servicios particulares.
- Tomar la decisión del tipo de filtro:
  - Denegar cierto tipo de tráfico, permitir todo lo demás.
  - Aceptar cierto tipo de tráfico, denegar todo los demás.
- De implementarse ACL tener en cuenta que mientras menos condiciones mejora el Throughput, condiciones generales en la cima y condiciones específicas al final.

3.10.2.7. Firewalls

- Puede ser un router con ACL, una caja en hardware dedicada, o algún software en una PC o un sistema UNIX.
- Tener en cuenta firewalls:
  - Firewalls sin estado de la conexión “stateless”
  - Firewalls con estado de la conexión “statefull”
  - Proxy firewall

3.10.2.8. Prevención de intrusos y sistemas de prevención

- Tener en cuenta el tipo de IDS:
  - Host: reside en el host y lo monitorea.
  - Red: monitorea todo el tráfico de la red que puede ver, por lo general directamente conectada al firewall.

3.10.3. Modularizar el Diseño de Seguridad

- Tener en cuenta el principio de:
  - Defensa de seguridad a profundidad: La seguridad debe ser en multicapa con varias técnicas para proteger la red.

- Tener seguridad en todos los componentes del diseño modular:
  - Conexiones a internet
  - Servidores públicos
  - Redes de acceso remoto y VPN
  - Granja de servidores
  - Servicios de usuario
  - Redes inalámbricas

3.10.3.1. Seguridad a conexiones de internet

- Debe ser asegurada con un grupo de mecanismos superpuestos, incluyendo firewalls, filtros de paquete, seguridad física, auditoria de logs, autenticación y autorización.
- Tener en cuenta la cantidad de conexiones a internet es más sencillo asegurar una conexión que asegurar varias.
- Los riesgos comunes son ataques de reconocimiento desde internet.
- Tener en cuenta NAT para proteger la red interna.

3.10.3.1.1. Seguridad a servidores públicos

- Deben ser protegidos ubicándolos en DMZ protegidos por firewalls.
- Para proteger ataques de DoS, debe tener los servidores actualizados y aplicaciones con los últimos parches de seguridad.

- De ser asequible, no incluir varios servicios en un solo servidor.
- En el caso de servidores de base de datos que son consultadas por servidores web estos deben estar o bien en la granja de servidores interna o en otra zona DMZ.

3.10.3.2. Seguridad de acceso remoto y VPN

- Para asegurar acceso remoto de usuarios se debe incorporar a la red Enterprise VPN Gateway, VPN sitio-a-sitio.

3.10.3.2.1. Dar seguridad a tecnología de acceso remoto

- La seguridad es crítica para el acceso de clientes remotos se debe tomar en cuenta: tecnologías de firewall, seguridad física, mecanismos de autenticación y autorización, auditoria y encriptación.
- Tener en claro los protocolos de seguridad:
  - PPP
  - CHAP
  - IP-Sec
  - Servicios de autenticación y autorización RADIUS

3.10.3.2.2. Seguridad en VPN

- En topologías VPN la encriptación es una obligación porque data privada circula a través de la red pública.
- La solución más común para la encriptación es el protocolo de seguridad IP IPsec que es el estándar para la IETF.

- Tener en claro el proceso de IPsec y los protocolos y puertos que son necesarios.

3.10.3.3. Seguridad a servicios de red y administración de la red

- Aplicar listas de acceso para la administración de dispositivos
- Utilizar mecanismos de autorización y autenticación como RADIUS o TACACS.
- Utilizar protocolos seguros de administración HTTPS y SHH en vez de HTTP y telnet.
- Utilizar administración centralizada pero limitando el uso de SNMPv1v2 por motivos de seguridad, si los equipos soportan SNMPv3 es válido.
- Tener en cuenta la administración out-of-band e in-band.
- De ser necesario colocar los equipos de administración en una DMZ privada.
- Actualizar los dispositivos a la última versión y con los parches necesarios además de deshabilitar servicios no necesarios.

3.10.3.4. Seguridad a granjas de servidores

- Las granjas de servidores albergan servidores de archivos, impresión, base de datos, aplicación, entre otros está dentro la red de campus. Estos manejan información sensible y deben estar protegidas.
- Performance por lo general es un problema crítico la cual puede limitar la elección de mecanismos de seguridad.
- Se deben asegurar con IDS de host y de red.
- Para maximizar la seguridad tanto cliente como servidor debe ser mantenido correctamente. Bugs en los sistemas operativos deben ser parchados y corregidos.

- En entornos donde la seguridad es un requerimiento principal, las aplicaciones de servidor deben ser encriptados.
- Para aplicaciones de servidor de archivos y otras debe tomarse en cuenta la autorización y autenticación.
- Privilegios de root o administrador solo deben ser dados a pocas personas.

3.10.3.5. Seguridad a servicios de usuarios

- Las PCs no deben descargar aplicaciones, para esto soporte técnico debe instalar las aplicaciones permitidas por la organización.
- Las PCs deben tener firewall y antivirus.
- Indicar a los usuarios cerrar sesiones hacia cualquier servicio cuando estén un tiempo prolongado fuera de sus escritorios. En caso contrario implementar políticas de cierre de sesión automático o bloqueo de pantalla.
- Los usuarios solo deben poder conectarse a las computadoras y a las interfaces de los equipos que le corresponden.
- Tener en cuenta el protocolo 802.1X y su implementación con LDAP, RADIUS.

3.10.3.6. Seguridad a redes inalámbricas

- Las mejores prácticas indican poner en un segmento distinto o una vlan aparte, esto simplifica el direccionamiento y mejora la seguridad.
- Para maximizar la seguridad es más idóneo subdividir la red inalámbrica en varias VLAN y segmentos IP.
- Los requerimientos de acceso para usuarios Wireless varían de acuerdo al tipo de usuario.
- Tener en cuenta los siguientes premisas:
  - Autenticación

- Privacidad de la data
- Acceso protegido a las wireless

3.11. Desarrollar Estrategias de Administración de la Red

La administración de la red es uno de los aspectos más importantes del diseño de red lógico. Un buen diseño de administración de red puede ayudar a la organización a cumplir con la disponibilidad, performance y metas de seguridad.

La administración de la red facilita la escalabilidad porque ayuda a analizar el comportamiento actual de la red, aplicar actualizaciones apropiadas y solucionar problemas con actualizaciones.

3.11.1. Diseño de la administración de la red

- Tener en cuenta:
  - Escalabilidad
  - Patrones de trafico
  - Formatos de data
  - Costo/beneficio
  - Compensaciones

- Revisar que equipos se van a monitorear y las métricas que se van a utilizar.
- Elegir cuidadosamente la data que se va a guardar y analizar.

3.11.1.1. Administración proactiva de la red

- El monitoreo proactivo se refiere a la revisión de la salud de la red en operaciones normales para reconocer problemas potenciales, optimizar performance y aplicar actualizaciones.
- Al realizar el diseño de administración proactiva se debe tener en cuenta que se requerirán herramientas sofisticadas que las tradicionales. Se puede hacer una compensación asumiendo menor tiempo fuera de servicio en caso de fallas.

3.11.1.2. Procesos de la administración de la red

3.11.1.2.1. Administración de fallas

- Se tiene que seguir el siguiente orden detectar, aislar diagnosticar y corregir problemas, además del rastreo respectivo para corregir el problema.
- Existen una variedad de herramientas para este tipo de administración como SNMP o RMON además de SYSLOG.

3.11.1.2.2. Administración de la configuración

- Mantener información de las configuraciones aplicadas a los dispositivos.
- Mantener inventario de los activos de red y de log de versiones.
- Facilitar cambios en la administración.

3.11.1.2.3. Administración de la contabilización

- Contabilización y facturación en el caso de que se ofrezca algún servicio.
- También para la revisión de quienes son los usuarios que abusan del servicio de red de forma intencional o no intencional.

3.11.1.2.4. Administración del performance

- Tener en cuenta los siguientes factores:
  - Examinar las aplicaciones de red y su comportamiento.
  - Analizar la accesibilidad.

- Medir tiempo de respuesta.
- Grabar el cambio de rutas de red.

- Cumplimiento de SLA

- Optimizar a partir de los resultados.

- Dos tipos a ser monitoreados:

  - Punto a punto: mide el performance a través de toda la red, tener en cuenta disponibilidad, capacidad, utilización, retraso y la variación del retraso.
  - Componente: mide el performance de dispositivos individuales, como utilización y Throughput de un segmento especifico.

- Utilizar analizadores de protocolo o herramientas SNMP para grabar cargas de tráfico.

3.11.1.2.5. Administración de la seguridad

- Permite al administrador de la red mantener y distribuir passwords y otra información de autenticación y autorización.
- Un aspecto importante es el proceso para recolectar, guardar y examinar log de seguridad.
- Tener los logs en un lugar seguro en caso contrario encriptarlos.
- Por lo general no utiliza mucho el protocolo SNMP a menos que sea SNMPv3.

3.11.2. Arquitecturas de la administración de la red

Cuenta de tres componentes principales:

- Dispositivo administrado: El dispositivo que recolecte y guarde información de los demás dispositivos de red como routers, switches entre otros.
- El agente: El software que reside en un dispositivo administrado.
- El sistema de administración de red NMS: Ejecuta aplicaciones para la visualización de la data administrada, monitorea y controla dispositivos administrados. Tener en cuenta de que el hardware donde se instale el NMS debe ser sofisticado en gráficos, memoria, procesamiento y almacenamiento.

3.11.2.1. En banda vs. Fuera de banda

- En banda:
  - Más fácil de implementar.
  - Más difícil de corregir problemas.
  - Facilita el uso de herramientas analizadoras de protocolo en caso de congestión.

- Fuera de banda:
  - Más complejo y costoso.
  - Nuevos enlaces para la administración entre agentes y NMS lo hace vulnerable.

3.11.2.2. Centralizada vs. Distribuida

- Centralizada: Todos los NMS residen en un área de red en el Centro de Operación de Red NOC. Los agentes dispersos en toda la red y envían la información al NMS. Por lo general es la mejor elección.
- Distribuida: NMS y agentes están dispersos por toda la red. Es un diseño jerárquico donde un NMS envía información de varios NMS

al NMS principal. MoM Manager de Manager es la comunicación que utiliza además puede filtrar la data antes de enviarla. Tener en cuenta que es una arquitectura compleja y difícil de administrar.

3.11.3. Seleccionar herramientas de administración de red y protocolos

3.11.3.1. Herramientas de administración de red

- Para asegurar disponibilidad de la red, se tiene que tomar en cuenta las características de las herramientas:
  - Performance
  - Fallas
  - Configuración
  - Seguridad
  - Administración de la contabilidad
  - Flexibilidad
  - Interfaz de administración

3.11.3.2. Protocolo simple de administración de red SNMP

- Soportado por la mayoría de dispositivos y vendors y puede trabajar en entornos multivendor.
- Tener en cuenta las características de SNMPv3 de seguridad sobre SNMPv1, SNMPv2.

3.11.3.2.1. MIB

- Tener en cuenta las MIB generales y propietarias.
- Actualizar NMS con las MIB de los vendor que se utilice.

3.11.3.2.2. RMON

- Son importantes porque capturan información de CRC, colisiones Ethernet, distribución de tamaño de paquete, numero de paquetes de entrada y salida, y la tasa de paquetes de broadcast.
- RMON1 se enfoca en capas de enlace y física, tener en cuenta RMON2 que describe performance de aplicaciones y comunicaciones punto a punto.

3.11.3.3. Estimar el trafico causado por la administración de red

- Después de determinar que protocolos de administración se van a utilizar se debe calcular cuanta cantidad de tráfico generara la administración de la red.
- Se debe tener que red y dispositivo será administrado.
- Se debe tener en cuenta la cantidad de dispositivos y que característica será monitoreada.
- El tráfico de administración no debe superar el 5% de la capacidad total de la red.

DISEÑO DE RED FÍSICO

3.12. Seleccionar tecnologías y Dispositivos para redes de Campus

El diseño físico incluye la selección de tecnologías LAN y WAN para diseños de campus y de Enterprise. Un diseño efectivo debe enfocarse primero en la implementación de redes campus, seguido de accesos remoto y soluciones WAN.

3.12.1. Diseño de planta de cableado LAN

- Tener en cuenta que otros componentes del diseño de la red generalmente tiene un tiempo vida de pocos años antes que la tecnología cambie, la infraestructura de cableado debe durar por varios años.
- El cableado que se encuentra actualmente en los edificios se debe tener en cuenta lo siguiente:
    - Topologías de cableado de campus y de edificio.
    - Tipos y longitudes de cables entre edificios.
    - Ubicación de cuartos de telecomunicaciones y conexiones cruzadas entre edificios.
    - Tipos y longitudes de cables para el cableado vertical entre pisos.
    - Tipos y longitudes de cables para el cableado horizontal entre pisos.
    - Tipos y longitudes de cables para el cableado entre gabinetes de telecomunicaciones y estaciones de trabajo finales.

3.12.1.1. Topologías de cableado

Tener el cableado centralizado como es la topología estrella, y la distribuida como son los desarrollos anillo, bus y mallas.

3.12.1.1.1. Construir Topología de cableado

- Entre el mismo edificio, se puede utilizar desarrollos centralizados o distribuidos.
- Para edificios pequeños un desarrollo centralizado sería la mejor opción por la administración pero no tendría escalamiento.
- Para edificios grandes una topología distribuida es más eficiente.

3.12.1.1.2. Topología de cableado de campus

- La exposición del cableado que interconecta edificios está más expuesto a daño físico que pueda ser ocasionados por obras civiles, fenómenos naturales o daño humano. Por este motivo este cableado debe ser seleccionado cuidadosamente.
- En algunos ambientes tener en cuenta los obstáculos para la interconexión como: arroyos y otras construcciones.

3.12.1.2. Tipos de cable

- En implementaciones de campus: STP, Coaxial, twinax, UTP, Fibra óptica
- STP, coaxial ya no se utilizan para nuevas implementaciones a menos que se requiera un alto grado de blindaje.
- Para instalaciones nuevas UTP Cat 5e debe ser el mínimo a utilizar. TIA recomienda al menos UTP Cat 6.
- Utilizar fibra óptica para conexiones verticales y horizontales entre gabinetes de comunicación y edificios. La desventaja principal es la instalación y costo. Además ver la perdida por tipo de conector.

3.12.2. Tecnologías LAN

Tener en cuenta:

- Sesgos de la tecnología
- Políticas acerca de la tecnología o vendors
- Tolerancia a fallos
- Habilidad técnica del personal y plan para capacitación
- Presupuesto y programación de tiempo

3.12.2.1. Bases de Ethernet

- Ethernet es actualmente capaz de soportar requerimientos de ancho de banda e implementada con altos componentes para cableado, NICs y dispositivos de interconexión para cumplir con los más altos requerimientos de disponibilidad.
- Para la resolución de problemas cuenta con herramientas como testeadores de cables, analizadores de protocolo, aplicaciones de administración de red entre otros.
- Tener en cuenta Ethernet II y el estándar IEEE 802.3 para lo que es cableado UTP y de fibra óptica.

3.12.2.2. Opciones de tecnología Ethernet

Tener en cuenta las siguientes tecnologías:

- Full y Half duplex Ethernet, CDMA/CD
- 100-Mbps Ethernet, IEEE 802.3
- Gigabit Ethernet:
  - 1000 Base-SX, ideal para cableado horizontal y backbone
  - 1000 Base-LX, para enlaces distantes entre edificios de campus.
  - 1000 Base-T, para enlaces horizontales y área de trabajo, requiere Cat 5 o mejor.

- 10-Gbps Ethernet
  - 10G Base-L, distancias largas, tener en cuenta el tipo de fibra óptica.
  - 10G Base-S, distancias corta, tener en cuenta el tipo de fibra óptica.
  - 10G Base-T, para estaciones que requieren alto ancho de banda como data-stores, servidores.

- Metro Ethernet
  - Soporta cobre y fibra además de varios tipos de protocolos de transporte como SONET, ATM, DWDM y MPLS.

- Long-Reach (Larga distancia) Ethernet LRE: Velocidad síncrona de hasta 11.25Mbps a distancia de 1km.
- Link-agregattion: Tener en cuenta tecnologías de agregación de enlace para sumar y balancear carga a través de 2, 4 u 8 enlaces del mismo tipo y hacerlos trabajar como uno solo.

Cada una de las tecnologías presentadas son posibles para las capas de acceso, distribución o core. La elección del tipo de tecnología en capas de acceso, depende de la ubicación y tamaño de comunidades de usuario, ancho de banda y requerimientos de QoS. Para las capas de Core y distribución depende en la topología de red, la ubicación de data-stores, y el flujo de tráfico.

3.12.3. Seleccionar dispositivos para el diseño de red de campus

- A este punto ya se debe tener desarrollada la topología de red y tener una idea de que segmentos serán interconectados.
- En la mayoría de los casos se utilizaran routers o switches ya que hubs y bridges ya no son utilizados.

- Después de haber analizado los requerimientos y tener claro el diseño se puede hacer las recomendaciones de los dispositivos a adquirir.

3.12.3.1. Criterio para la selección de dispositivos de la red

Para dispositivos como router y switches:

- Numero de puertos
- Velocidad de procesamiento
- Cantidad de memoria
- Total de latencia
- Throughput en paquetes por segundo
- Colas de ingreso y salida y técnicas de buffer
- Tecnologías LAN, WAN soportadas
- Autosensing de velocidad, 10/100/100
- Auto detección de operación half, full
- Cable soportado
- Facilidad de configuración
- Administración, SNMP, RMON
- Costo
- Tiempo entre fallas MTBF y Tiempo de reparación MTTR
- Soporte de filtro de paquetes y otras medidas de seguridad
- Soporte de componentes hot-swap
- Soporte de actualizaciones en servicio.
- Soporte de fuentes de poder redundantes
- Soporte de QoS
- Disponibilidad y calidad de soporte técnico
- Disponibilidad y calidad de documentación
- Disponibilidad y calidad de entrenamiento
- Reputación y viabilidad del vendor
- Disponibilidad de pruebas y resultados independientes que prueben la capacidad del dispositivo.

Para switches se puede añadir lo siguiente:

- Soporte de tecnologías de Bridging (STP)
- STP Avanzado RSTP, MSTP
- Numero de direcciones MAC que el equipo puede aprender
- Soporte de stack de switches donde varios dispositivos se pueden administrar como uno solo
- Soporte de autenticación 802.1X
- Soporte de tecnologías VLAN 802.1Q
- Soporte de multicast
- Cantidad de memoria para tablas de switcheo y ruteo (switches L3)
- Disponibilidad de un módulo de ruteo.
- Power over Ethernet POE, 802.3af o POE+ 802.3at

Para routers y switches L3 los siguientes criterios pueden ser añadidos:

- Soporte de protocolos de capa de red
- Soporte para protocolos de ruteo
- Soporte de aplicaciones multicast
- Soporte avanzado de colas, switching y otros adicionales de optimización.
- Soporte de compresión
- Soporte de encriptación

3.12.3.2. Características de optimización en dispositivos de la red

- QoS en LAN para requerimientos de latencia baja y jitter.
- QoS por lo general en uplinks de capa de acceso a distribución y de distribución a core.
- Tener en cuenta que en la mayoría de redes existe sobresuscripción y por consecuencia se requiere de reglas de QoS.

3.12.4. Ejemplo de un diseño de red de campus

- Información de fondo para el proyecto de diseño de la red de campus
- Metas del negocio
- Metas técnicas
- Aplicaciones de red
- Comunidades de usuario
- Servidores o Data Stores
- Red actual
  - Identificación del tráfico de la red actual
  - Resumen del flujo de trafico
  - Identificación de performance de la red actual
- Rediseño de la red
  - Optimización del direccionamiento IP y ruteo en el backbone de campus
  - Red inalámbrica
  - Mejora de la performance y seguridad de la red de perímetro

3.13. Seleccionar Tecnologías y Dispositivos para redes Enterprise

3.13.1. Tecnologías de acceso remoto

- A medida que las organizaciones se vuelven móviles y geográficamente dispersadas las tecnologías de acceso remoto son un ingrediente principal en el diseño de redes Enterprise.
- El fin es proveer conexión a usuarios externos para que puedan desarrollar su trabajo como si fuese de manera local.
- Se debe tener un análisis de las aplicaciones que los usuarios utilizaran de manera remota.
- Además de la ubicación y la cantidad de usuarios y el tiempo que utilizara cada usuario de manera remota
- Tener en cuenta la ubicación de sucursales y la disponibilidad de tecnología en esos lugares.
- PPP es el protocolo de conexión remota con mayores implementaciones.

3.13.1.1. Líneas telefónicas

- Solo soporta hasta 56kbps y son conexiones lentas, actualmente las aplicaciones de los usuarios remotos requieren un ancho de banda mayor

3.13.1.2. Cable Modem

- Soportan un ancho de banda mayor a líneas telefónica, utilizan las conexiones de la empresas de televisión por cable fibra hibrida coaxial HFC.
- Algunas desventajas es que de velocidad asíncrona mayor ancho de banda de bajada que de subida. No es una buena opción para aplicaciones cliente/servidor.

- Si se va a elegir esta tecnología consulte con su proveedor cuantas conexiones concurrentes habrá en el mismo cable y que aplicaciones utilizaran.

3.13.1.3. DSL

- Altas velocidad mediante el cable par telefónico simple.
- Tener en cuenta la tecnología de DSL a utilizar asimétrica o simétrica.
- La conexión simétrica es una buena opción para sucursales pequeñas.

3.13.2. Seleccionar dispositivos de acceso remoto Enterprise

Primero identificar la oficina principal y las oficinas sucursales.

3.13.2.1. Seleccionar dispositivos para usuarios remotos

Tomar en cuenta los siguientes criterios:

- Seguridad y características de VPN
- Soporte de NAT
- Confiabilidad
- Costo
- Facilidad de configuración y administración
- Soporte de uno o más interfaces de alta velocidad Ethernet
- Soporte de router inalámbrico
- Soporte de agregación de canales
- Soporte de QoS para soportar aplicaciones de VoIP con requerimientos específicos.

3.13.2.2. Seleccionar dispositivos para usuarios en la sede central

Tomar en cuenta los criterios para los usuarios remotos además agregar características de funcionabilidad VPN.

- Si la cantidad de usuarios VPN superan 100 utilizar un concentrador VPN fuera del router para evitar congestionamiento.
- Por lo general las redes Enterprise existe un firewall VPN entre el concentrador o router VPN y la red interna.
- Tener en cuenta el software de los clientes VPN que se utilizaran y la correcta configuración y actualización para la conexión con el concentrador VPN.
- Tener en cuenta el número de conexión concurrentes que el firewall soporta y la cantidad de tráfico que puede reenviar.
- El firewall debe tener un procesador rápido, memoria RAM de alta velocidad. También tomar en cuenta las siguientes características:
  - Protocolos de túnel: IP-Sec, PPTP, L2TP, SSL
  - Algoritmos de encriptación: DES, 3DES, RC4, AES.
  - Algoritmos de autenticación incluyendo MD5, SHA1, HMAC.
  - Protocolos DNS, RADIUS, LDAP, Kerberos
  - Protocolos de ruteo
  - Soporte de certificados de autoridades certificadoras Entrust, VeriSign, Microsoft
  - Administración mediante SSH y HTTPS

3.13.3. Tecnologías WAN

3.13.3.1. Sistemas para el aprovisionamiento de ancho de banda en la WAN

- Se tiene que tomar en cuenta los requerimientos de capacidad actualmente y provisionar para dos o tres años.

- Se puede tomar el estándar americano "North American Digital Hierarchy"

  - T1 → 1.544Mbps
  - T2 → 6.312 Mbps
  - T3 → 44.736 Mbps
  - T4 → 274.176 Mbps
  - T5 → 400.252 Mbps

- También se puede tomar el estándar SDH "Syncrhronous Digital Hierarchy"

  - STS-1 → 51.84 Mbps
  - STS-12 → 622.08 Mbps
  - STS-24 → 1.244 Gbps
  - STS-48 → 2.488 Gbps
  - STS-96 → 4.976 Gbps
  - STS-192 → 9.952 Gbps

3.13.3.2. Líneas arrendadas

- Circuitos dedicados que ofrecen los ISP por un periodo de tiempo de meses o años
- Topología punto a punto, ofrecen ancho de banda desde 64kbps hasta T3.
- Tomar en cuenta la encapsulación PPP, HDLC
- Estas líneas tienen ventaja sobre las demás porque están maduras y probadas tecnológicamente.
- La desventaja es que son costosas pero a medida que los carriers implementan nueva tecnología estas líneas bajan en costo.

3.13.3.3. SONET - Red Síncrona Óptica

- Tendencia a crecer debido a que los ISP implementan en su planta.
- Tienen mayor capacidad de ancho de banda desde 51.84 Mbps en STS-1

3.13.3.4. ATM

- Velocidades 9.952 Gbps o superiores utilizando WDM.
- Buen manejo de QoS utilizando el medio compartido
- Interfaces costosas puede ser desventaja para su implementación.
- Ethernet sobre ATM utiliza la simplicidad de Ethernet y reduce costos y utiliza las ventajas de ATM, es una tendencia en carriers para proveer enlaces WAN.

3.13.3.5. Metro Ethernet

- Utiliza interfaces de 10/100 Mbps o 1Gbps o 10 Gbps para llegar a la red del ISP y de esta manera tener un enlace hacia internet.
- Utiliza varios protocolos de transporte incluyendo SONET, ATM, DWDM y MPLS.
- Tener en cuenta que permite al proveedor agregar ancho de banda a medida que se requiera.

3.13.4. Seleccionar un proveedor WAN

- Tener en cuenta que el costo no debe ser el criterio principal, bajo ese punto de vista tener en cuenta lo siguiente:

  - Servicios y la tecnología que ofrece el proveedor
  - Áreas geográficas cubiertas por el proveedor

- Características de confianza y performance de la planta de red del proveedor
- Nivel de seguridad ofrecida por el proveedor
- Nivel de soporte técnico
- Probabilidad de que el proveedor siga en el mercado
- Voluntad del proveedor para cumplir las necesidades

- Investigar la planta del proveedor estructura, seguridad, confiablidad, contactar clientes similares, contactar ingenieros basado en eso se debe tener en cuenta:

  - Las rutas físicas de los enlaces
  - Redundancia en la red
  - Ver si el proveedor confía en cuales otros proveedores para redundancia.
  - El nivel de sobresuscripción de la red.
  - Asignación de ancho de banda y mecanismos para cumplir requerimientos de QoS
  - Frecuencia y causas típicas de cortes de red
  - Métodos de seguridad utilizados para proteger la red de intrusos
  - Métodos de seguridad utilizados para proteger la data del cliente
  - Recuperación ante desastres

- Tener en cuenta niveles de servicio SLA (Service Level Agreement) para definir y medir como el servicio será garantizado. Por lo general se tiene que definir, disponibilidad de la red, performance, latencia. Además de misión crítica 7*24*365.

3.13.5. Ejemplo de diseño WAN

- Información de fondo del proyecto WAN
- Metas de negocio y técnicas
- Aplicaciones de red
- Comunidades de usuario
- Servidores o data-stores
- Red actual
- Identificación del tráfico de la WAN actual

PRUEBAS, OPTIMIZACIÓN, DOCUMENTACIÓN DEL DISEÑO

3.14. Probar el Diseño de Red

Tener en cuenta que cada sistema de red es distinto entonces se debe seleccionar métodos y herramientas que requieran mentalidad técnica, creatividad, ingenio, y entendimiento completo del sistema de red a ser evaluado. Además revisar lo siguiente:

- Verificar que el diseño cumpla con las expectativas del negocio y metas técnicas.
- Verificar las tecnologías LAN y WAN y los dispositivos seleccionados.
- Verificar que el/los proveedores de servicio provean el servicio acordado.
- Identificar cuellos de botella o problemas de conectividad
- Probar la redundancia de la red.
- Analizar efectos en performance a causa de fallas de enlaces de red.
- Determinar técnicas de optimización para cumplir performance y metas técnicas.
- Pasar un test de aceptación que obtenga aprobación para la implementación de la red.
- Convencer a las jefaturas y trabajadores que el diseño es efectivo.
- Identificar riesgos que impidan la implementación y realizar plan de contingencia.
- Identificar cuantas pruebas adicionales serán requeridas.

3.14.1. Utilizar testeadores

- De ser necesarios recurrir a laboratorios independientes como:
    - ICSA Labs
    - The Tolly group
    - Miercom
    - AppLabs

- En algunos casos se puede confiar en los resultados de las pruebas que provienen de vendors, laboratorios independientes o revistas comerciales pero tomarlos solo de manera informativa.
- En caso de redes de campus basado en tecnología de un solo vendor especifico, verificar pruebas realizadas a los dispositivos por algún laboratorio independiente para probar la efectividad del diseño.
- En caso de diseños más complejos se debe hacer pruebas propias para probar la efectividad del diseño.
- Es usualmente necesario construir un prototipo o laboratorio para comprender como se comportaran los componentes de red en la su configuración con las aplicaciones, tráfico de red y otros requerimientos.

3.14.2. Construir y testear un prototipo de sistema de red

- El prototipo permitirá al diseñador validar la operación y performance del nuevo sistema de red.
- Tiene que ser funcional, pero no necesita ser una implementación a full escala.

3.14.2.1. Determinar el ámbito del prototipo de sistema

- No es práctico hacer un prototipo a full escala, se debe aislar que aspectos del diseño de red son los más importantes.

- Tener en cuenta los recursos para desarrollar el prototipo, como personas, equipamiento, tiempo y dinero. Pero utilizar los recursos suficientes para no incurrir en sobregiros de presupuesto, demoras.

- El prototipo puede ser:
  - Un test de laboratorio
  - Integrada a la red de producción pero probada en horas de descanso.
  - Integrada a la red de producción y probada en horas de trabajo normal.

- Antes de llevarlo al entorno de producción es mejor probar la configuración en un test de laboratorio para no afectar en el peor de los casos a la red de producción.

3.14.2.2. Testear el prototipo de una red de producción

- Después que el diseño es aceptado es importante testear una parte de la implementación para identificar cuellos de botella u otros problemas que el tráfico real pueda disparar.

- A continuación se detallan algunos parámetros para pruebas en tiempo real:

  - Advertir a los usuarios que puede ocurrir algún tipo de degradación de performance en algún momento, pero que sigan realizando sus labores de manera normal.
  - Advertir a los administradores u otros para que no realicen pruebas al mismo tiempo.
  - Advertir a los managers de confundirse por alarmas inesperadas en el comportamiento de la red.

- De ser posible realizar ejecutar pruebas cortas de 2 minutos o menos para minimizar el impacto en la red.
- Ejecutar pruebas con configuración y tráfico menor luego ir incrementando.
- Monitorear los resultados de las pruebas y descontinuarlas cuando generen un impacto largo de fallas.

3.14.3. Escribir e implementar un plan de test para su diseño de red

- Después de haber analizado el ámbito del proyecto de pruebas se debe escribir el plan de implementación de pruebas, el cual debe contener:

  - Objetivos y criterios de aceptación
  - Los tipos de pruebas que se van a ejecutar
  - Equipos de red y otros recursos requeridos
  - Scripts de prueba
  - Determinar la línea de tiempo e hitos del proyecto de prueba.

3.14.3.1. Desarrollar test de objetivos y criterio de aceptación

  - Los objetivos deben ser específicos y concretos y deben incluir información si el test pasó o falló.
  - Deben basarse en los objetivos del diseño de red además deben ser formales y definidos específicamente.
  - El criterio para declarar que el test pasó o fallo debe ser claro y aceptado por el testeador y el usuario final.
  - El objetivo del test debe medir el resultado y no si el resultado es en su favor y basarse en los estándares de la industria.

3.14.3.2. Determinar el tipo de test a ejecutarse

- En general los test deben incluir performance, análisis de stress y análisis de fallas.
- Performance test incluyen Throughput, retrasos, tiempo de respuesta y eficiencia.
- Análisis de stress examina alguna variación o degradación del servicio a causa del incremento de carga en la red.
- Análisis de fallas debe calcular la disponibilidad de la red y la precisión además de analizar el porqué de la caída de red.
- Test usuales incluyen lo siguiente:

    - Test de tiempo de respuesta de aplicaciones, enfocándose al usuario final de cuánto tiempo es lo que tendrá que esperar para que una aplicación cumpla una tarea.
    - Test de Throughput: mide en kilobytes y megabytes por segundo o en paquetes por segundo debe ser probado gradualmente.
    - Test de disponibilidad: debe ser probado entre 24 y 72 horas en un ambiente de carga media a pesada.
    - Test de regresión: tener en cuenta que el nuevo sistema de red no debe malograr alguna aplicación o componente que haya funcionado hasta que se instaló el nuevo sistema de red.

3.14.3.3. Documentar el equipo de red y otros recursos

- Tener en cuenta que se debe incluir todos los recursos que se necesitaran incluyendo los siguientes:

    - Programar horarios en ambiente de laboratorio y organización donde se llevara a cabo.

- Energía eléctrica, aire acondicionado, espacio de rack, y otros recursos físicos.
- Ayuda de otros cotrabajadores y personal de la organización.
- Ayuda de usuarios para probar aplicaciones.
- Direcciones de red y nombres.

3.14.3.4. Escribir scripts para las pruebas

- Para cada test, tener en claro el objetivo del test, criterio de aceptación y para detallar el test escribir scripts que listen todos los pasos que se tiene que seguir para cumplir el objetivo del test. El script debe incluir las herramientas que se utilizan para cada paso que se realice además de las mediciones relevantes y los logs del test.

3.14.3.5. Documentar la línea de tiempo del proyecto

- Para proyectos complejos y/o amplios se debe documentar la línea de tiempo que se empleara, incluyendo las fechas de inicio y fin para el proyecto y los principales hitos. A continuación se detalla una lista del plan de pruebas:
  - Escribir objetivos y criterio de aceptación.
  - Diseñar la topología para el ambiente de pruebas.
  - Determinar que hardware y software de red se utilizará.
  - Adquirir hardware o software de ser necesario
  - Determinar que herramientas de testeo se utilizaran
  - Adquirir herramientas de testeo de ser necesario
  - Determinar que otras recursos serán necesarios
  - Escribir los scripts para los test
  - Instalar y configurar hardware y software
  - Empezar las pruebas

- Guardar los resultados de la pruebas en logs.
- Revisar y analizar los resultados
- Reducir la data de los resultados de ser necesario
- Presentar los resultados al Manager de TI
- Archivar resultados

3.14.3.6. Implementar el plan de prueba

- La implementación del plan de prueba depende mucho de los scripts de prueba y la documentación del trabajo realizado.
- Tener en cuenta que algunas veces los scripts de prueba no pueden ser llevados precisamente debido a que pueden surgir problemas en el camino, por esta razón es importante mantener los logs para su posterior revisión.
- Adicionalmente guardar los log que documenten data y resultados de las pruebas.
- Los log de actividad diaria pueden ser utilizados para rastrear algún problema y sus posibles causas.

3.14.4. Herramientas para las pruebas del diseño de red

3.14.4.1. Tipos de herramientas

En general los tipos de herramientas que se pueden utilizar para testear la red incluyen las siguientes:

- Herramientas de administración y monitoreo
- Herramientas de generación de trafico
- Herramientas de modelamiento y simulación
- QoS y herramientas de administración de acuerdo a nivel

3.14.4.2. Herramientas para realizar las pruebas

- Cisco Works Internetwork performance monitor
- WANDL Network planning and analysis tools
- OPNET Technologies
- Ixia Tools
- NetIQ Voice and Video Management Solution
- NetPredictor

3.15. Optimizar el Diseño de Red

Las razones por la cuales se debe optimizar la red:

- Cumplir con los objetivos de negocio y metas técnicas.
- Utilizar el ancho eficientemente.
- Controlar el retraso de serializacion.
- Soportar servicio preferencial para aplicaciones esenciales.
- Cumplir con requerimientos de Calidad de Servicio QoS.

3.15.1. Optimizar el uso de ancho de banda con tecnologías IP multicast

- En el caso de que se utilice aplicaciones como clases online dentro del campus, reuniones virtuales, transmisiones de video entre otras utilizar el uso de tecnologías multicast para utilizar eficientemente el ancho de banda de la red.

- Tener en muy claro los parámetros y el funcionamiento de multicast en caso de que se implemente, a continuación se listan los ítems a tener en cuenta:

  - Direccionamiento Multicast: IP, MAC
  - Protocolo IGM: administración de la conexiones.
  - Protocolos de ruteo de multicast

- Vector-Distancia – DVMRP
- Protocolo independiente multicast - PIM

3.15.2. Optimizar el performance para cumplir requerimientos de QoS

- En el punto 3.4 se especifica de clasificar las aplicaciones para proveer que tipo de QoS requerirá.

- Tener en cuenta los dos tipos que ofrecen garantía de QoS en comparación del servicio de mejor esfuerzo.

    - Servicio de carga controlada, destinado hacia aplicaciones sensibles a condiciones de sobrecarga.
    - Servicio garantizado, destinado a hacia aplicaciones que necesitan la garantía de que un paquete llegue a su destino sin demoras.

- Tener en claro los protocolos y configuraciones para cumplir con los requerimientos de QoS como: Precedencia IP y tipo de servicio, Servicios diferenciados IP “diffserv”, DSCP.

3.15.2.1. Clasificando el trafico LAN

- La IEEE especifica métodos para etiquetar LAN frames con clase de servicio en el documento 802.1D pero más conocido como 802.1p, el cual especifica mecanismos para los switches de acelerar el envío de tráfico critico en tiempo y limitar el exceso de ancho de banda multicast en una LAN switcheada.
- Tener en cuenta las 8 tipo de clasificaciones
- Se tiene que tener en cuenta que la mayoría de veces no se requiere QoS en la LAN debido que tiene un ancho de banda alto 100 Mbps, 1Gbps, 10Gbps.

- Tener en cuenta los uplinks y backbones, y que la QoS son necesarias en redes de redes Enterprise y campus por el desarrollo aplicaciones que utilizan la red como video y voz.

3.16. Documentar el Diseño de Red

Tener en cuenta que el trabajo del diseñador de la red nunca se da por terminado, el proceso de análisis de requerimientos y desarrollo de soluciones empieza tan pronto el diseño esta implementado.

3.16.1. Responder a las solicitudes propuestas por la organización

- En el caso de que exista listas de solicitudes “RFP Request for proposal” responder las solicitudes en el mismo formato que especifica la RFP.

- Todas las RFP son distintas pero por lo general incluyen:

  - Metas de negocio del proyecto
  - Ámbito del proyecto
  - Información de la red actual y de las aplicaciones
  - Información de nuevas aplicaciones
  - Requerimientos técnicos incluyendo escalabilidad, disponibilidad, performance, seguridad, capacidad de administración, usabilidad, adaptabilidad y asequibilidad
  - Garantía de los productos
  - Restricciones del entorno o de arquitectura que pueden dificultar la implementación
  - Requerimientos de soporte y de entrenamiento
  - Programación preliminar con hitos y entregables
  - Términos y condiciones

- Además respuestas a las RFP deben incluir:

  - Topología de red del nuevo diseño
  - Información de protocolos, tecnologías y productos que componen el diseño
  - Un plan de implementación

- Opciones de precios y pagos
- Calificaciones del vendor y del distribuidor
- Recomendaciones de terceros que fueron atendidos por el distribuidor
- Términos y condiciones

3.16.2. Contenido del documento del diseño de red

- De no tener RFP especificas o cuando los requerimientos de la organización son respuestas en RFP básicos, se debe escribir el documento del diseño que describe completamente el diseño de la red. El documento debe incluir los componentes del diseño lógico y físico. En los siguientes puntos se detallara los temas que deben ser incluidos.

3.16.2.1. Resumen del proyecto

- Incluye los puntos principales del documento.
- No debe ser de más de una página y debe ser dirigido a managers y participantes clave del proyecto quienes decidirán si aprueban el diseño propuesto.
- La información técnica debe ser resumida y organizada en función a la prioridad de los objetivos del proyecto de diseño.

3.16.2.2. Metas del proyecto

- Enfocarse en la meta principal del diseño de red.
- Debe ser orientado al negocio y relacionado al objetivo total.
- No debe ser de más de un párrafo.

3.16.2.3. Ámbito

- Provee el resumen de los departamentos y redes que serán afectadas por el proyecto.
- Nuevas redes o modificaciones para una solo segmento de red, un conjunto de LANs, una red de edificio o de campus, un conjunto de WAN o redes remotas o la red Enterprise total.

3.16.2.4. Requerimientos de diseño

- Listar todos los requerimientos técnicos y de negocio para el diseño de red.
- Las metas de requerimientos de diseño deben listarse en orden de prioridad.

3.16.2.4.1. Metas de Negocio

- Implica como la organización se beneficiara para proveer mejores productos y servicios a sus clientes.
- Tener en cuenta la forma de cómo resolver problemas reales del negocio y plasmarla en el diseño y las metas.

3.16.2.4.2. Metas técnicas

- Escalabilidad: cuanto crecimiento puede soportar.
- Disponibilidad: tiempo de actividad estable de la red, tener en cuenta el costo por caída de red.
- Performance: Throughput, precisión, eficiencia, retardo, jitter y tiempo de respuesta.
- Seguridad: capacidad de operación normal sin verse afectada por interferencia de intrusos que puedan acceder al equipamiento o la data.

- Capacidad de Administración: para medir y monitorear performance, fallas, configuraciones, seguridad y contabilización.
- Usabilidad: la facilidad con la que un usuario puede tener acceso a la red, direccionamiento, nombramiento, y acceso a recursos.
- Adaptabilidad: a fallas de red, cambiar patrones de tráfico, requerimientos de negocio o técnicos.
- Asequibilidad: información general de costo de equipamiento de red y operación de la red.

3.16.2.4.3. Comunidades de usuario y data-stores (servidores)

- Listar las comunidades de usuario incluyendo su tamaño, ubicación y aplicaciones principales que utiliza.
- Listar los data-stores, servidores o host y sus ubicaciones.

3.16.2.4.4. Aplicaciones de red

- Listar e identificar las nuevas y existentes aplicaciones de red.

3.16.2.5. Estado actual de la red

- Describe la estructura y performance de la red actual. Debe incluir un mapa de red que identifique la ubicación de los principales dispositivos de red, procesamiento de data, dispositivos de almacenamiento y segmentos de red además de incluir direcciones y nombres.
- Para redes amplias se debe tener dos o tres mapas.
- Mapas muy detallados se deben incluir en apéndices y no en esta sección.

- Debe incluir componentes del diseño lógico y físico como VPN, Firewall, LAN, VLANS, servidores entre otros.
- Los dibujos de red deben indicar si existe jerarquía o plana, estructurada o no, en capas o no. Además debe indicar la geometría de la red como estrella, anillo, bus, Mesh.
- Resumir el direccionamiento y el nombramiento asignado.

3.16.2.6. Diseño lógico

- Topología de red: incluir uno o varios dibujos que ilustren la arquitectura lógica de la red.
- El modelo para direccionamiento de segmentos de red y dispositivos de red.
- El modelo para el nombramiento de dispositivos de red.
- La lista de todos los protocolos de switching y routing que fueron seleccionados para la implementación.
- Mecanismos y productos de seguridad recomendados, incluyendo un resumen de políticas y procedimientos de seguridad.
- Productos, procesos y arquitecturas de administración recomendados.
- Diseño racional indicando porque se eligieron varias opciones, en función de las metas de la organización y de la red actual.

3.16.2.7. Diseño físico

- Describir las características y recomendaciones de uso para las tecnologías y dispositivos que se seleccionó durante el diseño.
- Puede incluir información acerca de la red de campus, acceso remoto, conexión WAN y también el/los proveedores WAN seleccionados.
- De ser necesario y si la organización lo solicita el diseño físico debe incluir información acerca de precios de dispositivos de red y

servicios. Tener en cuenta que los precios son negociables y no es recomendado incluirlo en solución propuesta.

- También debe incluir información acerca de la disponibilidad de los productos, para ver la disponibilidad de los equipos indicando si están en stock, en proceso de envío y cuánto tiempo toma el proceso de envío.

3.16.2.8. Resultados de las pruebas de diseño de red

- En esta sección describir los resultados que las pruebas que se realizaron para verificar el diseño de red.
- Es uno de los puntos más importantes porque aquí se comprueba que el diseño cumplirá todos sus requerimientos.
- En las pruebas con implementaciones piloto o prototipo se obtiene lo siguiente:
  - Objetivos de la prueba
  - Criterio de aceptación de la prueba
  - Herramientas para la prueba
  - Scripts para la prueba
  - Resultados y observaciones

- En el punto de resultados y observaciones, incluir alguna técnica de optimización que usted recomendé para su aplicación para cumplir con los requerimientos.

3.16.2.9. Apéndice y anexos de diseño

- La mayoría de documentos de diseño de red incluyen uno o más apéndices que presentan información suplementaria al diseño e implementación.
- Puede incluir mapas de topología detallada, configuraciones de dispositivos, direccionamiento de red y detalles de nombramiento, y resultados compresivos de las pruebas del diseño de red.

Capítulo 4

Implementación de la red de campus de la UCSM

4.1. Resumen del proyecto

El proyecto ha sido diseñado tomando en cuenta los requerimientos analizados por la UNIVERSIDAD CATÓLICA DE SANTA MARIA es importante mencionar que la solución busca maximizar el impacto positivo sobre los procesos de negocios sin disminuir la calidad del servicio y no tener ningún impacto en la red.

En el actual ambiente de negocios cada vez más complejo, la red se enfrenta a nuevos retos y debe ofrecer más servicios necesarios para su óptimo funcionamiento. Las aplicaciones y la infraestructura de red de switches que los transportan, son herramientas fundamentales para mejorar la productividad del usuario y aumentar la capacidad de una organización para crecer y seguir siendo competitivos. Es por esto que la UCSM debe optimizar su red de datos.

Actualmente las organizaciones están invirtiendo en proporcionar un mayor acceso a las aplicaciones avanzadas a lo largo de toda su geografía extendida, creando una nueva demanda de infraestructura de red, incluyendo requerimientos como:

- Mayor capacidad en las redes de switches para soportar la demanda de ancho de banda de las aplicaciones.
- Soporte de nuevos servicios convergentes como: la telefonía IP, voz sobre redes LAN y WLAN, y servicios de vídeo.
- Alta disponibilidad y el acceso ininterrumpido a la información y a las aplicaciones de la empresa.
- Mayor protección contra amenazas de seguridad internas y externas.
- Soluciones más manejables para los administradores de TI, buscando reducir el costo y la complejidad de la red de switches.

La diferencia operativa entre los niveles de personal de TI y los requisitos que las empresas están poniendo en sus redes sigue creciendo. Las organizaciones

deben utilizar los switches con funciones inteligentes y más funcionalidad para:

- Garantizar la disponibilidad de las aplicaciones.
- Permitir una mayor simplicidad en términos automatización de las tediosas tareas de TI

Proporcionar una nueva funcionalidad para permitir a las personas a obtener el máximo valor de sus aplicaciones

4.2. Metas del proyecto

La meta principal del proyecto es iniciar y expandir la renovación tecnológica de infraestructura de redes de la Universidad Católica de Santa Maria hacia las redes convergentes, donde se podrá convivir en un entorno de data, video y voz bajo una misma arquitectura. Además con esto se quiere lograr que el acceso a internet y a la información de la organización se encuentre al alcance de los usuarios finales.

4.3. Ámbito

El proyecto comprende el rediseño físico y lógico todas las áreas que se encuentran en el Campus principal Urb. San Jose s/n y Campus Esclavas.

Las Áreas involucradas son:

- Unidad Administrativa Rectorado
- Unidad Administrativa Vicerrectorado Académico
- Unidad Administrativa Vicerrectorado Administrativo
- Unidades Académicas:
    - Área Administrativa
    - Área Académica
- Organismos Autónomos

- Representaciones Gremiales y Académicas
- Otros Organismos

Los servicios que se tomaran en cuenta:

- Data Center
  - Servidores
  - Hardware
- Comunicaciones
  - Telefonía IP, futura implementación
- Video
  - Video IP

4.4. Requerimientos de diseño

4.4.1. Metas de Negocio

La Universidad Católica de Santa Maria (UCSM) en continua mejora de sus servicios a sus estudiantes, visitantes y trabajadores docentes y administrativos tiene como misión cumplir las siguientes metas:

- Mejorar la eficiencia en sus diversas facultades para participar en proyectos de investigación con otras instituciones.
- Mejorar la eficiencia en los estudiantes y eliminar problemas con la ejecución de tareas.
- Permitir a los alumnos y visitantes el acceso a internet desde su propia portable, Tablet, celular, etc, lo que se conoce como “BYOD” (Bring Your Own Device).
- Proteger la red e información de intrusos.
- Invertir el presupuesto asignado en tecnología de manera eficiente, el presupuesto debe ejecutarse hasta diciembre de cada año.

4.4.2. Metas técnicas

- Rediseño del direccionamiento IP.
- Incrementar el ancho de banda interno y de internet para soportar nuevas aplicaciones y expandir el uso de las aplicaciones actuales.
- Proveer seguridad a los usuarios que acceden a las redes de la organización por el medio cableado o inalámbrico.
- Proveer una red que ofrezca un tiempo de respuesta de aproximadamente 0.1 segundo o menos en aplicaciones interactivas.
- Proveer una red de campus que sea disponible 99.90% y que ofrezca un MTBF de 3000 horas (alrededor de 4 meses) y MTTR de 3 horas (Con una baja desviación estándar de estos números promedio) para aplicaciones publicadas.
- Proveer una red de campus que sea disponible 99.93% y que ofrezca un MTBF de 3000 horas (alrededor de 4 meses) y MTTR de 2 horas (Con una baja desviación estándar de estos números promedio) para aplicaciones internas.
- Proveer seguridad para proteger conexiones hacia internet y la red interna de intrusos.
- Utilizar herramientas de administración para incrementar la eficiencia y efectividad del área de TI.
- Proveer una red que pueda escalar y soportar una futura expansión de uso de aplicaciones de multimedia.

4.4.3. Comunidades de usuario y data-stores

4.4.3.1. Comunidades de usuario

➔ **Alumnos:** Es la comunidad de usuarios más amplia de la UCSM, alrededor de 12K a 14K alumnos matriculados por semestre, ingresantes cada año 2000, en su mayoría solo utilizan los laboratorios, aulas y redes inalámbricas.

- **Autoridades:** Es la comunidad de usuarios compuesta por Rector, Vicerrector Académico, Vicerrector Administrativo, son 3 en total, solo utilizan las computadoras asignadas a su persona y tienen acceso a todas las aplicaciones.

- **Decanos:** Es la comunidad de usuarios compuesta por los decanos de las diversas facultades de la UCSM, son 13 incluyendo al director de la Escuela de Postgrado, solo utilizan las computadoras asignadas a su persona y tienen acceso a los sistemas académicos.

- **Directores:** Es la comunidad de usuarios compuesta por los directores de los distintos programas profesionales de la UCSM, son 29, solo utilizan las computadoras asignadas a su persona y tienen acceso a los sistemas académicos.

- **Docentes:** Es la comunidad de usuarios de ingenieros, licenciados, magísteres, doctores de la UCSM, son alrededor 700, en su mayoría utilizan los laboratorios, aulas y redes inalámbricas.

- **Jefaturas:** Es la comunidad de usuarios que está compuesta por las personas que cumplen la labor de jefe o dirección de determinada área administrativa, son alrededor de 40, tienen acceso a su computador personal y a los sistemas que se les haya asignado acceso.

- **Personal Administrativo**

  Está compuesto por los siguientes grupos de usuarios:

- **Personal de procesos:** Es la comunidad de usuarios que realiza la parte transaccional y operativa de la UCSM, alrededor 100, en su mayoría utilizan los PCs de las áreas administrativas y redes inalámbricas.
- **Secretarias:** Es la comunidad de usuarios que realiza la labor operativa de la UCSM, alrededor 200, en su mayoría utilizan los PCs de las áreas administrativas y redes inalámbricas.
- **Servicio:** Es la comunidad de usuarios que realiza la labor de servicios varios de la UCSM, alrededor 100, en su mayoría utilizan los PCs de las áreas administrativas y redes inalámbricas.

➔ **Organizaciones:** Es la comunidad de usuarios que reside en la UCSM de acuerdo a la labor que desempeñen, en su mayoría utilizan los PCs según a la organización que pertenezcan.

➔ **Administradores de Dominio:** Es la comunidad de usuarios que administran el total de las computadoras de la UCSM, en su mayoría utilizan sus respectivos PCs y tienen acceso a las todas las áreas del dominio de organización.

➔ **Administradores de Servidores:** Es la comunidad de usuarios que administran los servidores de la UCSM, en su mayoría utilizan sus respectivos PCs y tienen acceso a de acuerdo al servidor que administren.

➔ **Administradores de Red:** Es la comunidad de usuarios que administran los dispositivos de red de la UCSM, en su mayoría utilizan sus respectivos PCs y tienen acceso a todos los dispositivos de red.

- **Administradores de Sistemas:** Es la comunidad de usuarios que administran los sistemas académicos y administrativos de la UCSM, en su mayoría utilizan sus respectivos PCs y tienen acceso total a los sistemas dependiendo del sistema que administren.

- **Soporte Técnico:** Es la comunidad de usuarios que da soporte técnico a los computadores de la UCSM, tienen acceso a los computadores de toda la organización en cuanto a aplicaciones tienen acceso a internet e intranet.

- **Operadores:** Es la comunidad de usuarios que da operan los sistemas de seguridad como cámaras o control de acceso.

Ítem	Comunidad de Usuario	Tamaño de la comunidad	Ubicación	Aplicaciones que utiliza la comunidad
1	**Alumnos**	12K-14K	Campus	Internet, Matriculas, Notas
2	**Autoridades**	3	Campus	Internet, Intranet, Sistemas Académicos, Administrativos, Intranet
3	**Decanos**	13	Campus	Internet, Sistemas Académicos, Intranet
4	**Directores**	29	Campus	Internet, Sistemas Académicos, Intranet
5	**Docentes**	700	Campus	Internet, Notas, Intranet
6	**Jefaturas**	40	Campus	Internet, Sistemas Académicos, Administrativos, Intranet
7	**Personal Administrativo**	300	Campus	Internet, Sistemas Académicos, Administrativos, Intranet
8	**Secretarias**	200	Campus	Internet, Sistemas Académicos, Administrativos, Intranet
9	**Organizaciones**	20	Campus	Internet, Intranet
10	**Administradores de Dominio**	2	Informática	Todas
11	**Administradores de Servidores**	2	Informática	De acuerdo a la aplicación
12	**Administradores de red**	1	Informática	De acuerdo a la aplicación
13	**Administradores de sistemas**	6	Informática	De acuerdo a la aplicación
14	**Soporte**	4	Informática	Internet, Intranet
15	**Operadores**	4	Informática	De acuerdo a la aplicación

Tabla 4.4-1: Comunidades de Usuarios
Fuente: Elaboración Propia

4.4.3.2. Data-Stores

➔ **Data Store publicados**

- **Data Store 1 SVRWWW01:** Brinda el servicio de portal web, está basado en Linux Centos 6.4 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R720
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 2 SVRMYS01:** Brinda acceso a las bases de datos que utilizan el portal web, aula virtual, Cybertesis entre otras, está basado en Linux Centos 6.4 de 64 bits. Actualmente se encuentra en migración y operara bajo el siguiente hardware:

  - Servidor: Dell Poweredge R720
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 3 SVRIIS01:** Brinda el servicio de sistema de matrículas y notas, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R710
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 4 SVRAULA01:** Brinda el servicio de aula virtual, está basado en Linux Centos 6.4 de 64 bits. Actualmente se encuentra en migración y operara bajo el siguiente hardware:

  - Servidor: Dell Poweredge R710
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 5 SVRRADIO01:** Brinda el servicio de radio, está basado en Linux Centos 6.4 de 64 bits. Actualmente se encuentra operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV 2008R2
  - Procesador: 2 procesadores virtuales
  - RAM: 2 GB RAM

- **Data Store 6 SVRBIBLIOTECA02:** Brinda el servicio de Cybertesis, está basado en Windows Server 2008 R2 de 64 bits. Actualmente se encuentra operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV 2008R2
  - Procesador: 4 procesadores virtuales
  - RAM: 8 GB RAM

- **Data Store 7 SVRCICA01:** Brinda el servicio del CICA, está basado en Windows Server 2008 R2 de 64 bits. Actualmente se encuentra operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV 2008R2
  - Procesador: 2 procesadores virtuales
  - RAM: 2 GB RAM

- **Data Store 8: SVRPROY01:** Brinda el servicio de portal web de proyectos especiales, está basado en Linux Centos 6.4 de 64 bits. Actualmente se encuentra en migración y operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV 2008R2
  - Procesador: 4 procesadores virtuales
  - RAM: 8 GB RAM

- **Data Store 9 SVRACAD01:** Brinda el servicio de aplicaciones de las diversas facultades, está basado en Windows Server 2008 R2 de 64 bits. Actualmente se encuentra operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV 2008R2
  - Procesador: 4 procesadores virtuales
  - RAM: 4 GB RAM

Ítem	Data Store	Ubicación	Aplicación	Comunidad(es) de Usuario
1	**Centos 6.4 - SVRWWW**	Data Center - Granja Servidores DMZ	Portal Web	Todas
2	**Centos 6.4 - SVRMYS01**	Data Center - Granja Servidores DMZ	Portal Web	Aplicaciones, Administradores
3	**W2008R2 - SVRIIS01**	Data Center - Granja Servidores DMZ	Matriculas Notas	Alumnos, Docentes
4	**Centos 6.4 - SVRAULA01**	Data Center - Granja Servidores DMZ	Aula Virtual	Alumnos, Docentes
5	**Centos 6.4 - SVRRADIO01**	Data Center - Granja Servidores DMZ	Radio	Todas
6	**W2008R2 - SVRBIBLIOTECA02**	Data Center - Granja Servidores DMZ	Cybertesis	Alumnos, Docentes, Administrativos
7	**W2008R2 - SVRCICA01**	Data Center - Granja Servidores DMZ	CICA	Todas
8	**Centos 6.4 - SVRPROY01**	Data Center - Granja Servidores DMZ	Proyectos	Todas
9	**W2008R2 - SVRACAD01**	Data Center - Granja Servidores DMZ	Aplicaciones Académicas	Alumnos, Docentes

Tabla 4.4-2: Data Stores Publicados
Fuente: Elaboración Propia

➔ **Data Store internos**

- **Data Store 1: SVRDC01, SVRDC02:** Brinda el servicio de sistema de Active Directory el cual se encuentra replicado, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R710
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 2 SVRFS01:** Brinda el servicio de sistemas Académicos y Administrativos en Fox, Btrieve, por medio de un servidor de archivos, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R710
  - Procesador: 2 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 3: SVRCORPORATE01:** Brinda el servicio del sistemas Calipso Corporate, por medio de un terminal server, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R720
  - Procesador: 2 Intel E52630 Xeon
  - RAM: 32 GB RAM

- **Data Store 4: SVRDB01:** Brinda el servicio de base de datos a las diversas aplicaciones que lo requieran, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R910
  - Procesador: 4 Intel E74830 Xeon
  - RAM: 64 GB RAM

- **Data Store 5: SVRBIBLIOTECA01:** Brinda el servicio de base de datos a las diversas aplicaciones de la biblioteca, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 8 GB RAM

- **Data Store 6 SVRTS01:** Brinda el servicio del sistemas Académicos, por medio de un terminal server, está basado en Windows Server 2008R2 de 64 bits. Actualmente se encuentra en migración y operara bajo el siguiente hardware:

  - Servidor: Dell Poweredge R720
  - Procesador: 2 Intel E52630 Xeon
  - RAM: 32 GB RAM

- **Data Store 7: SVRTD01:** Brinda el servicio de intranet, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 8 GB RAM

- **Data Store 8 SVRSCM01:** Brinda el servicio de configuración y monitoreo de las PCs en dominio de la UCSM, está basado en Windows Server 2008R2 de 64 bits. Actualmente se encuentra en implementación y operara bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 8 GB RAM

- **Data Store 9 SVR0001/SVR0002:** Brinda el servicio de actualizaciones y licencias, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 4 GB RAM

- **Data Store 10 SVRMGMT01:** Brinda el servicio de administración de red, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R310
  - Procesador: 1 Dell X3430
  - RAM: 4 GB RAM

- **Data Store 11 SVRBACKUP01:** Brinda el servicio de backup, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 4 GB RAM

- **Data Store 12 SVRVIDEO01:** Brinda el servicio de gestión y monitoreo de cámaras IP, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Dell Poweredge R410
  - Procesador: 1 Intel E5620 Xeon
  - RAM: 32 GB RAM

- **Data Store 13: SVRAC01:** Brinda el servicio de control de accesos, está basado en Windows Server 2008R2 de 64 bits. Actualmente operativo bajo el siguiente hardware:

  - Servidor: Virtual HyperV R2
  - Procesador: 4 procesadores virtuales
  - RAM: 4 GB RAM

- **Data Store 14: FORTIGATE 621B: Brinda** el servicio de internet y seguridad a la UCSM, está basado en un appliance marca FORTINET modelo FORTIGATE 621B.

Ítem	Data Store	Ubicación	Aplicación	Comunidad(es) de Usuario
1	**W2008R2 - SVRDC01,02**	Data Center - Granja Servidores Internos	Active Directory	Todas
2	**W2008R2 - SVRFS01**	Data Center - Granja Servidores Internos	File Server	Alumnos, Docentes
3	**W2008R2 - SVRCORPORATE01**	Data Center - Granja Servidores Internos	ERP	Alumnos, Docentes
4	**W2008R2 - SVRDB01**	Data Center - Granja Servidores Internos	Base Datos	Aplicaciones, Administradores
5	**W2008R2 - SVRBIBLIOTECA01**	Data Center - Granja Servidores Internos	Base Datos	Aplicaciones, Administradores
6	**W2008R2 - SVRTS01**	Data Center - Granja Servidores Internos	Sistemas Académicos	Todas
7	**W2008R2 - SVRTD01**	Data Center - Granja Servidores Internos	Intranet	Alumnos, Docentes, Administrativos
8	**W2008R2 - SVRSCM01**	Data Center - Granja Servidores Internos	Administración Infraestructura	Administradores de dominio
9	**Centos 6.4 - SVR0001/SVR0002**	Data Center - Granja Servidores Internos	Licencias Actualizaciones	Administradores de Servidores
10	**W2008R2 - SVRMGMT01**	Data Center - Granja Servidores Internos	Adminis. de red	Administradores de Red
11	**W2008R2 - SVRBACKUP01**	Data Center - Granja Servidores Internos	Backup	Administradores de Servidores
12	**W2008R2 - SVRVIDE01**	Data Center - Granja Servidores Internos	Cámaras IP	Administradores de Red
13	**W2008R2 - SVRAC01**	Data Center - Granja Servidores Internos	Control de Acceso	Administradores de Servidores
14	**FORTIGATE 621B**	Data Center - Granja Servidores Internos	Internet	Administradores de Red

Tabla 4.4-3: Data Stores Internos
Fuente: Elaboración Propia

4.4.4. Aplicaciones de red

La descripción de las aplicaciones que se presentaran en este punto está graficada de acuerdo al diseño propuesto.

➔ **Aplicaciones Publicadas**

- **Aplicación 1: Portal**

  El entorno de la institución ingresa al portal web para ver el contenido de la información colgada, además es utilizado como pasarela para el acceso a sistema de matrículas, notas, aula virtual, entre otros.

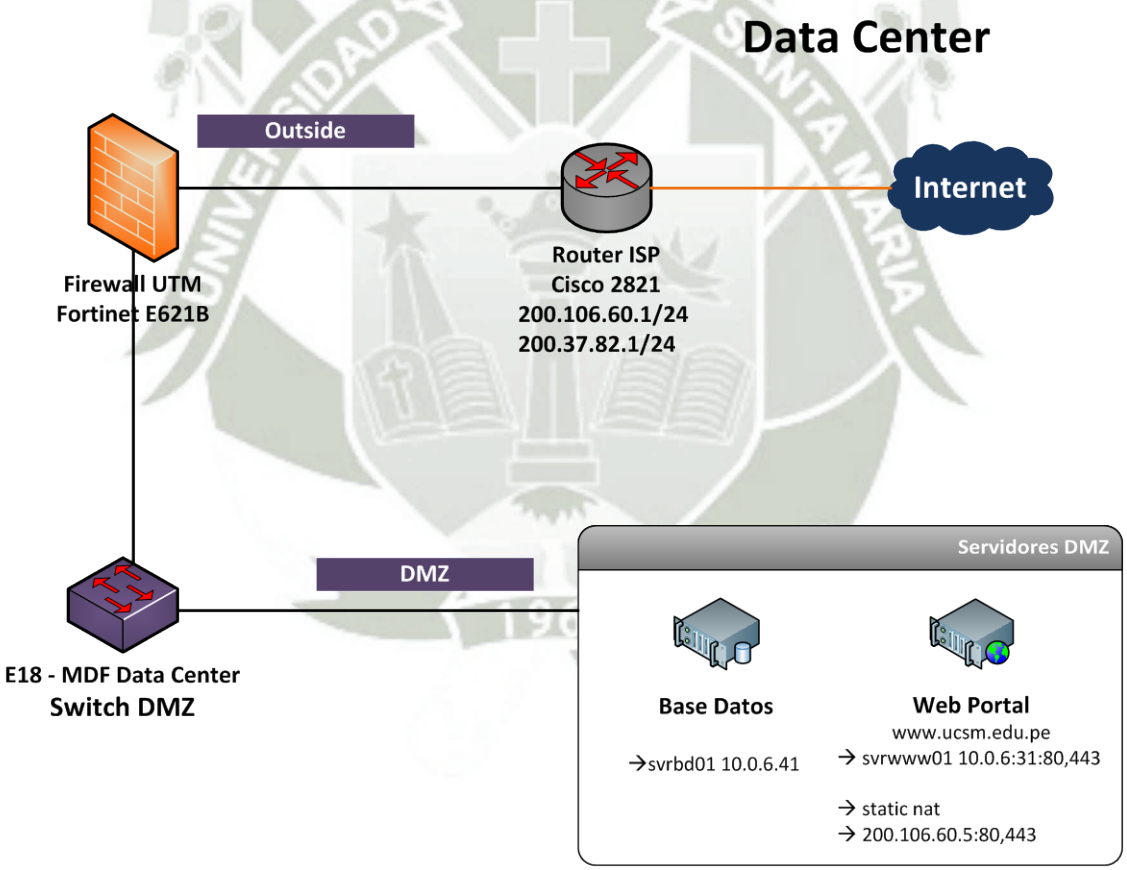

Figura 4.4-5: Aplicación Publicada 1
Fuente: Elaboración Propia

- **Aplicación 2: Base Datos**

  Las aplicaciones del portal web, aula virtual y biblioteca se conectan a la base de datos para el correcto funcionamiento de la aplicación.

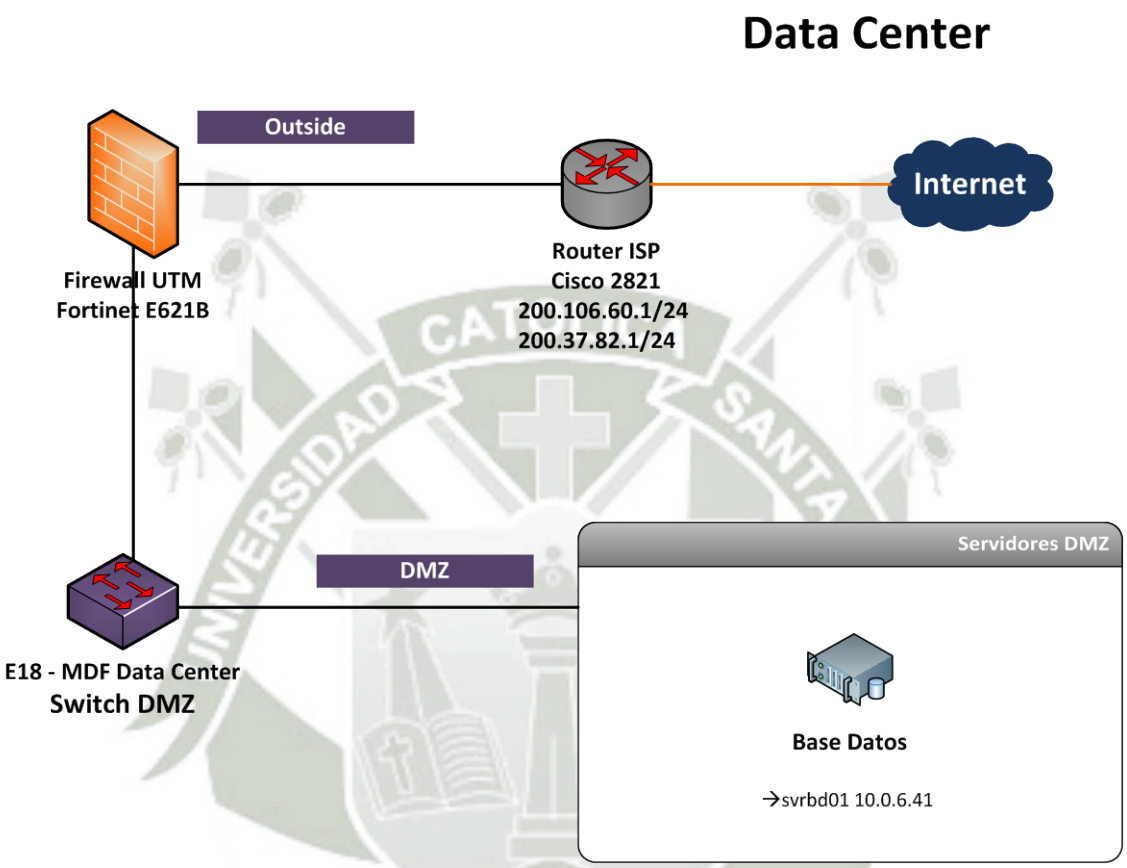

Figura 4.4-2: Aplicación Publicada 2
Fuente: Elaboración Propia

- **Aplicación 3: Matriculas y Notas Online**

  Docentes, estudiantes de pregrado, postgrado y otras especialidades utilizan el sistema para realizar transacciones que les corresponda.

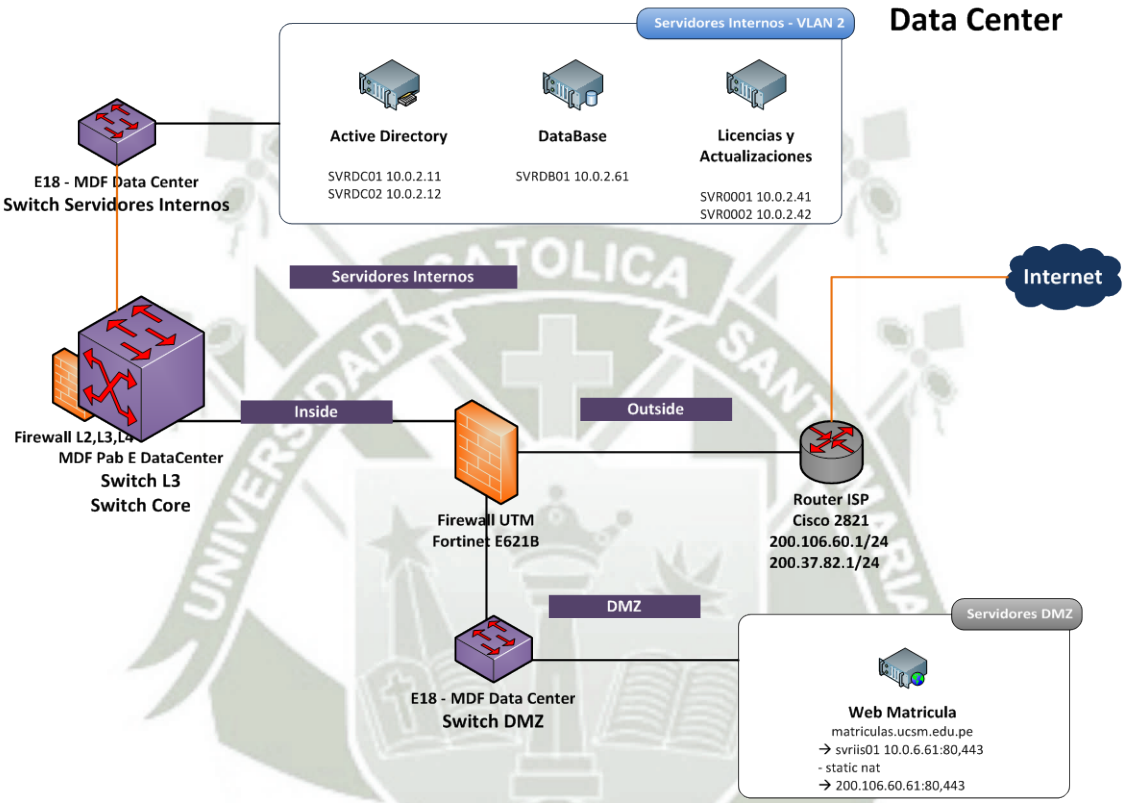

Figura 4.4-3: Aplicación Publicada 3
Fuente: Elaboración Propia

- **Aplicación 4: Aula Virtual**

  Docentes, estudiantes de pregrado, postgrado y otras especialidades utilizan el sistema para acceder a los contenidos y clases virtuales.

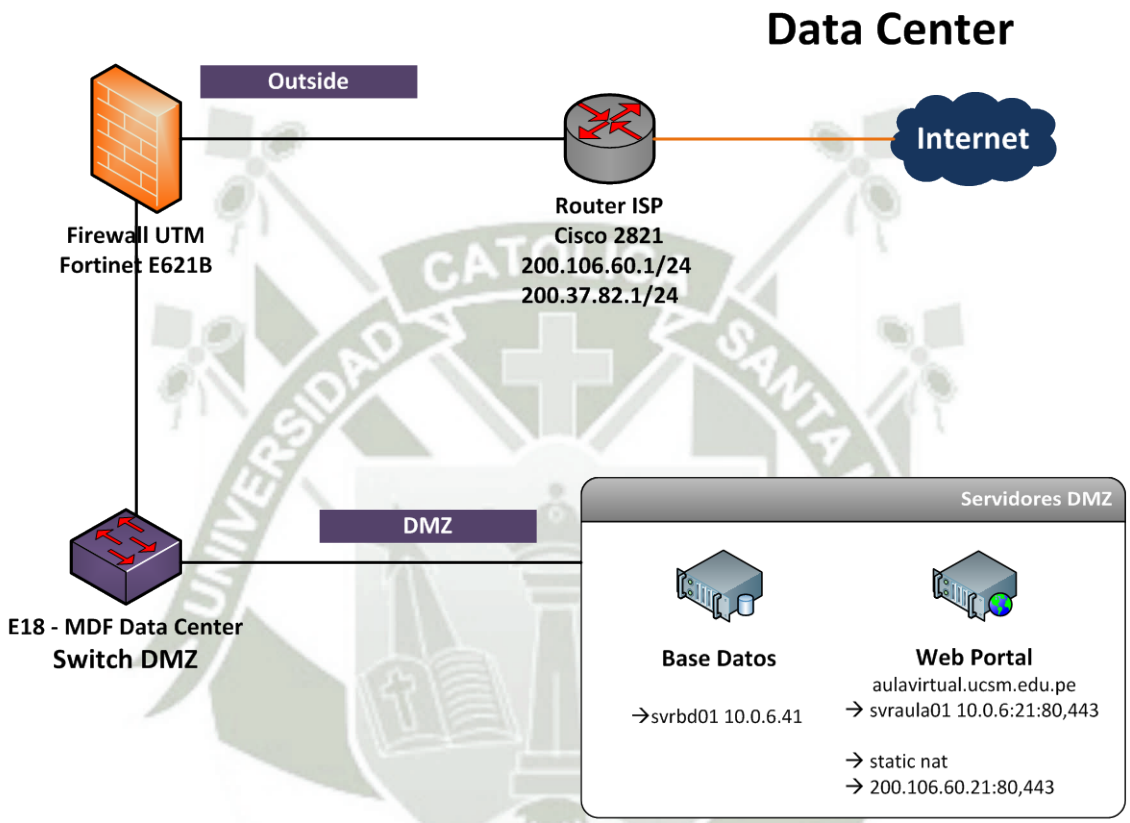

Figura 4.4-4: Aplicación Publicada 4
Fuente: Elaboración Propia

- **Aplicación 5: Radio**

  El entorno de la institución y público en general puede ingresar al portal de la radio UCSM para escuchar las transmisiones que realiza la radio de la institución.

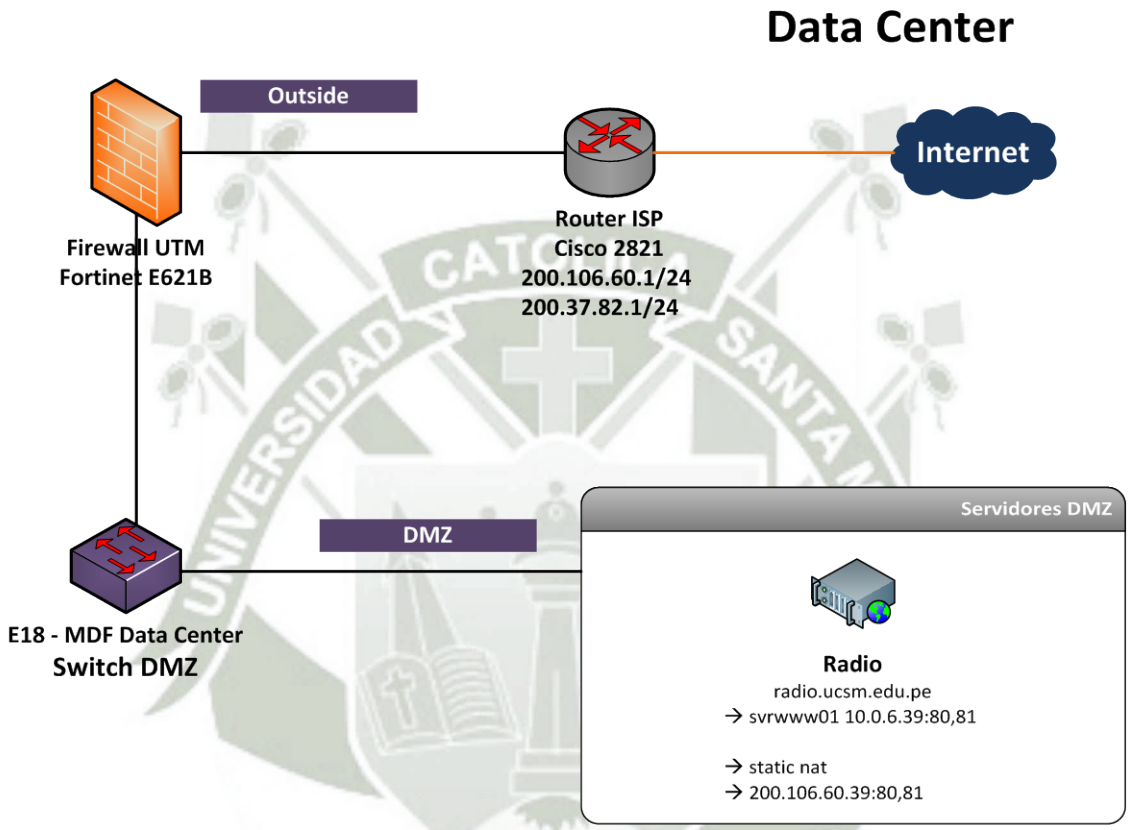

Figura 4.4-5: Aplicación Publicada 5
Fuente: Elaboración Propia

- **Aplicación 6: Cybertesis Biblioteca**

  Docentes, estudiantes de pregrado, postgrado, otras especialidades y público acreditado utilizan el sistema para acceder a los contenidos de tesis publicadas.

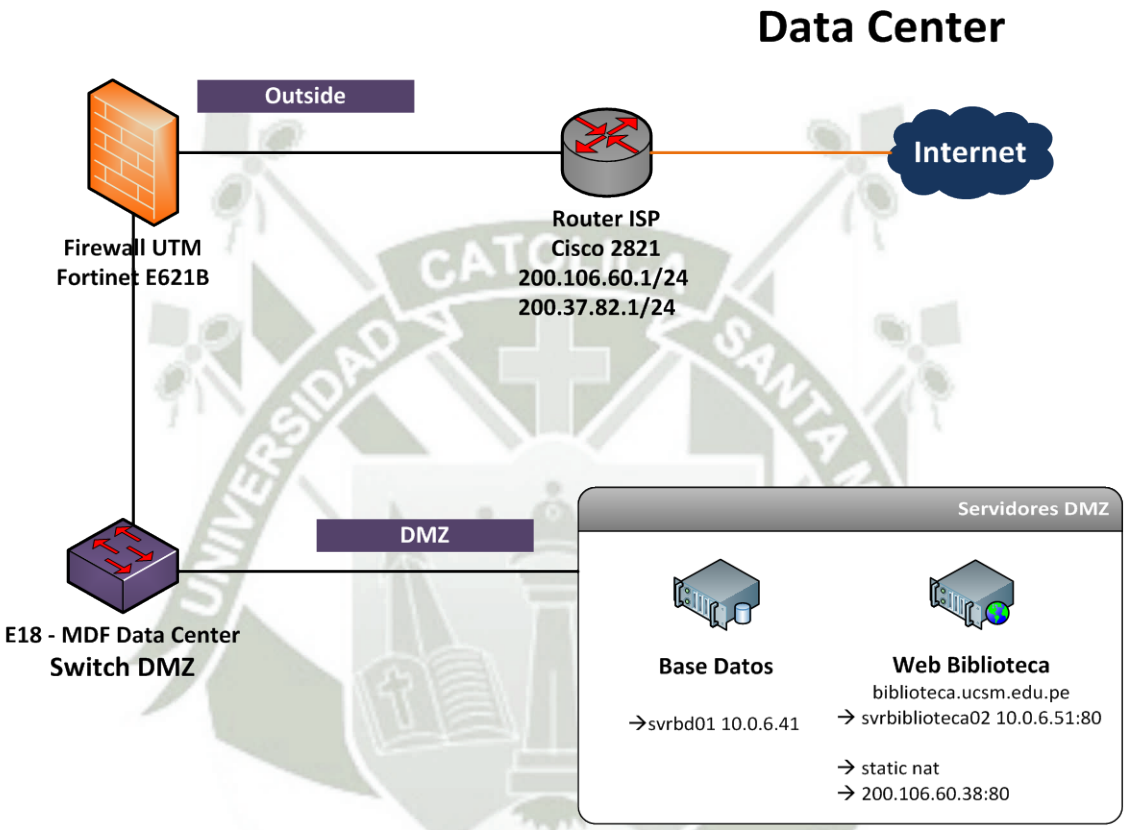

Figura 4.4-6: Aplicación Publicada 6
Fuente: Elaboración Propia

- **Aplicación 7: Investigación CICA**

  El entorno de la institución ingresa al portal web del CICA para ver el contenido de la información colgada, investigaciones realizadas o en curso, entre otras acciones.

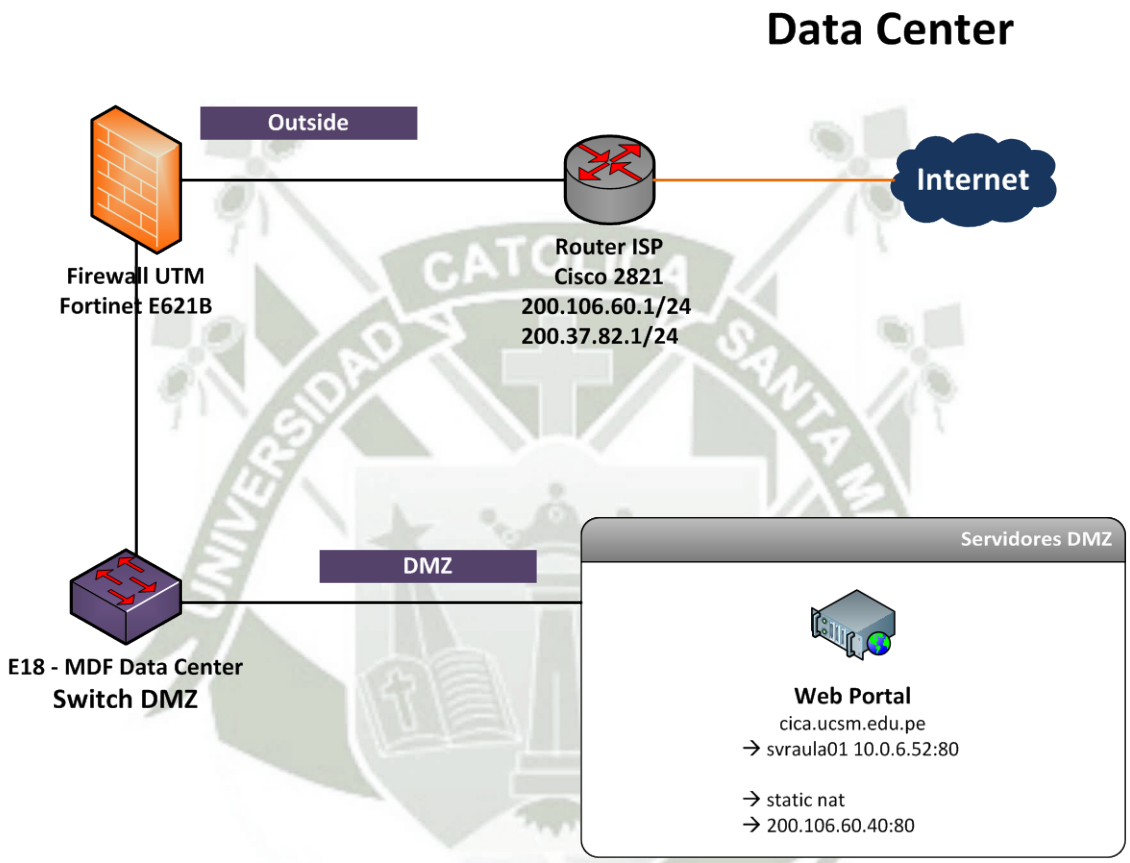

Figura 4.4-7: Aplicación Publicada 7
Fuente: Elaboración Propia

- **Aplicación 8: Proyectos Especiales**

  El entorno de la institución ingresa al portal web del CICA para ver el contenido de la información colgada, investigaciones realizadas o en curso, entre otras acciones.

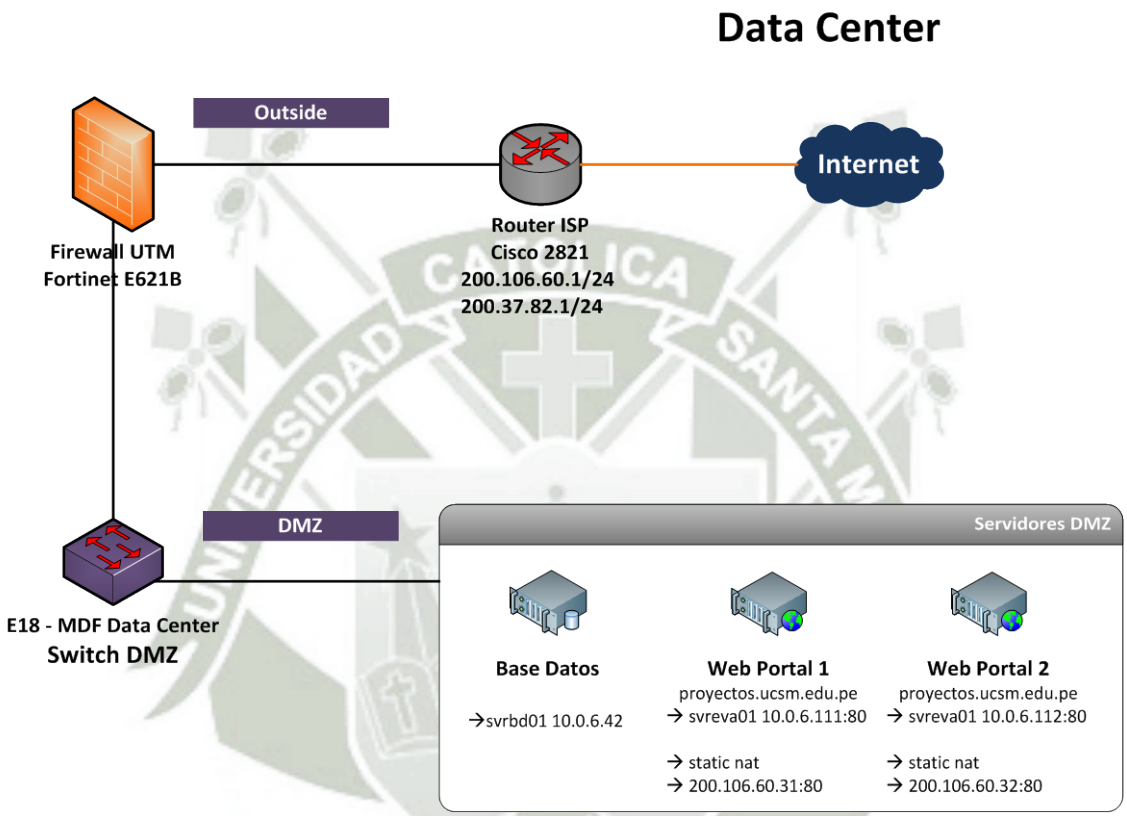

Figura 4.4.8: Aplicación Publicada 8
Fuente: Elaboración Propia

- **Aplicación 9: Aplicaciones Académicas**

  Docentes, estudiantes de pregrado, postgrado y otras especialidades utilizan el sistema para acceder a los contenidos como simuladores, acceso a sistemas transaccionales, entre otros.

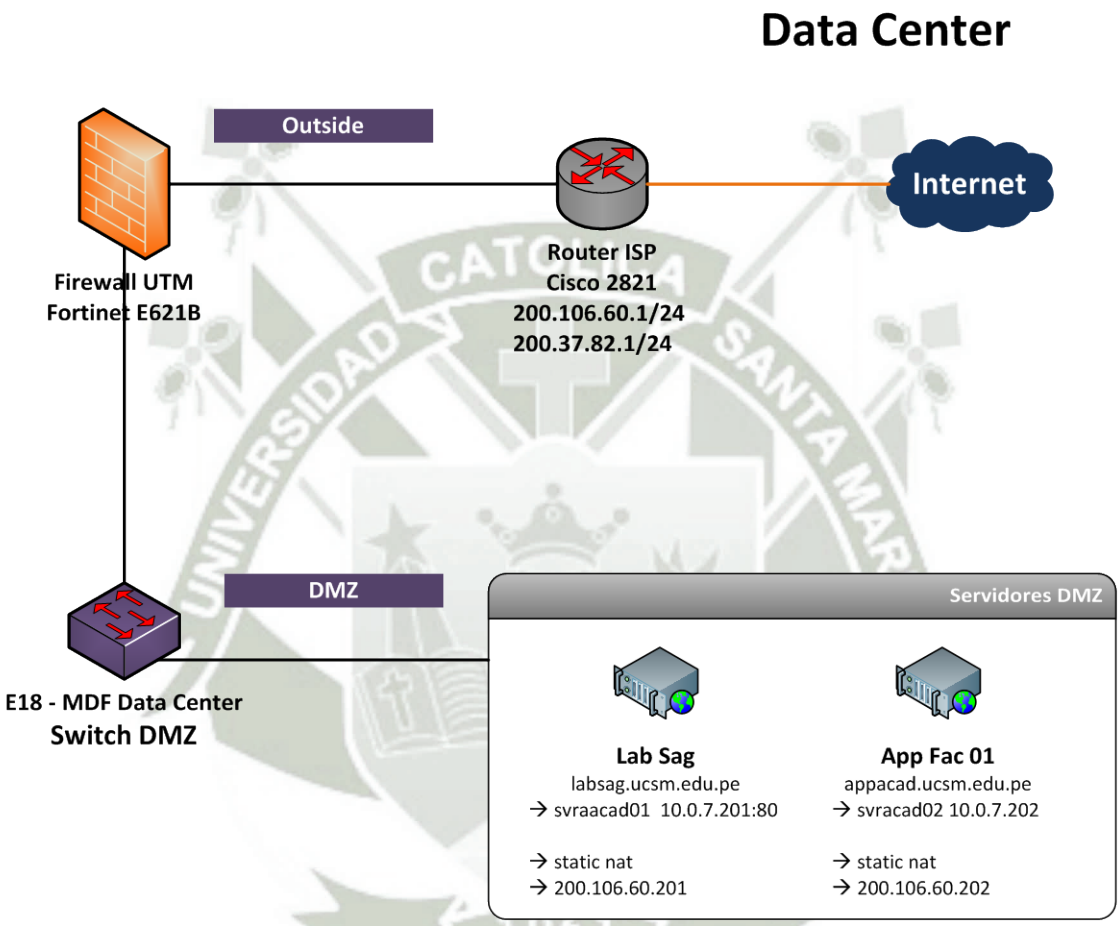

Figura 4.4-9: Aplicación Publicada 9
Fuente: Elaboración Propia

Ítem	Nombre aplicación	Tipo de aplicación	¿Aplicación Nueva?	Criticidad	Costo de fuera de servicio	MTBF aceptable
Publicadas						
1	**Portal**	Web	No	Alta	Alto	3 horas
2	**Base Datos**	SQL	No	Alta	Alto	3 horas
3	**Matrículas y Notas Online**	Web	Si	Alta	Alto	3 horas
4	**Aula Virtual**	Web	No	Alta	Alto	3 horas
5	**Radio**	Web	No	Media	Media	3 horas
6	**Cybertesis**	Web	Si	Media	Media	3 horas
7	**CICA**	Web	Si	Media	Media	3 horas
8	**Proyectos Especiales**	Web	Si	Alta	Alta	3 horas
9	**Aplicaciones Académicas**	Web	Si	Media	Media	3 horas

Tabla 4.4-4: Aplicaciones Publicadas
Fuente: Elaboración Propia

Ítem	Nombre aplicación	Tipo de flujo	Protocolos utilizados	Comunidades de usuario	Ancho de banda requerido	Req QoS
Publicadas						
1	**Portal**	Cliente servidor	HTTP, HTTPS	Todas	Nube: 24 Mbps Interno: 200 Mbps	qp3
2	**Base Datos**	Servidor Servidor	TCP 3306	Administradores	Nube: 0 Mbps Interno: 1 Gbps	qp3
3	**Matriculas y Notas Online**	Cliente servidor	HTTP, HTTPS	Alumnos, Docentes, Administrativos, Administradores	Nube: 24 Mbps Interno: 1 Gbps	qp3
4	**Aula Virtual**	Cliente servidor	HTTP	Alumnos, Docentes, Administradores	Nube: 24 Mbps Interno: 200 Mbps	qp3
5	**Radio**	Cliente servidor	HTTP	Todas	Nube: 8 Mbps Interno: 10 Mbps	qp3
6	**Cybertesis**	Cliente servidor	HTTP	Alumnos, Docentes, Administradores	Nube: 8 Mbps Interno: 100 Mbps	qp3
7	**CICA**	Cliente servidor	HTTP	Alumnos, Docentes, Administradores	Nube: 8 Mbps Interno: 10 Mbps	qp3
8	**Proyectos Especiales**	Cliente servidor	HTTP	Todas	Nube: 16 Mbps Interno: 100 Mbps	qp3
9	**Aplicaciones Académicas**	Cliente servidor	HTTP, FTP	Alumnos, Docentes, Administradores	Nube: 8 Mbps Interno: 100 Mbps	qp2

Tabla 4.4-5: Aplicaciones Publicadas Detalle
Fuente: Elaboración Propia

➔ **Aplicaciones Internas**

- **Aplicación 1: Active Directory**

Docentes, estudiantes de pregrado, postgrado, otras especialidades, trabajadores administrativos utilizan el AD para la autenticación, autorización y contabilización de acceso hacia cualquier dispositivo, unidad de red, recurso remoto que se encuentre dentro de la UCSM. Además cumple con el servicio de DNS interno para la resolución de nombres.

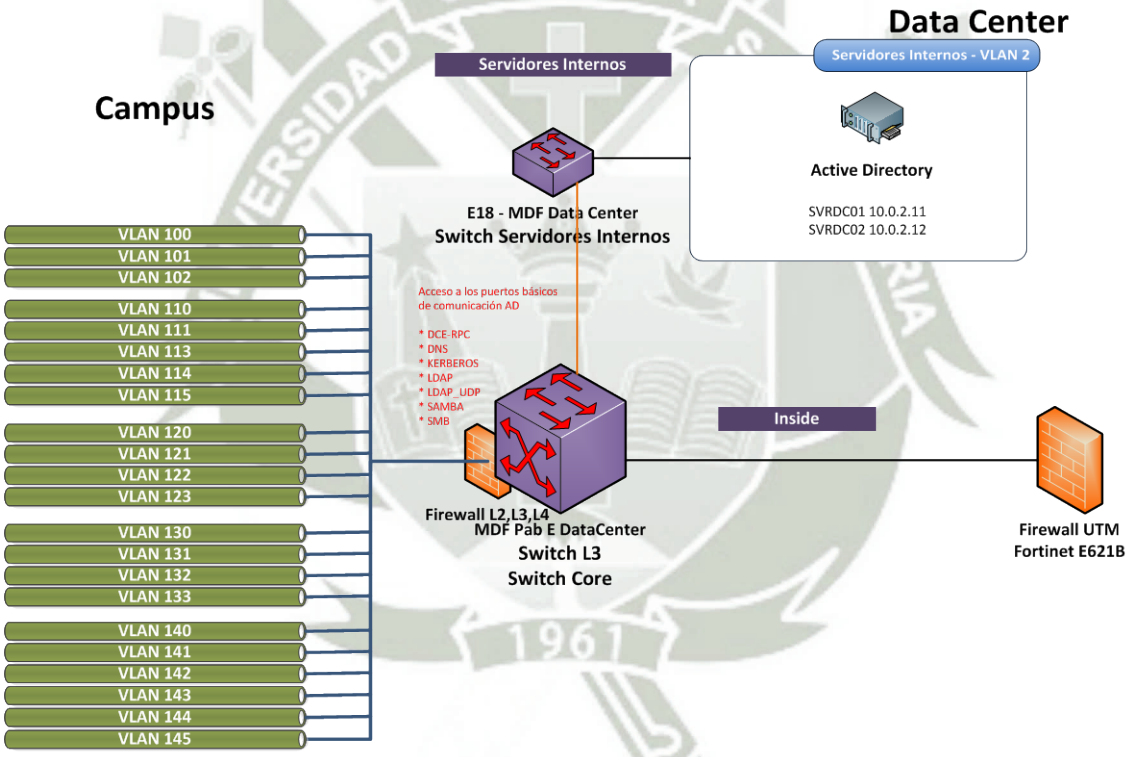

Figura 4.4-10: Aplicación Internas 1
Fuente: Elaboración Propia

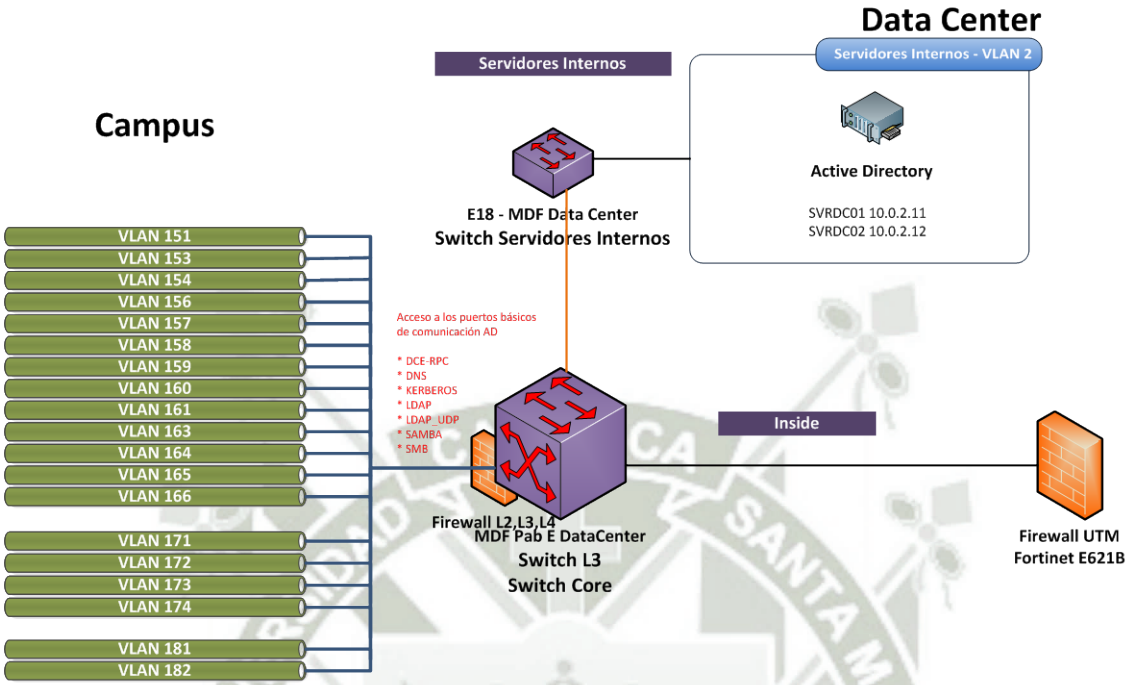

Figura 4.4-11: Aplicación Internas 1'
Fuente: Elaboración Propia

- **Aplicación 2: File Server, Sistemas Académico, Biblioteca y Administrativos**

  Trabajadores administrativos, docentes utilizan los sistemas publicados en el Windows File Server para realizar las transacciones que se les haya encomendado, pueden ser las unidades administrativas de la UCSM, unidades académicas.

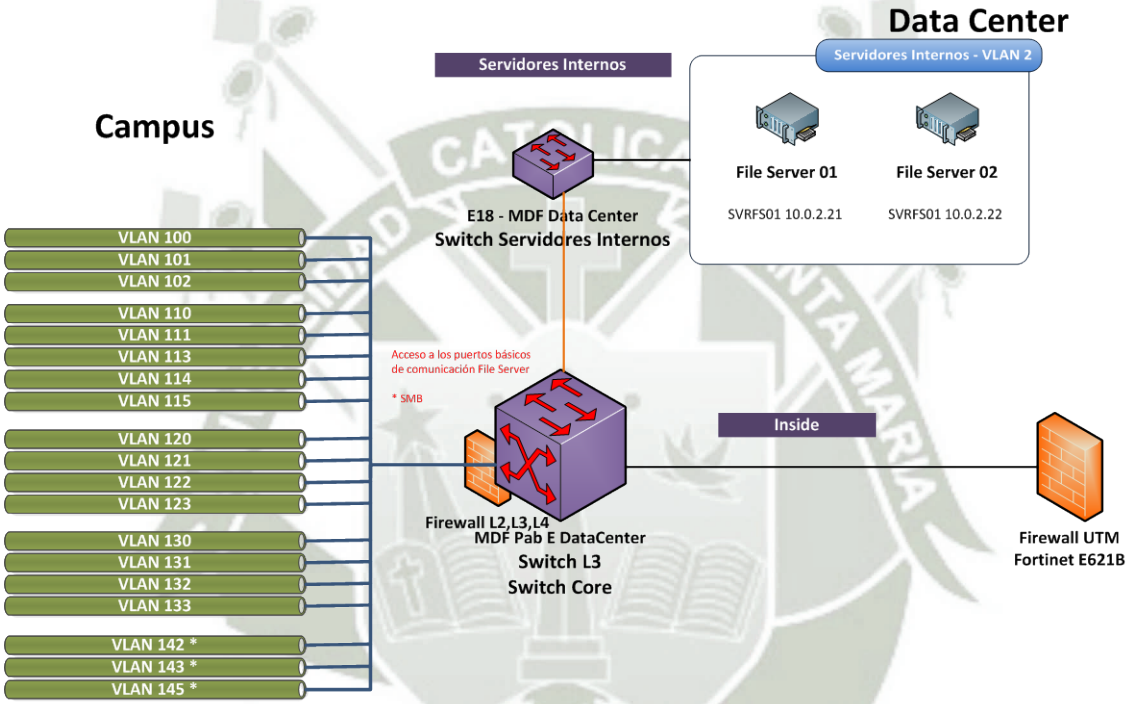

Figura 4.4-12: Aplicación Internas 2
Fuente: Elaboración Propia

- **Aplicación 3: ERP**

Trabajadores administrativos, utilizan el sistema ERP Corporate para realizar las funciones administrativas de la UCSM, pueden ser las unidades administrativas de la UCSM, unidades académicas. Actualmente este sistema se encuentra en implementación.

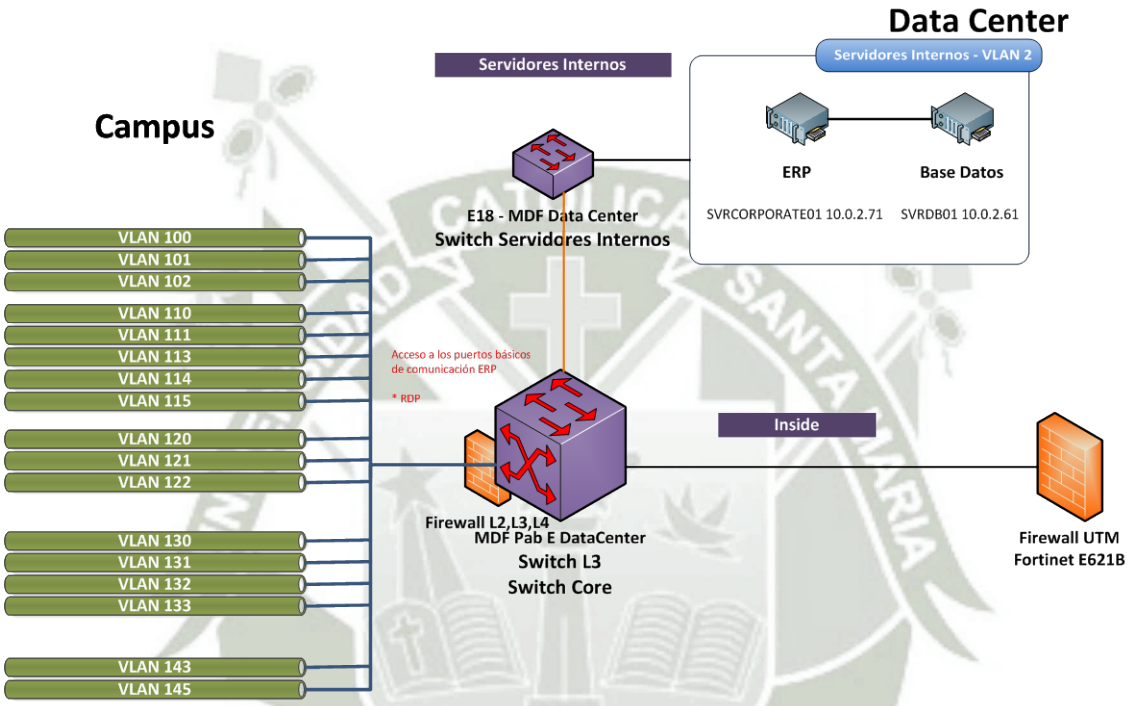

Figura 4.4-13: Aplicación Internas 3
Fuente: Elaboración Propia

- **Aplicación 4: Base Datos**

Las demás aplicaciones del sistema académico se conectan a la base de datos principal de donde obtienen todas las consultas requeridas. Solo los Administradores tienen acceso directo a esta base de datos.

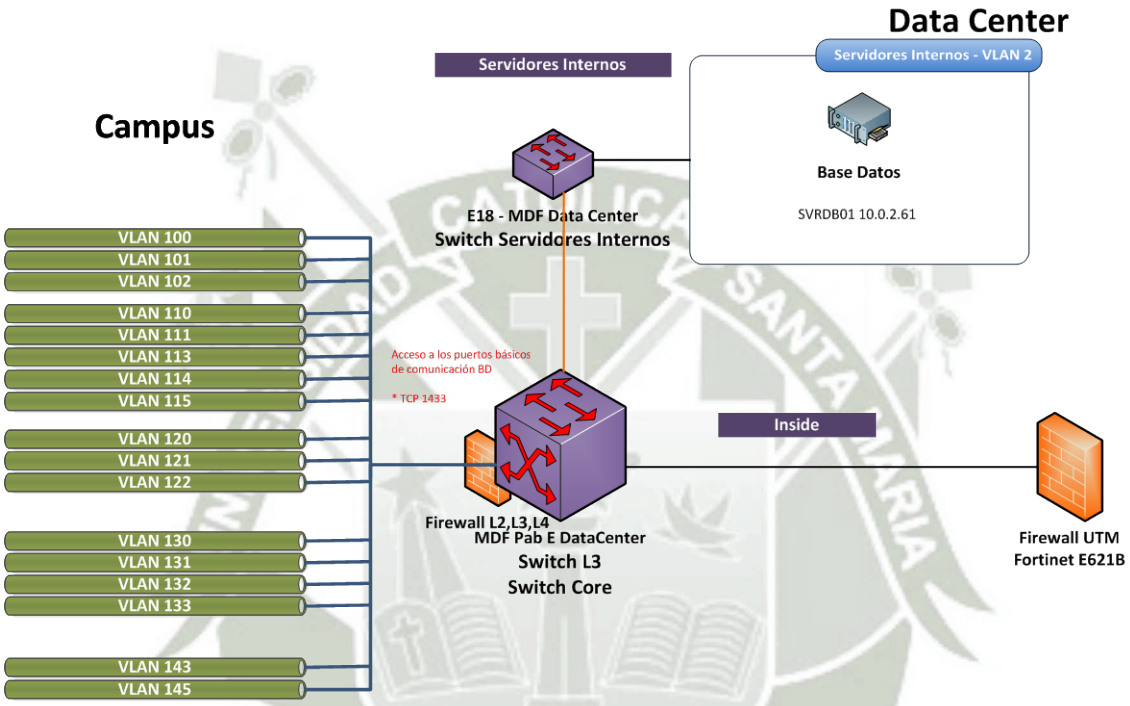

Figura 4.4-14: Aplicación Internas 4
Fuente: Elaboración Propia

- **Aplicación 5: Biblioteca**

  Las aplicaciones del sistema de biblioteca se conectan a la base de datos de biblioteca de donde obtienen todas las consultas requeridas. Solo los Administradores tienen acceso directo a esta base de datos.

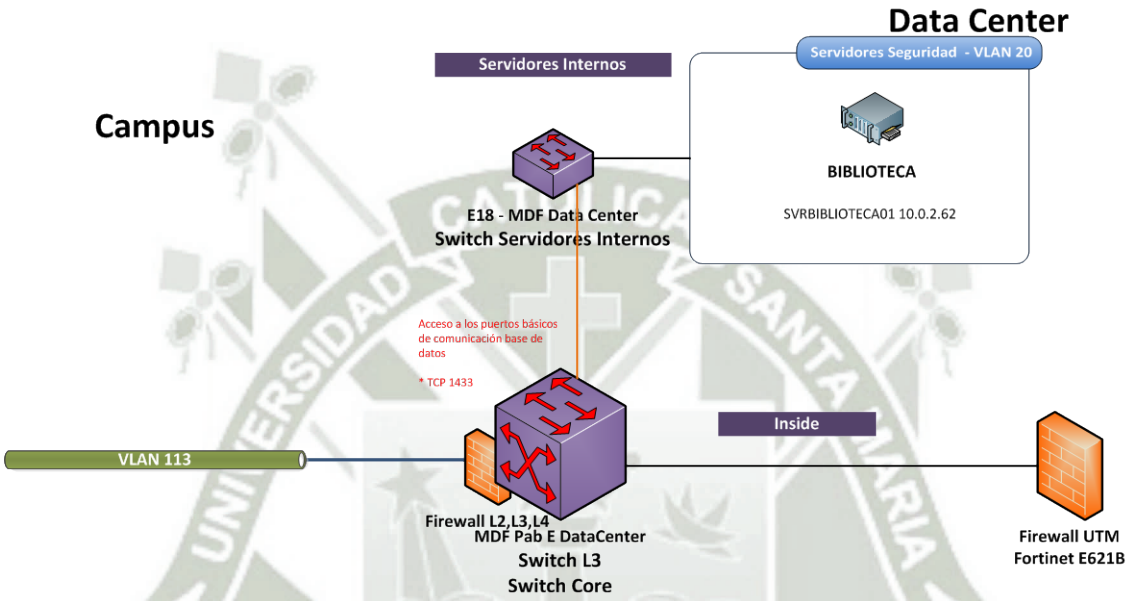

Figura 4.4-15: Aplicación Internas 5
Fuente: Elaboración Propia

- **Aplicación 6: Sistemas Académicos**

  Trabajadores administrativos, docentes utilizan el sistema académico de acceso terminal server para realizar las transacciones académicas que se les haya encomendado, pueden ser las unidades administrativas de la UCSM, unidades académicas.

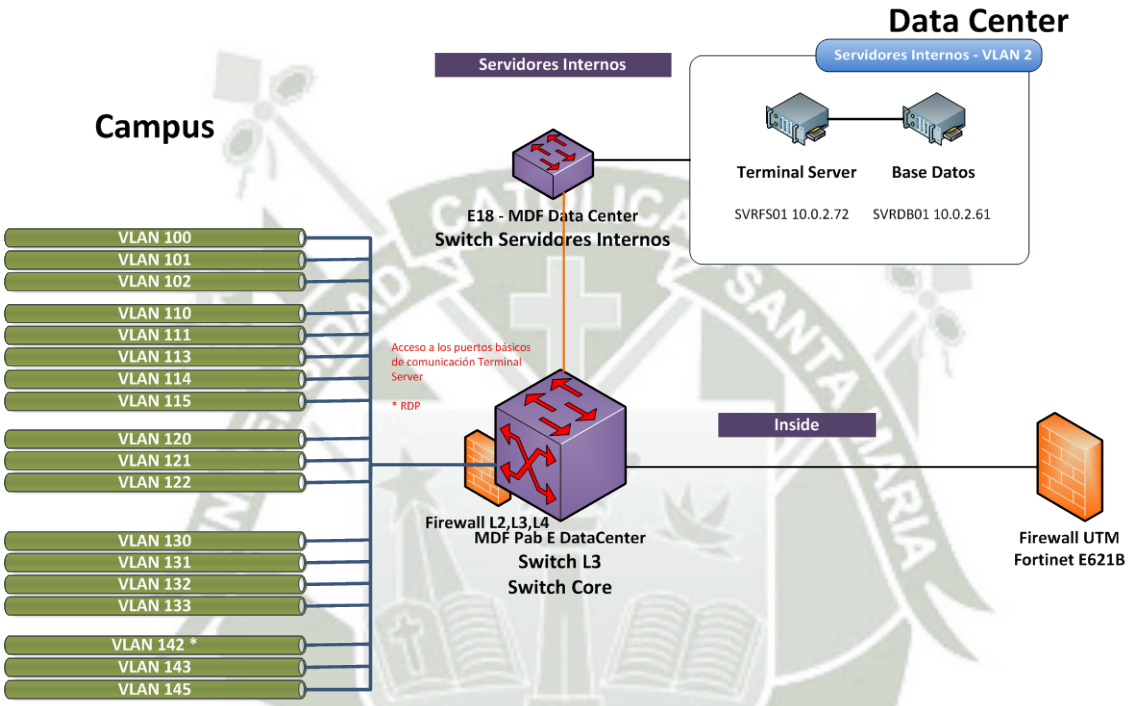

Figura 4.4-16: Aplicación Internas 6
Fuente: Elaboración Propia

- **Aplicación 7: Intranet**

  Trabajadores administrativos, docentes, organizaciones utilizan la intranet para revisar la publicación interna que realiza la UCSM.

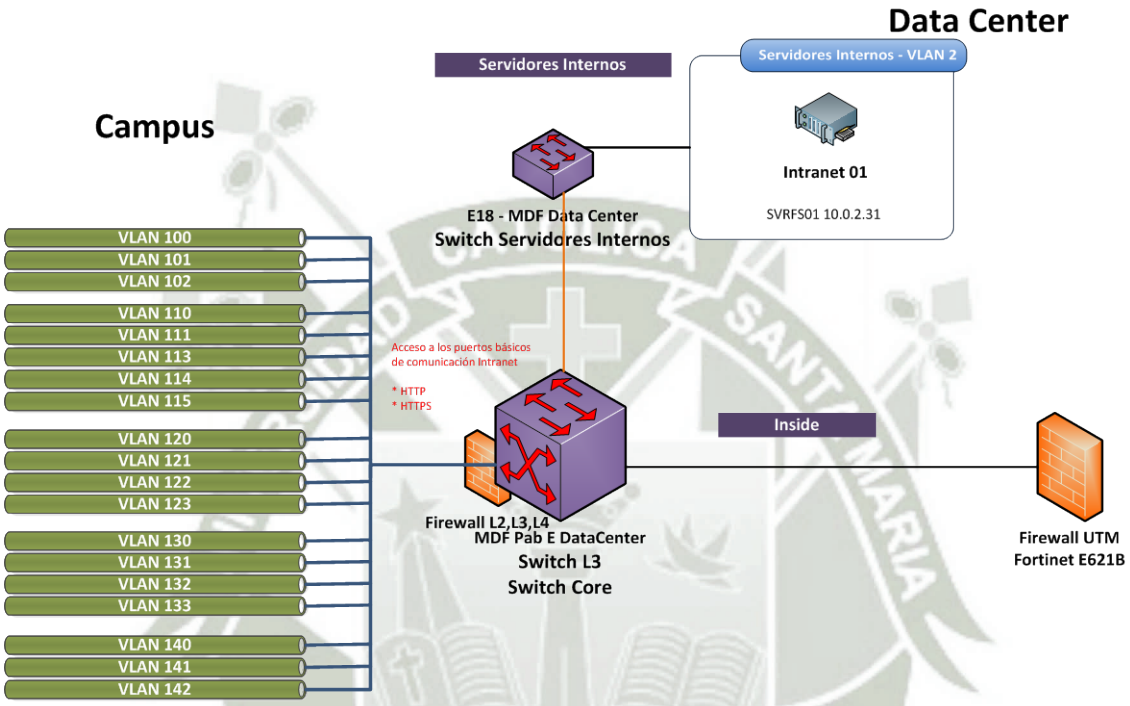

Figura 4.4-17: Aplicación Internas 7
Fuente: Elaboración Propia

- **Aplicación 8: Licencias y Actualizaciones**

  Las computadoras de la UCSM se conectan a este servicio para activar las licencias y actualizar el sistema operativo entre otras aplicaciones, este servicio solo está activo a través del servicio de Active Directory.

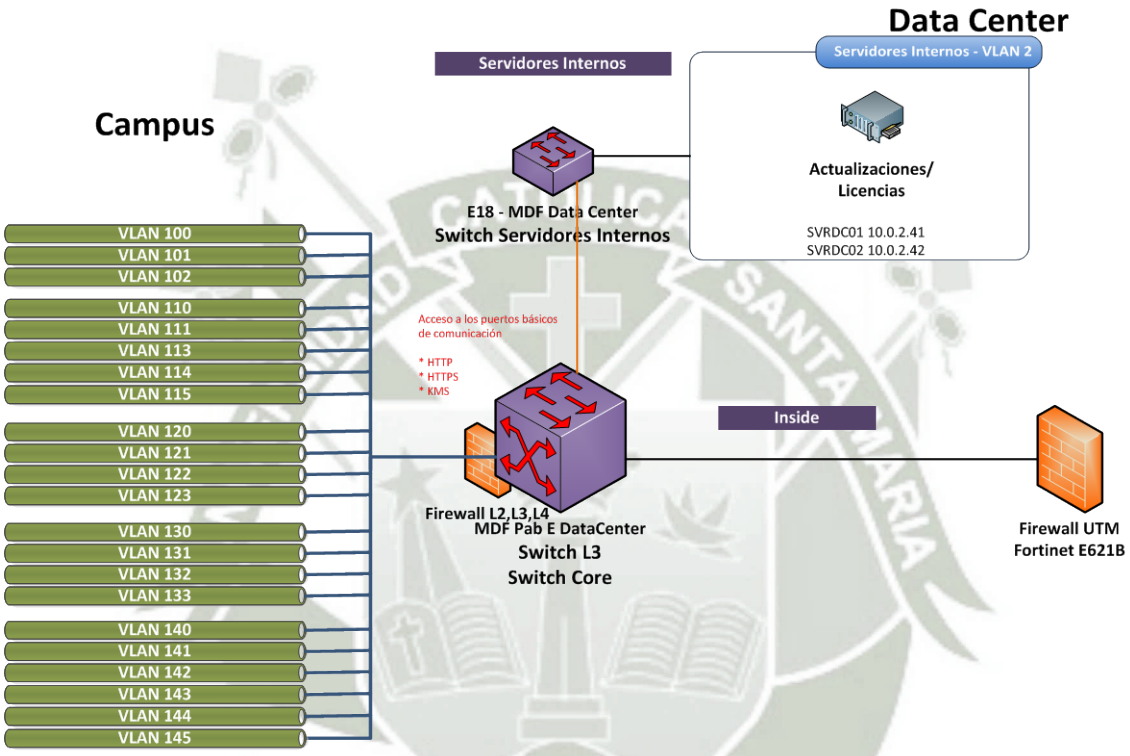

Figura 4.4-18: Aplicación Internas 8
Fuente: Elaboración Propia

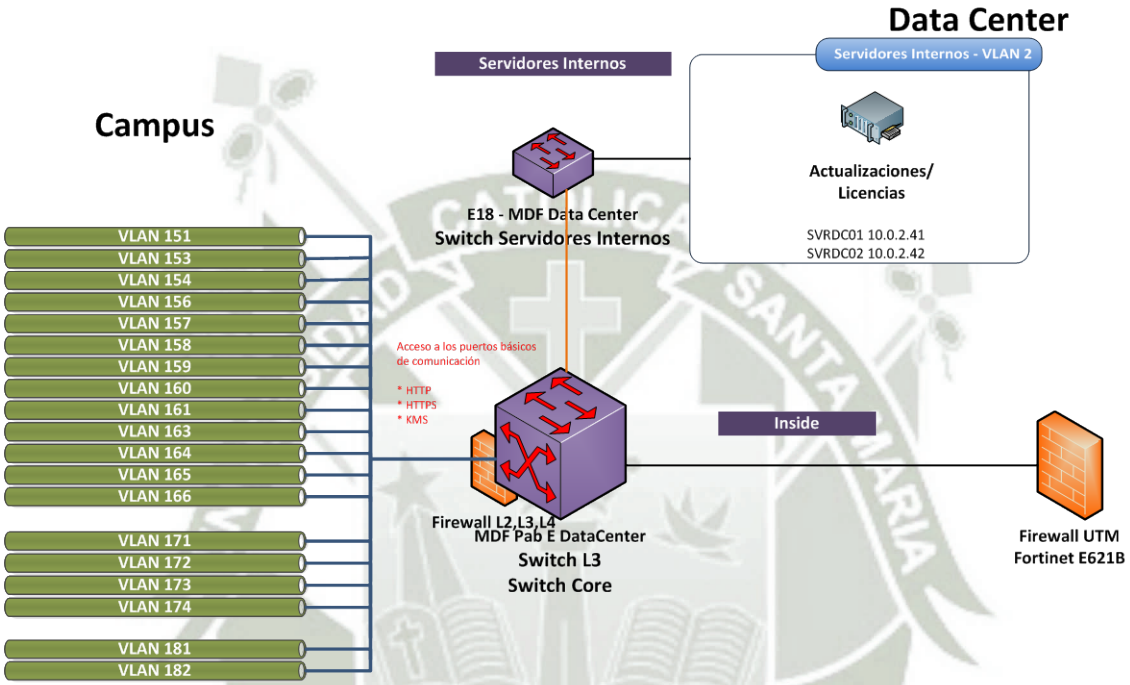

Figura 4.4-19: Aplicación Internas 8'
Fuente: Elaboración Propia

- **Aplicación 9: Administración de Infraestructura**

  Las computadoras, servidores entre otros, de la UCSM se conectan a este servicio para ser administrados, este servicio solo está activo a través del servicio de Active Directory. Actualmente se encuentra en implementación.

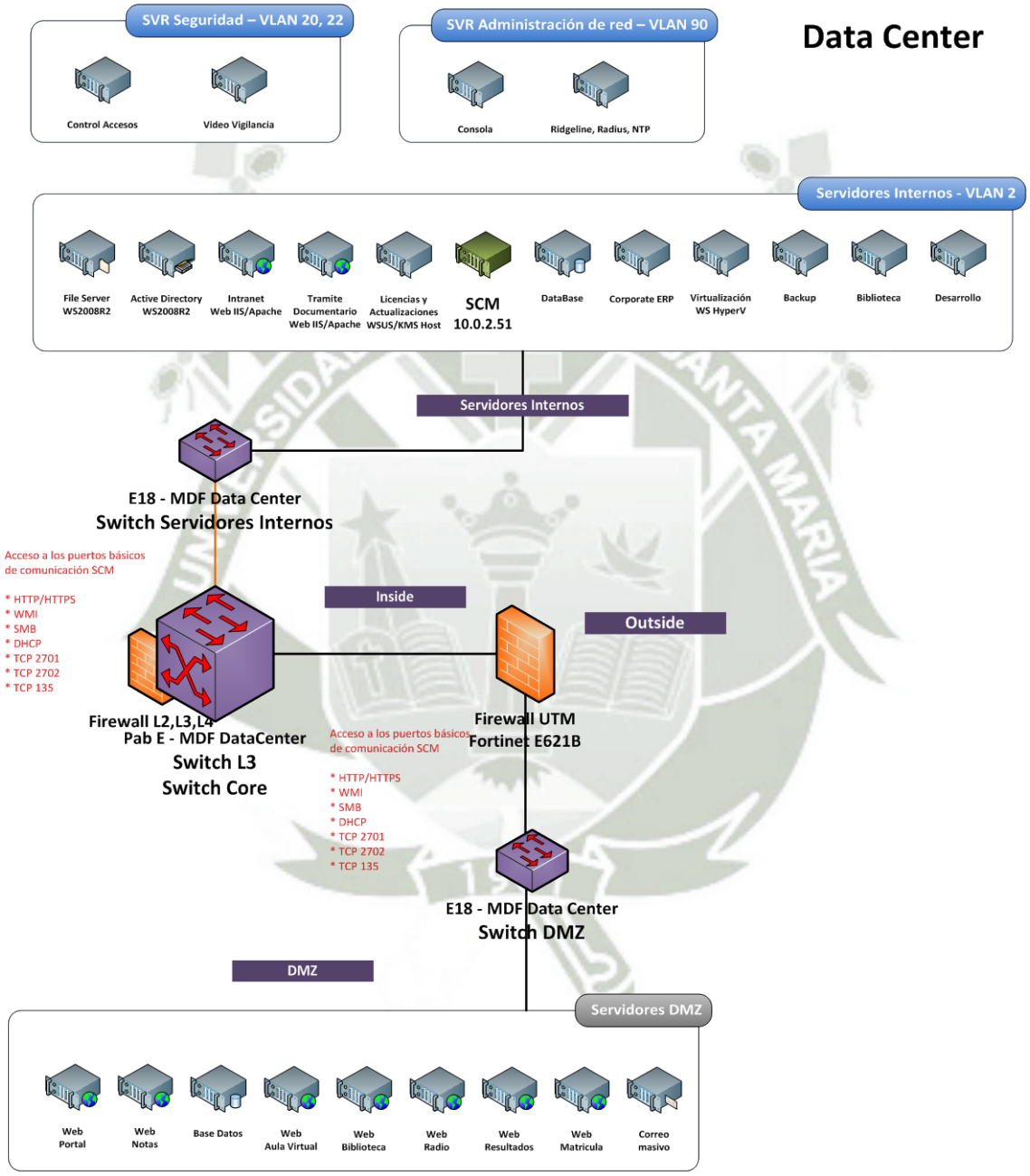

Figura 4.4-20: Aplicación Internas 9
Fuente: Elaboración Propia

- **Aplicación 10: Administración de Infraestructura de Red**

  Los dispositivos de red, de la UCSM se conectan a este servicio para ser administrados, este servicio solo está activo a través del servicio de administración Ridgeline.

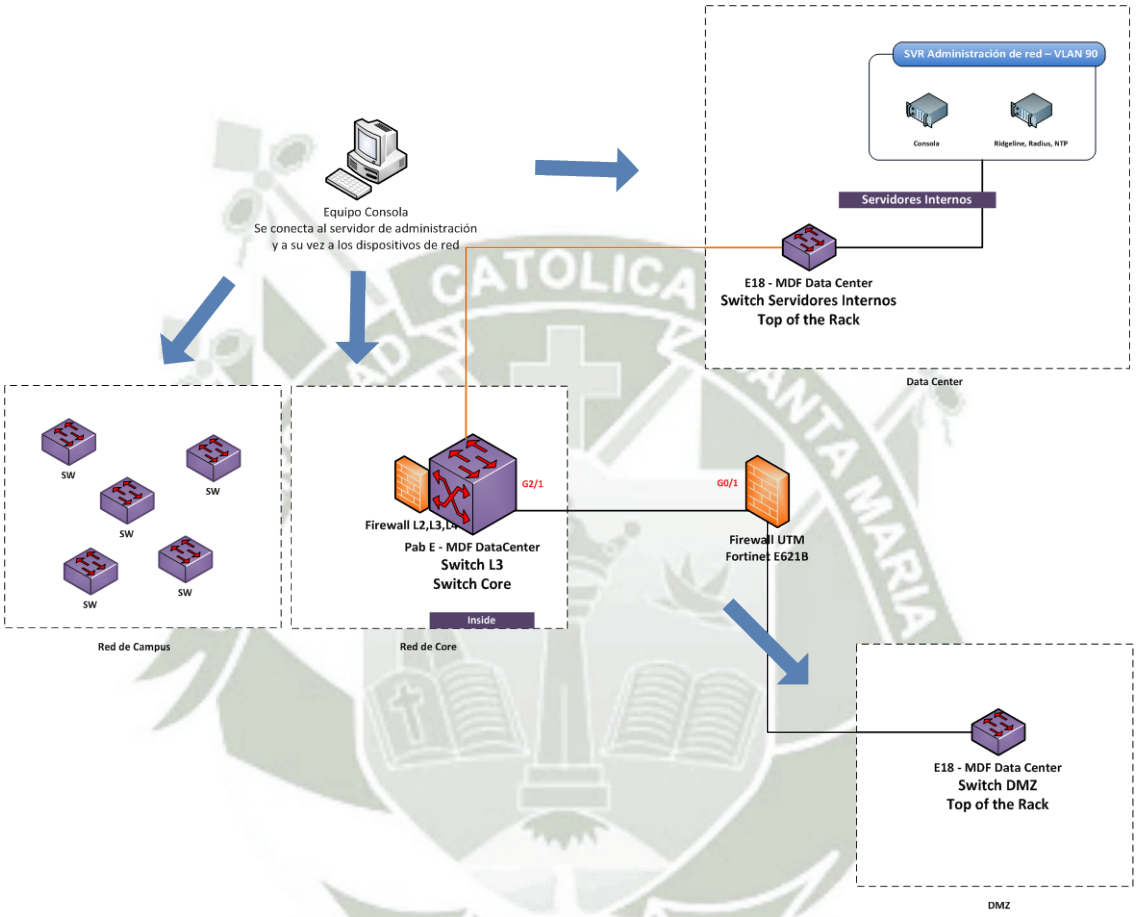

Figura 4.4-21: Aplicación Internas 10
Fuente: Elaboración Propia

- **Aplicación 11: Backup**

  Los servidores, de la UCSM se conectan a este servicio para ser protegidos con copias de seguridad backups, este servicio solo está activo a través del servicio de Active Directory.

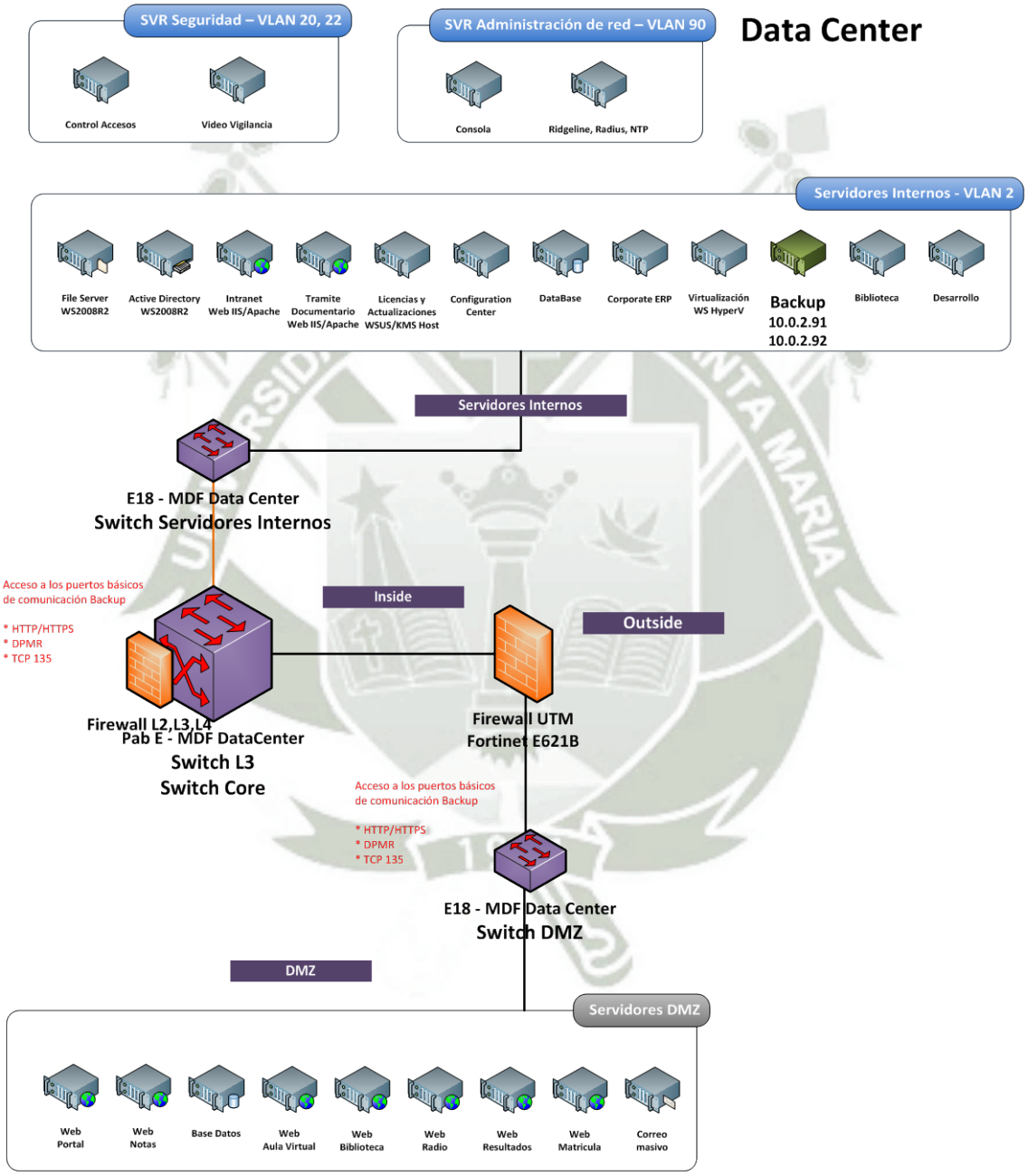

Figura 4.4-22: Aplicación Internas 11
Fuente: Elaboración Propia

- **Aplicación 12: Cámaras IP**

  Las cámaras de seguridad IP, de la UCSM se conectan a este servicio para grabar todas las incidencias que estas reciban. Allí se puede ver el registro con fecha y hora de los eventos guardados.

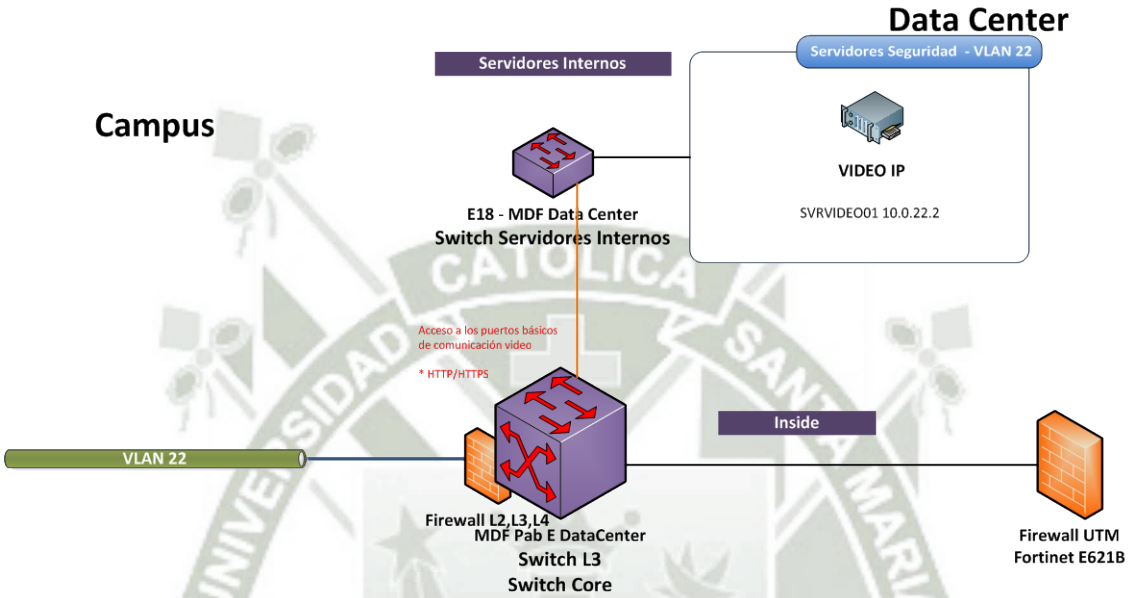

Figura 4.4-23: Aplicación Internas 12
Fuente: Elaboración Propia

- **Aplicación 13: Control de Acceso**

  Registran el acceso de todas las puertas electrónicas que se encuentran en los accesos de la UCSM por medio de las tarjetas de proximidad.

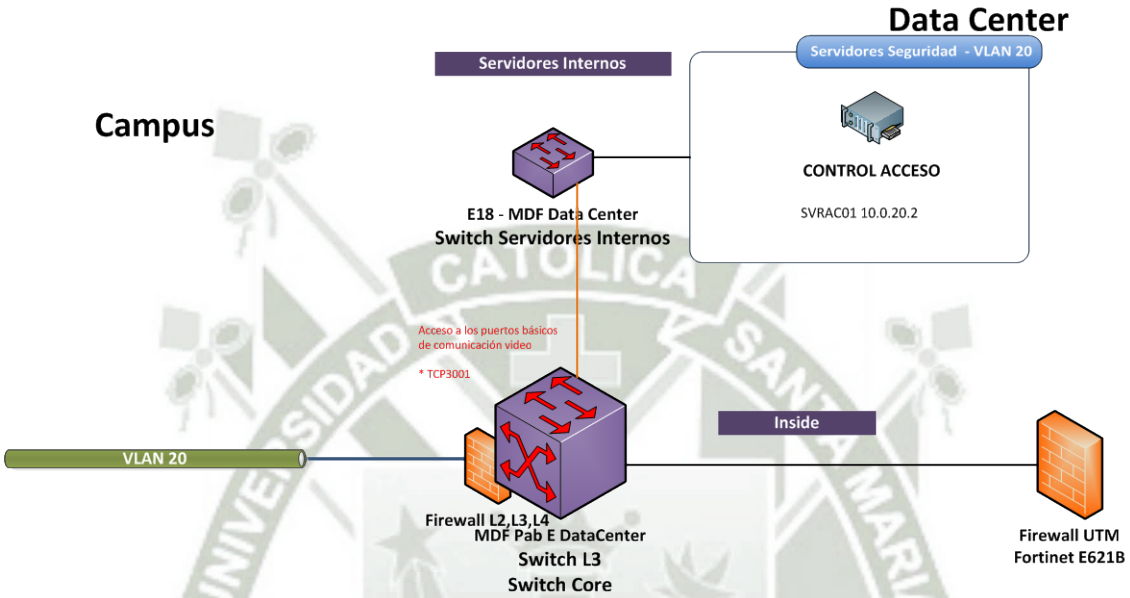

Figura 4.4-24: Aplicación Internas 13
Fuente: Elaboración Propia

- **Aplicación 14: Internet**

  Docentes, estudiantes de pregrado, postgrado, otras especialidades, trabajadores administrativos, organizaciones, visitantes utilizan el servicio de internet el cual esta administrado y tiene sus diversas políticas según el origen y rol. Utiliza el servicio de Active Directory.

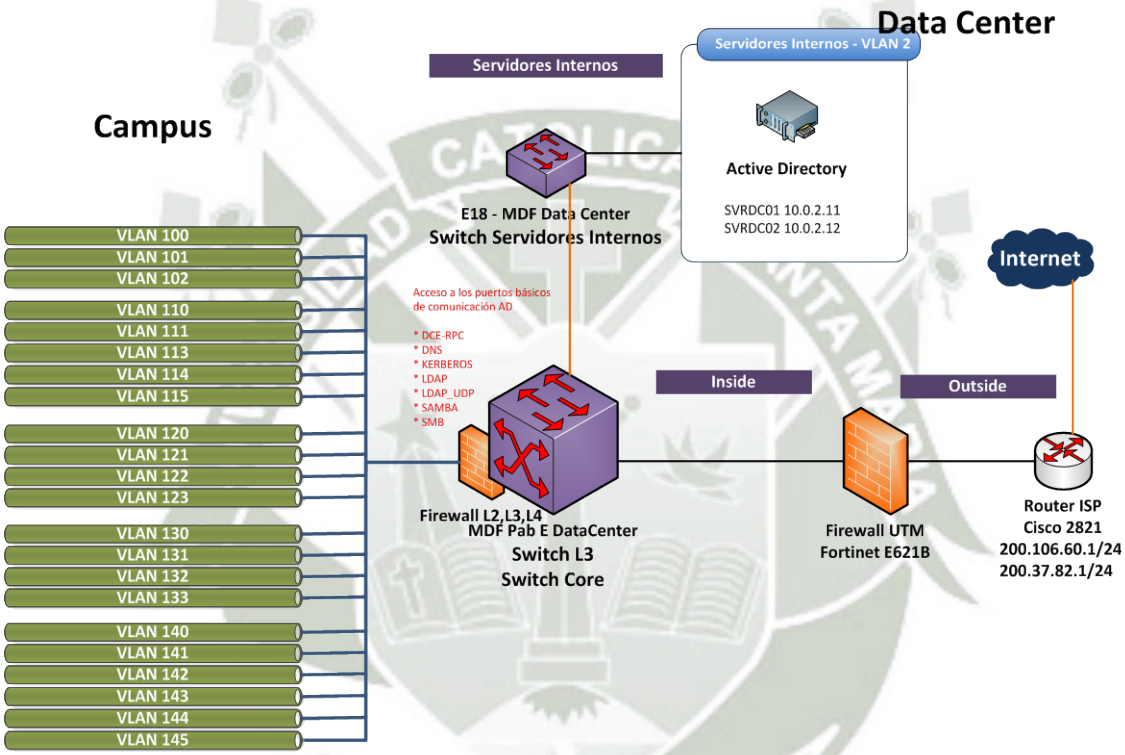

Figura 4.4-25: Aplicación Internas 14
Fuente: Elaboración Propia

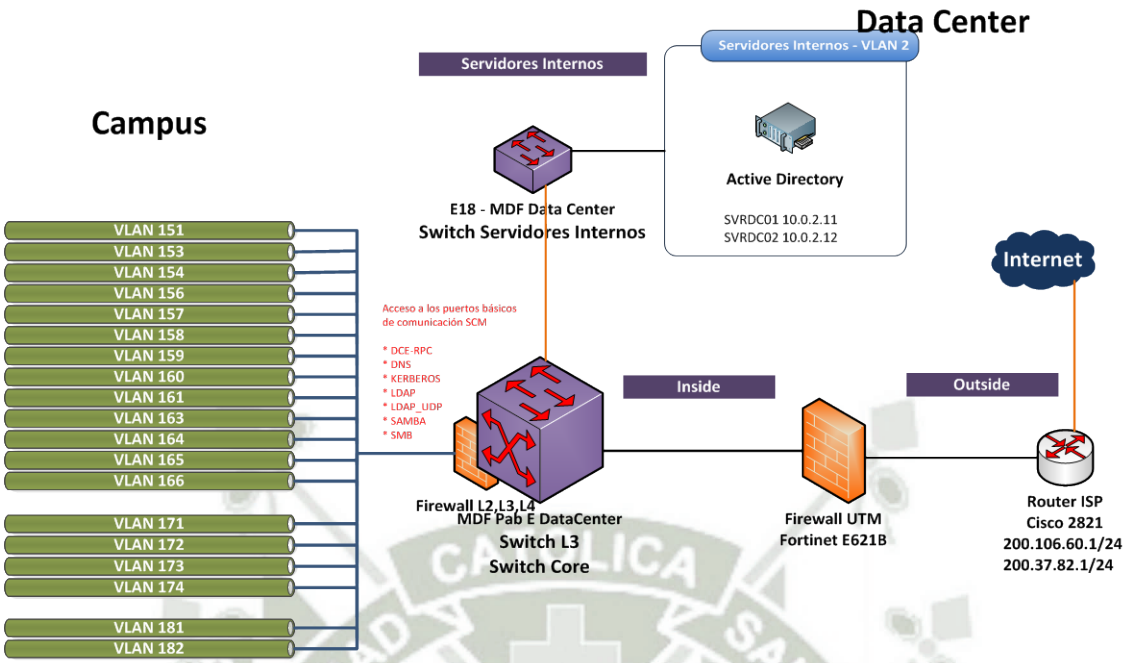

Figura 4.4-26: Aplicación Internas 14'
Fuente: Elaboración Propia

Ítem	Nombre aplicación	Tipo de aplicación	¿Aplicación Nueva?	Criticidad	Costo de fuera de servicio	MTBF aceptable
Internas						
1	**Active Directory**	MS	SI	Alta	Alto	2 horas
2	**File Server**	SMB	No	Alta	Alto	2 horas
3	**ERP**	TS	Si	Alta	Alta	2 horas
4	**Base Datos**	MSSQL	Si	Alta	Alta	2 horas
5	**Biblioteca**	MSSQL	Si	Media	Media	2 horas
6	**Sistemas Académicos**	TS	Si	Alta	Alta	2 horas
7	**Intranet**	Web	No	Media	Media	2 horas
8	**Administración infraestructura**	MS	Si	Alta	Alta	2 horas
9	**Licencias y Actualizaciones**	KMS/WSUS	SI	Media	Media	2 horas
10	**Administración infraestructura de red**	SNMP/WS	Si	Alta	Alta	2 horas
11	**Backup**	MS	Si	Alta	Alta	2 horas
12	**Cámaras IP**	RTP	Si	Alta	Alta	2 horas
13	**Control de Acceso**	MS	Si	Alta	Alta	2 horas
14	**Internet**	Varios	No	Alta	Alta	2 horas

Tabla 4.4-6: Aplicaciones Internas
Fuente: Elaboración Propia

Ítem	Nombre aplicación	Tipo de flujo	Protocolos utilizados	Comunidades de usuario	Ancho de banda requerido	Req QoS
Internas						
1	**Active Directory**	Cliente servidor	DCE-RPC DNS KERBEROS LDAP_TCP_UDP SAMBA, SMB	Todas	Interno: 1Gbps	qp4
2	**File Server**	Cliente servidor	SMB	Autoridades, Jefaturas, Direcciones, Administrativos	Interno: 1Gbps	qp4
3	**ERP**	Terminal Cliente	RDP	Autoridades, Jefaturas, Direcciones, Administrativos	Interno: 1Gbps	qp4
4	**Base Datos**	Servidor Servidor	MSSQL	Administradores	Interno: 1Gbps	qp4
5	**Biblioteca**	Servidor Servidor	MSSQL	Administradores	Interno: 200 Mbps	qp4
6	**Sistemas Académicos**	Terminal Cliente	RDP	Autoridades, Jefaturas, Direcciones, Administrativos	Interno: 1Gbps	qp4
7	**Intranet**	Cliente servidor	HTTP, HTTPS	Autoridades, Jefaturas, Direcciones, Administrativos	Interno: 1Gbps	qp4
8	**Administración infraestructura**	Cliente servidor	HTTP, HTTPS, WMI, SMB, TCP 2701, 2702, 135	Administradores	Interno: 1Gbps	qp4
9	**Licencias y Actualizaciones**	Cliente servidor	KMS, HTTP	Todas	Interno: 1Gbps	qp4
10	**Administración infraestructura de red**	Cliente servidor	SNMPv3	Administradores	Interno: 1Gbps	qp4
11	**Backup**	Servidor Servidor	HTTP, HTTPS, DPMR, TCP 135	Administradores	Interno: 1Gbps	qp4
12	**Cámaras IP**	Cliente servidor	RTP, UDP	Operadores, Administradores	Interno: 1Gbps	qp4
13	**Control de Acceso**	Cliente servidor	TCP 8000, 8001	Operadores, Administradores	Interno: 100 Mbps	qp4
14	**Internet**	Cliente servidor	ANY	Todas	Nube 80 Mbps	qp4

Tabla 4.4-7: Aplicaciones Internas Detalle
Fuente: Elaboración Propia

4.5. Estado actual de la red – Mayo 2011

En Junio del 2011 desde cuando se empezó a realizar el estudio de la situación actual de la red de datos IP de la UCSM indicaba que era una red jerárquica de hasta 6 capas solo existían 12 puntos backbone de interconexión que conectaba algunas áreas del campus, además no se encontró redundancia de enlaces, la redundancia solo existía en la supervisora del equipo Core. Respecto a la WAN contaba con un router y un servidor proxy ambos actuaban como acceso a internet de 8 Mbps y firewall respectivamente.

4.5.1. Infraestructura de red

4.5.1.1. Mapa de red

- La red utiliza switches Ethernet y en algunos casos Hubs. Un equipo en la capa superior en el data center que cumple las funciones de core, los dispositivos de pabellón conectados que cumplen la función de distribución además que soportan la carga de otros equipos de acceso conectados y estos dispositivos de distribución se conectan al equipo de Core vía backbone.

- En cada punto de interconexión hacia el backbone existe un Switch Ethernet de 48 puertos, el cual conecta a usuarios finales y a otros switches que se conectan hacia este equipo.

- Se cuenta con un servidor Proxy basado en Linux Centos 5, el cual cumple funciones de acceso a internet, firewall, filtro de páginas web y de log de acceso web.

- Existen 10 dominios de broadcast en las 5 VLANs existentes.

- No se tiene configurado ninguna calidad de servicio ya que la red es plana y no tiene servicios de voz y video.

- Para el detalle de los equipos de red se clasifico la red en las siguientes zonas:

  - **Zona Data Center**: Incluye todos los equipos de data center.
  - **Zona Campus 1**: Incluye los equipos que están distribuidos por los pabellones A, B, C, D, San Jose D3.
  - **Zona Campus 2**: Incluye los equipos que están distribuidos por los pabellones E, F, G, H, I, O.
  - **Zona Campus 3**: Incluye los equipos que están distribuidos por los pabellones Biblioteca, L, R, S.
  - **Zona Campus Esclavas**: Incluye los equipos que están distribuidos por los pabellones Esclavas Nivel 1, Esclavas Nivel 2, Samuel Velarde 303, Samuel Velarde 305, San Jose C3.

- El detalle de las zonas presentan se muestra a continuación:

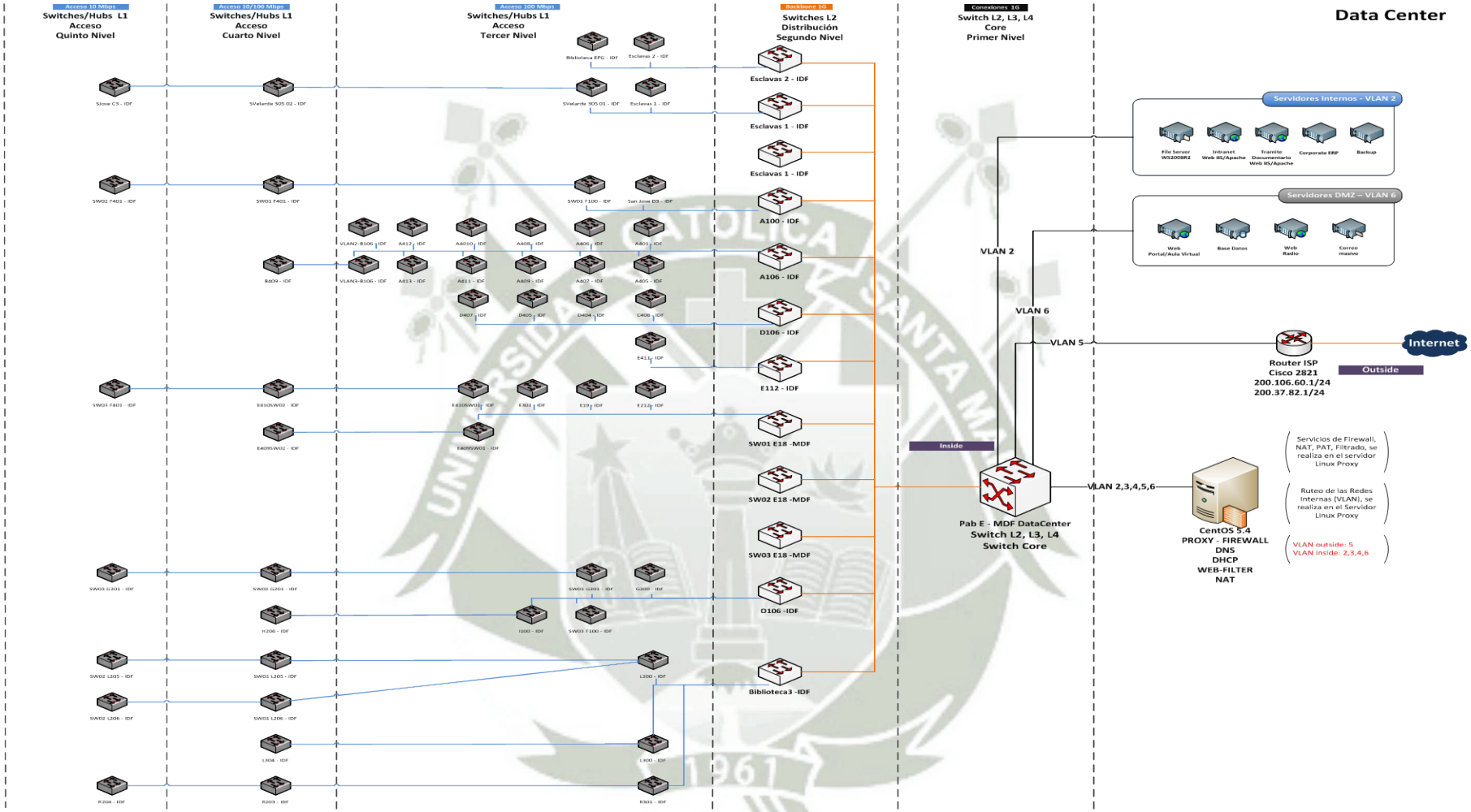

Figura 4.5-1: Mapa de red general
Fuente: Elaboración Propia

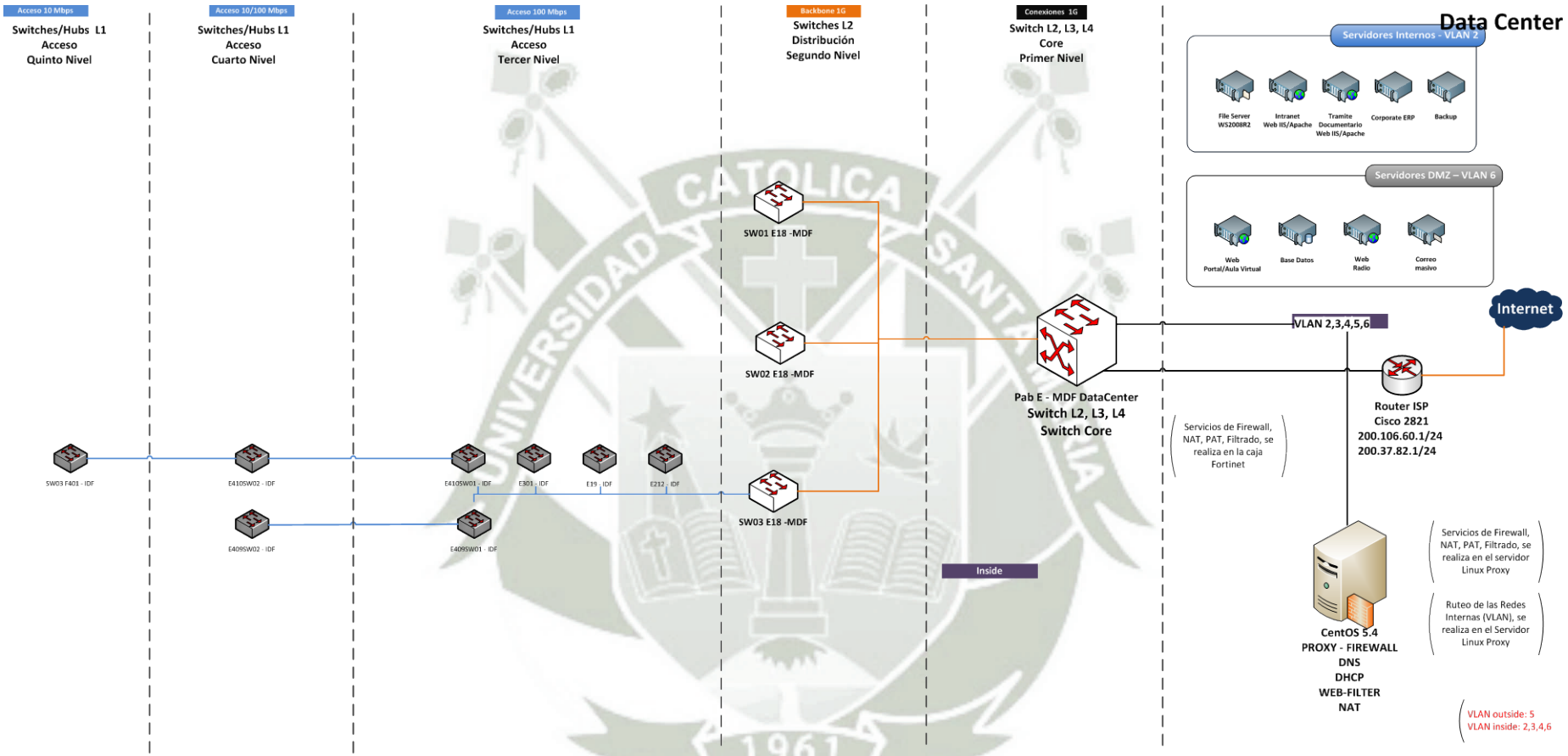

Figura 4.5-2: Mapa de red Data Center
Fuente: Elaboración Propia

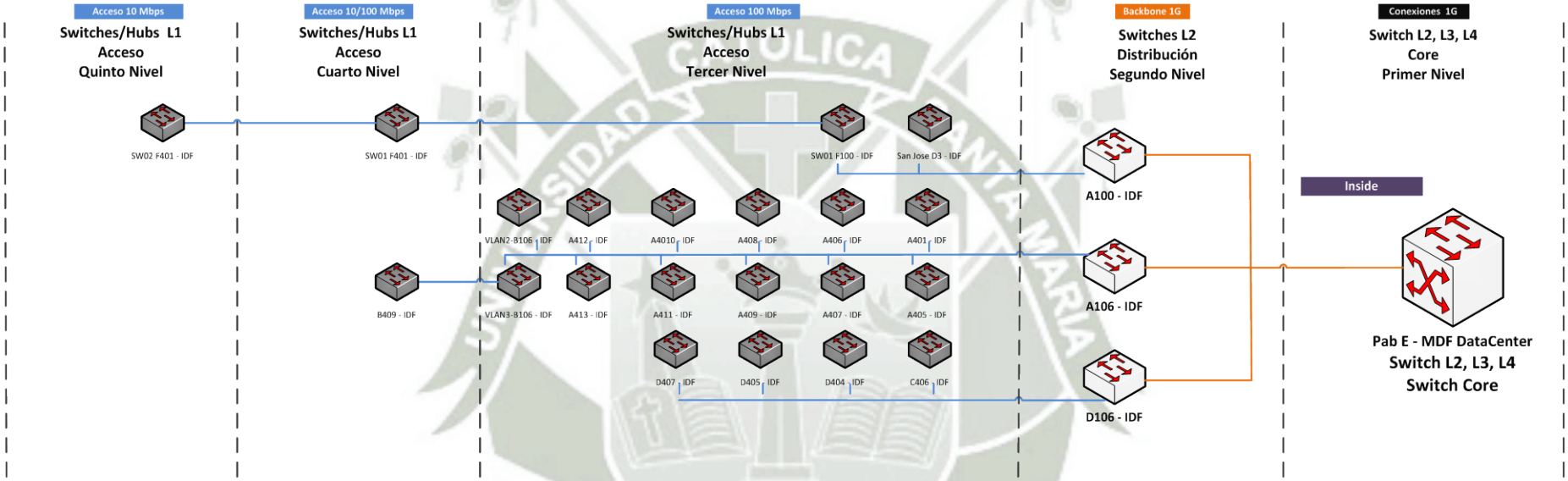

Figura 4.5-3: Mapa de red Zona Campus 1
Fuente: Elaboración Propia

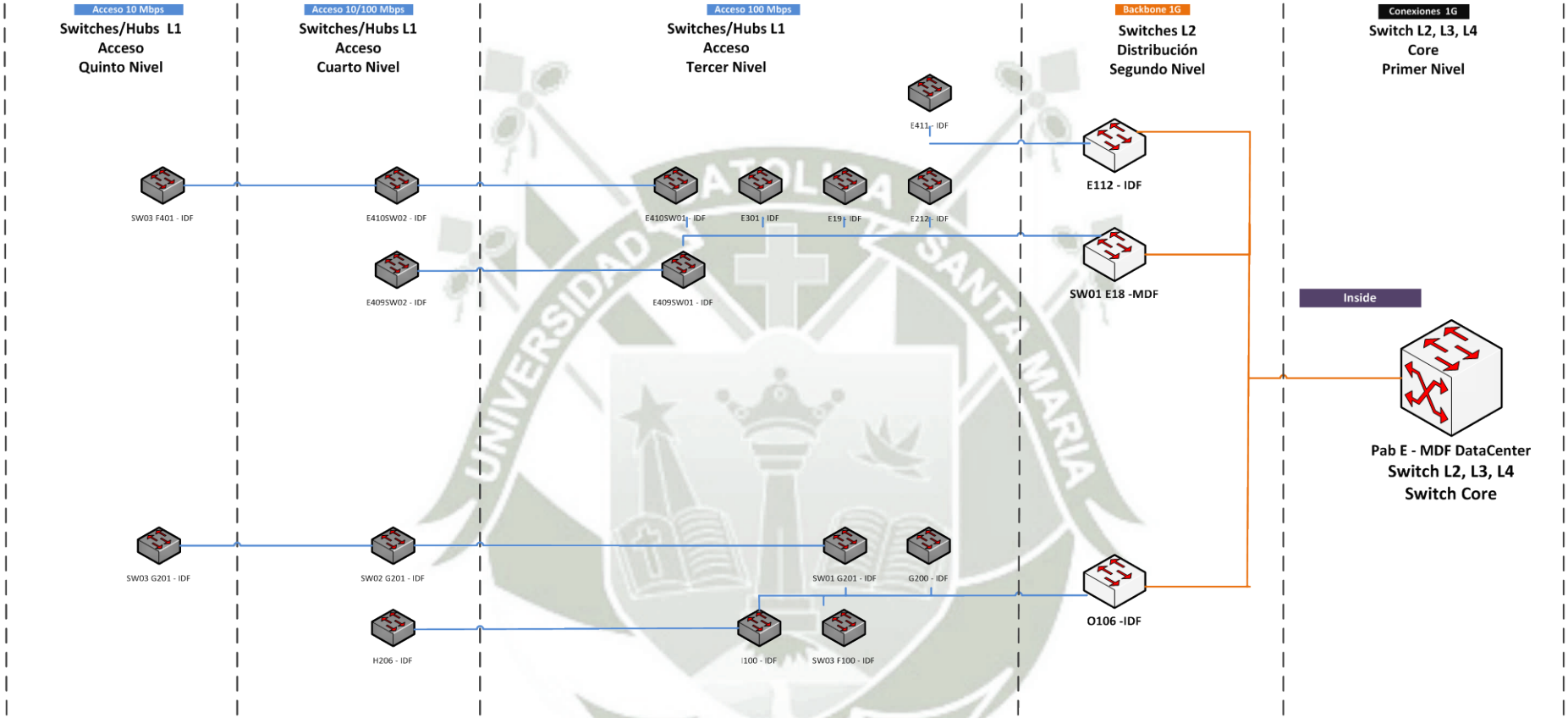

Figura 4.5-4: Mapa de red Zona Campus 2
Fuente: Elaboración Propia

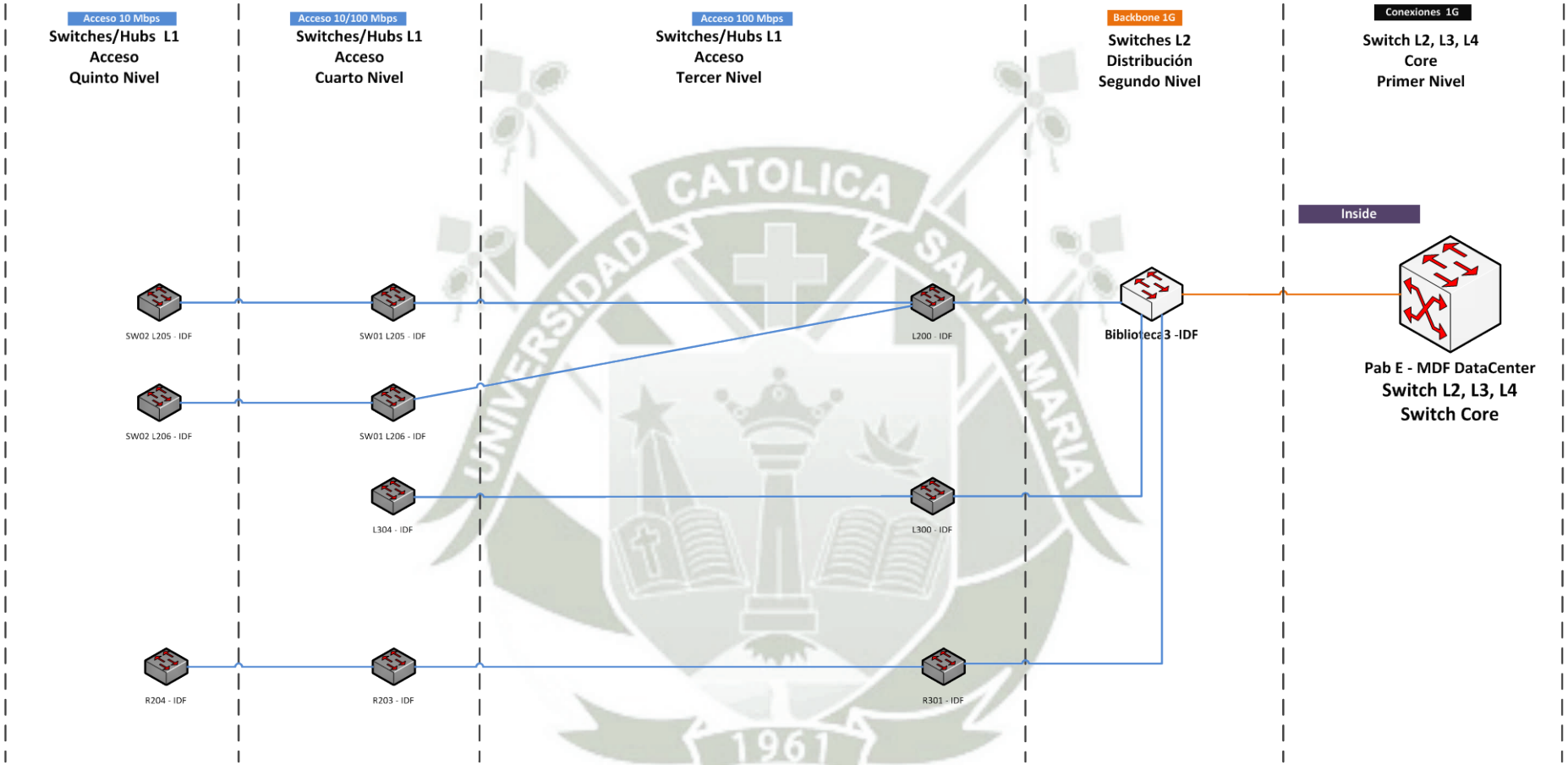

Figura 4.5-5: Mapa de red Zona Campus 3
Fuente: Elaboración Propia

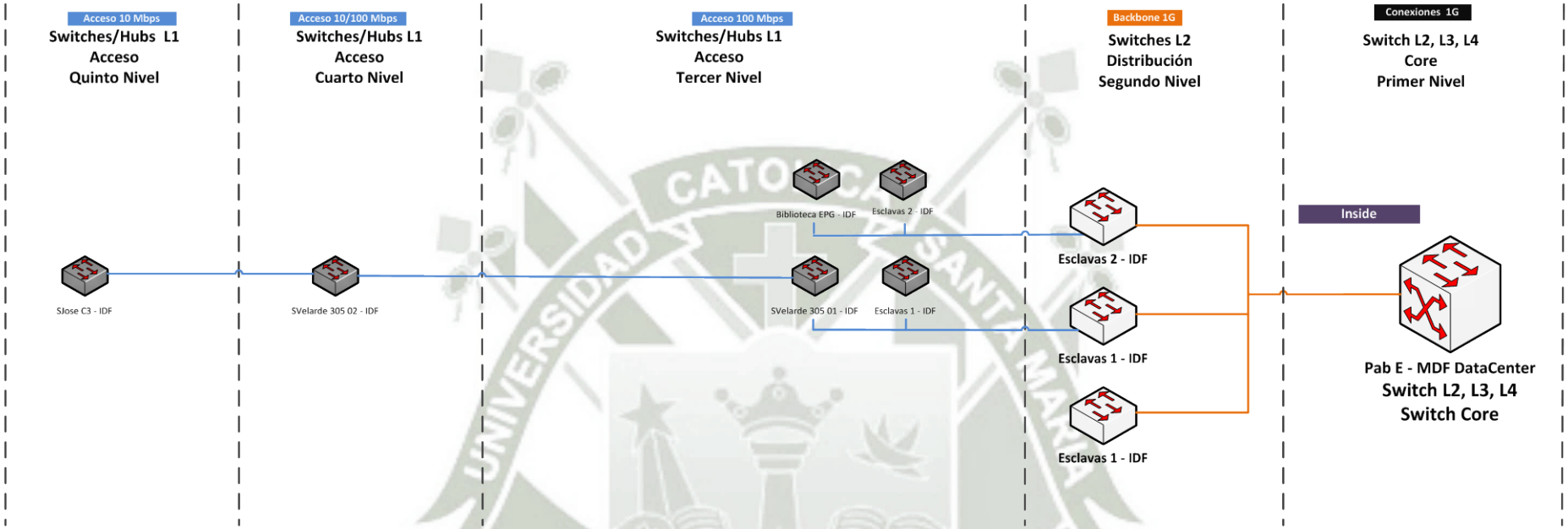

Figura 4.5-6: Mapa de red Zona Campus Esclavas
Fuente: Elaboración Propia

4.5.1.2. Direccionamiento

El direccionamiento de todas las áreas a excepción de la red inalámbrica es estático, el administrador de red otorga las direcciones según demanda. A continuación se detalla:

- Red Internet → Estático
- Red Administrativa → Estático
- Red Laboratorios → Estático
- Red DMZ → Estático
- Red Administración dispositivos → Estático
- Red Inalámbrica → Dinámico

4.5.1.3. Nombramiento

La asignación de nombres a los dispositivos las realiza el administrador de red, no tiene un patrón definido en cuanto al nombre que se asigna a los dispositivos. A continuación se presenta un ejemplo de los dispositivos encontrados según la función que realiza:

- Servidores:
  - De archivos → svrsamba
  - Intranet → intranet
  - Proxy → proxy
  - Web portal → svrweb
  - Base datos web → svrbd
- Host
  - Oficina de presupuesto → OPRE3
  - Oficina de mantenimiento → PIMSG7
  - Informática analista → ANAPRO01
  - Secretaria Dep. Académico Medicina → FMED5

- Switches
  - Valor por defecto

4.5.1.4. Protocolos

- **Capa 1**
  - UTP Categoría 5
  - UTP Categoría 5e
  - UTP Categoría 6
  - Fibra óptica multimodo
- **Capa 2**
  - IEEE 802.1D Spanning Tree (solo equipos capa L2)
  - IEEE 802.1Q (solo equipos capa L2)
  - ARP
  - Fast Ethernet (determinados equipos)
  - Gigabit Ethernet (determinados equipos)
- **Capa 3**
  - Ruteo estático
- **Capa 4**
  - TCP/UDP (Solo equipo de core)
- **Capa 7**
  - SNMP v1 (solo equipos con funcionalidad activada)
  - RMON (solo equipos con funcionalidad activada)

4.5.2. Salud de la red

4.5.2.1. Performance

- **Equipo de Core: Alcatel 7800**
  - Máxima capacidad del equipo: 128 Gbps
  - Máxima Velocidad por puerto según slot:
    - Slot 1: 12 puertos 1 Gbps full duplex BaseT.
    - Slot 2: 24 puertos 100 Mbps full duplex BaseT.
    - Slot 7: 12 puertos 1 Gbps full duplex BaseSX.
  - Tiempo de convergencia: 1s

- **Equipo de Distribución:**

  - **Equipo 1: Alcatel 6148**
    - Máxima capacidad del equipo: 4 Gbps
    - Máxima Velocidad por puerto:
      - Equipada: 48 puertos 10/100 Mbps BaseT.
      - Tarjeta Opcional: 1 Gbps full duplex Base SX.
    - Tiempo de convergencia: 32s

  - **Equipo 2: Alcatel 6248**
    - Máxima capacidad del equipo: 8 Gbps
    - Máxima Velocidad por puerto:
      - Equipada: 48 puertos 10/100 Mbps BaseT, 2 puertos combo 1 Gbps BaseT/BaseSX.
    - Tiempo de convergencia: 26s

- **Equipo 3: Alcatel 6648**
  - Máxima capacidad del equipo: 12 Gbps
  - Máxima Velocidad por puerto según slot:
    - Equipada: 48 puertos 10/100 Mbps BaseT.
    - Tarjeta Opcional: 2 puertos 1 Gbps full duplex BaseSX.
  - Tiempo de convergencia: 15s

- **Equipo de Acceso:**

  En los equipos de acceso se tiene una amplia gama de equipos no administrables, los cuales son bloqueantes, esto quiere decir que no soportan la capacidad de la totalidad de los puertos que ofrecen con una sobresuscripción de 1 a 10. Por ejemplo si diez host se conectan a una carpeta compartida y tratan de copiar un archivo de 50 MB simultáneamente a una velocidad de 20 Mbps, este dispositivo se bloqueara y se colgara.

  En general los equipos de acceso tienen las siguientes características:

  - Máxima capacidad: 100-200 Mbps aprox.
  - Equipada: 24 puertos 10/100 Mbps
  - Marcas: DLINK, SATRA, EDIMAX.
  - Tiempo de convergencia: 60s

4.5.2.2. Disponibilidad

A continuación se presenta la siguiente tabla con información de disponibilidad de la red actual.

Ítem	Nombre aplicación	MTBF	MTTR	Fecha y duración de la última caída	Causa de la última caída	Solución de la última caída
1	**Enterprise**	4000	2	2011-05-09, 1 Hora	Prevención de bucles no configurado	Aplicación Protocolo STP
2	**VLAN 2**	2000	4	2011-05-09, 1 Hora	Prevención de bucles no configurado	Aplicación Protocolo STP
3	**VLAN 3**	2000	4	2011-05-09, 1 Hora	Prevención de bucles no configurado	Aplicación Protocolo STP
4	**VLAN 4**	2000	4	2011-05-09, 1 Hora	Prevención de bucles no configurado	Aplicación Protocolo STP
5	**VLAN 5**	4000	2	2011-02-20, 4 Hora	Actualización de equipos por parte del ISP	Reemplazo de equipos
6	**VLAN 6**	4000	2	2011-05-09, 1 Hora	Prevención de bucles no configurado	Aplicación Protocolo STP

Tabla 4.5-1: Disponibilidad de red actual
Fuente: Elaboración Propia

4.5.2.3. Utilización

A continuación se presenta la siguiente figura con información de utilización de la red actual.

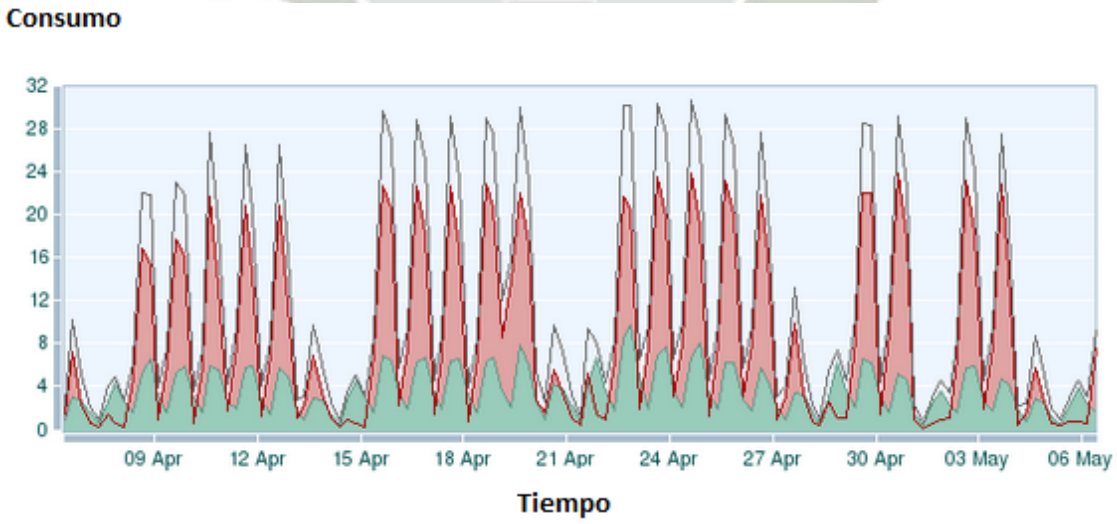

Figura 4.5-7: Utilización de red actual
Fuente: Elaboración Propia

4.5.3. Diseño lógico

4.5.3.1. Topología

La topología lógica de la red actual está compuesta por seis VLAN cada una de las cuales se detalla a continuación:

- **VLAN 2:**

  - **Intercat:** Está compuesta por las oficinas de siguientes áreas:

Ítem	Descripción	Act.	Disp.	Nombre	Vlan	Mas.	Dir. Red
1	**Vlan "Intercat"**	**460**	**1022**	**Intercat**	**2**	**22**	**192.168.0.0/22**
Unidad Administrativa – Rectorado							
1	Rectorado	4					
2	Oficinas Dependientes	92					
Unidad Administrativa - Vicerrectorado Académico							
1	Vicerrectorado Académico	7					
2	Oficinas Dependientes	100					
Unidad Administrativa - Vicerrectorado Administrativo							
1	Vicerrectorado Administrativo	5					
2	Oficinas Dependientes	56					
Unidades Académicas							
1	Facultades Pregrado	150					
2	Escuela de Posgrado	9					
Campus							
1	Organismos Autónomos	8					
2	Representaciones Gremiales	15					
3	Otros Organismos	3					
4	Porterías	6					
5	Auditoria Externa	5					

Tabla 4.5-2: Áreas Administrativas
Fuente: Elaboración Propia

Los principales datos de la red se muestran a continuación:

- Dirección de red: 192.168.0.0/24
- Dominio broadcast: 192.168.3.255
- Direcciones utilizables: 1022
- Autenticación: No

- **Administración Switches:** Está compuesta por todos los dispositivos de switching que sean administrables.

  Los principales datos de la red se muestran a continuación:

  - Dirección de red 1: 192.168.50.0/24
  - Dominio broadcast 1: 192.168.50.255
  - Direcciones utilizables: 254
  - Autenticación: No

  - Dirección de red 2: 192.168.50.0/24
  - Dominio broadcast 2: 192.168.60.255
  - Direcciones utilizables: 254
  - Autenticación: No

- **VLAN 3:**

  - **Laboratorios:** Está compuesta por los laboratorios del Campus a continuación se detalla:

Ítem	Descripción	Act.	Disp.	Nombre	Vlan	Mas.	Dir. Red
1	Vlan "Laboratorios"	880	1022	Laboratorios	3	22	192.168.4.0/22
Ciencias Sociales							
1	Fac. Cs. Sociales	91					
	FCTSH						
Ciencias Jurídicas Empresariales							
2	Fac. Cs. Jurídicas Empresar.	109					
	FCCF						
	FCEA						
	FCJP						
Ciencias de la Salud							
3	Fac. Cs de la Salud	21					
	Facultad de Enfermería						
	Facultad de Medicina						
	Facultad de Odontología						
	FCFBB						
	Facultad de Obstetricia						
Ciencias e Ingenierías							
4	FCIBQ	21					
5	FAICA	56					
6	FCIFF	295					
Escuela de Postgrado							
10	Escuela de Post Grado	34					
Campus							
11	Aulas Campus	120					
12	SUM	12					
13	Auditorios	6					
Otras Áreas							
14	Biblioteca Virtual	62					
15	Estadística	25					
16	Proyecto Mercurio	14					
17	CICA	14					

Tabla 4.5-3: Laboratorios
Fuente: Elaboración Propia

Los principales datos de la vlan se muestran a continuación:

- Dirección de red: 192.168.4.0/22
- Dominio de broadcast: 192.168.7.255
- Direcciones utilizables: 1022
- Autenticación: No

- **VLAN 4:**

  - **Wifi:** Está compuesta por los host que se conectan por el medio inalámbrico y su red de administración.

    Los principales datos de la vlan se muestran a continuación:

    - Dirección de red 1: 192.168.10.0/24
    - Dominio de broadcast 1: 192.168.10.255
    - Direcciones utilizables: 254
    - Autenticación: MAC Address

    - Dirección de red 2: 192.168.11.0/24
    - Dominio de broadcast 2: 192.168.11.255
    - Direcciones utilizables: 254
    - Autenticación: MAC Address

    - Dirección de red 3: 192.168.12.0/24
    - Dominio de broadcast 3: 192.168.12.255
    - Direcciones utilizables: 254
    - Autenticación: No

    - Dirección de red 4: 192.168.51.0/24
    - Dominio de broadcast 4: 192.168.51.255
    - Direcciones utilizables: 254
    - Autenticación: No

- **VLAN 5:**

  - **Internet:** Está compuesta por las direcciones IP's públicas que asigna el proveedor de servicios.

Los principales datos de la red se muestran a continuación:

- Dirección de red 1: 200.106.60.0/24
- Dominio de broadcast 1: 200.106.60.255
- Direcciones utilizables: 254
- Autenticación: No

- Dirección de red 2: 200.37.82.0/24
- Dominio de broadcast 2: 200.37.82.255
- Direcciones utilizables: 254
- Autenticación: No

- **VLAN 6:**

  - **DMZ:** Está compuesta por las direcciones IP's asignadas a los servicios que se publican hacia la nube. Todos estos servicios se realizan mediante NAT.

    Los principales datos de la red se muestran a continuación:

    - Dirección de red 1: 192.168.16.0/24
    - Dominio de broadcast 1: 192.168.16.255
    - Autenticación: No

  - **Hardware Data Center:** Está compuesta por los dispositivos administrables que forman parte del data center.

    Los principales datos de la red se muestran a continuación:

- Dirección de red 1: 192.168.55.0/24
- Dominio de broadcast 1: 192.168.55.255
- Direcciones utilizables: 254
- Autenticación: No

4.5.4. Diseño físico

4.5.4.1. Forma

Diseño: Estrella extendida

4.5.4.2. Dispositivos

Los dispositivos de red encontrados en la red actual se detallan en las siguientes dos tablas:

Ítem		ID	Marca	Modelo	#Port	Adm.	Dirección 1	Dirección 2
Nivel Core								
	Core							
1	Alcatel 7800	1	Alcatel	7800	48	si	192.168.50.1/24	192.168.60.1/24
Nivel Distribución								
	Distribución							
1	A 100	21	Alcatel	6648	24	si	192.168.50.21/24	192.168.60.21/24
2	A	22	Alcatel	6148	48	si	192.168.50.22/24	-
3	D	24	Alcatel	6148	48	si	192.168.50.24/24	-
4	E	25	Alcatel	6148	24	si	192.168.50.25/24	-
5	Biblioteca	28	Alcatel	6148	48	si	192.168.50.28/24	-
6	O	29	Alcatel	6148	48	si	192.168.50.29/24	-
7	Esclavas 1	31	Alcatel	X460	48	si	192.168.50.31/24	-
8	Esclavas 1	31	Alcatel	X460	48	si	192.168.50.31/24	-
9	Esclavas 2	32	Alcatel	X460	48	si	192.168.50.32/24	-
Nivel Data Center								
	Distribución							
1	Switch 1	12	Alcatel	6248	48	si	192.168.50.12/24	192.168.60.12/24
2	Switch 2	13	Alcatel	6248	48	si	192.168.50.13/24	192.168.60.13/24
3	Switch 3	18	DLink hub	DGS3450	48	si	192.168.50.18/24	-
	Blade							
1	Blade sw 1	115	BNT	GbESM	20	si	192.168.50.115/24	-
2	Blade sw 2	116	BNT	GbESM	20	si	192.168.50.116/24	-

Tabla 4.5-4: Equipamiento actual 1
Fuente: Elaboración Propia

Ítem		ID	Marca	Modelo	#Port	Adm.	Dirección 1	Dirección 2
Nivel Acceso								
	Pabellón E							
1	E416 - SW01 Tutoría	-	Satra	HPv1910	48	no	-	-
2	E301 - SW01 CPU	-	Satra	S24P	24	no	-	-
3	E213 - SW01 Electrónica	-	Satra	S24P	24	no	-	-
4	E406 - SW01 Idiomas 01	-	DLink hub	DL24P	24	no	-	-
5	E406 - SW02 Idiomas 02	-	DLink hub	DL24P	24	no	-	-
6	E406 - SW01 Idiomas 03	-	DLink hub	DL24P	24	no	-	-
7	E406 - SW01 Idiomas 04	-	DLink hub	DL24P	24	no	-	-
	Pabellón F							
8	F100 - SW01	-	Satra	S24P	24	no	-	-
9	F100 - SW02	-	Satra	S24P	24	no	-	-
10	F100 - SW03	-	DLink hub	D24P	24	no	-	-
10	F401 - SW01	-	Edimax	E24P	24	no	-	-
11	F401 - SW02	-	Edimax	E24P	24	no	-	-
12	F401 - SW02	-	Edimax	E24P	24	no	-	-
	Pabellón I, H							
11	I 100 SW01	-	Edimax	E24P	24	no	-	-
12	I 100 SW02	-	Satra	S24P	24	no	-	-
13	I Lab Psicología	-	Satra	S24P	24	no	-	-
14	H Lab Mercurio	-	Satra	S24P	24	no	-	-
	Pabellón G							
15	G200 - SW01 Estadística	-	Satra	S24P	24	no	-	
16	G201 - SW01 Bib. Virtual	-	Edimax	E24P	48	no	-	
16	G201 - SW02 Bib. Virtual	-	Edimax	E24P	24	no	-	
17	G201 - SW03 Bib. Virtual	-	Edimax	E24P	24	no	-	
	Pabellón L							
18	L200 - Coordinación	-	DLink hub	D24P	24	no	-	-
19	L205 - SW01	-	DLink hub	D24P	24	no	-	-
20	L205 - SW02	-	DLink hub	D24P	24	no	-	-
21	L205 - SW03	-	DLink hub	D24P	24	no	-	-
22	L206 - SW01	-	DLink hub	D24P	24	no	-	-
23	L206 - SW02	-	DLink hub	D24P	24	no	-	-
24	L206 - SW03	-	DLink hub	D24P	24	no	-	-
25	L300 - SW01	-	DLink hub	D24P	24	no	-	-
26	L304 - SW01	-	DLink hub	D24P	48	no	-	-
	Pabellón R							
27	R203 - CEDIMSW01	79	DLink hub	D24P	48	no	-	-
28	R203 - CEDIMSW02	80	DLink hub	D24P	50	no	-	-
29	R203 - CEDIMSW03	81	DLink hub	D24P	24	no	-	-
30	R201 - SW01	82	DLink hub	D24P	24	no	-	-
	Biblioteca							
31	Biblioteca SW01	86	Extreme	X440	24	no	-	
	Pabellón A							
32	A - Lab A401	93	Satra	S24P	24	no	-	-
33	A - Lab A405	94	Satra	S24P	24	no	-	-
34	A - Lab A406	95	Satra	S24P	24	no	-	-
35	A - Lab A407	96	Satra	S24P	24	no	-	-
36	A - Lab A408	97	Satra	S24P	24	no	-	-
37	A - Lab A409	98	Satra	S24P	24	no	-	-
38	A - Lab A410	99	Satra	S24P	24	no	-	-
39	A - Lab A411	100	Satra	S24P	24	no	-	-
40	A - Lab A412	101	Satra	S24P	24	no	-	-
41	A - Lab A413	102	Satra	S24P	24	no	-	-

	Pabellón B							
42	B - Piso 1 SW01	103	Edimax	E24P	24	no	-	-
43	B - Piso 1 SW02	104	Edimax	E24P	24	no	-	-
44	B - Lab B409	107	Edimax	E24P	24	no	-	-
	Pabellón C							
45	C - Piso 4 SW01	108	Satra	S24P	24	no	-	-
	Pabellón D							
46	D - Lab 404 SW01	116	Satra	S24P	24	no	-	-
47	D - Lab 405 SW01	117	Satra	S24P	24	no	-	-
48	D - Lab 407 SW01	118	Satra	S24P	24	no	-	-
	Esclavas							
49	Esclavas 1 - SW01	119	Satra	S24P	48	no	-	-
50	Esclavas 1 - SW01 EPG	120	Satra	S24P	48	no	-	-
51	Esclavas 2 - SW01	122	Satra	S24P	48	no	-	-
52	Esclavas 2 - SW02 EPG	123	Satra	S24P	24	no	-	-
	Samuel Velarde 303, 305							
53	SVelarde 305 - SW01	125	Satra	HPv1910	48	no	-	-
54	SVelarde 305 - SW02	126	Satra	S24P	24	no	-	-
	San Jose C3, D3							
55	San Jose C3 01	128	Satra	6248	48	no	-	-
56	San Jose D3 01	130	Satra	3C2250	50	no	-	-

Tabla 4.5-5: Equipamiento actual 2
Fuente: Elaboración Propia

4.5.4.3. Tecnologías

4.5.4.3.1. LAN

Dentro de las tecnologías LAN se encuentran implementadas las siguientes:

- Fast Ethernet
- Gigabit Ethernet

4.5.4.3.2. WAN

El enlace WAN es un circuito digital de 8 Mbps de ancho de banda, siendo el proveedor de Telefónica del Perú.

La conexión se realiza mediante el router Cisco 2801 y el CSU/DSU M1000 Huawey siendo el medio por el cual llega la señal: fibra óptica.

4.5.4.4. Cableado

El cableado implementado a la fecha es el siguiente:

- **Backbone**

  La fibra óptica negra tendida en el campus de la universidad tiene las siguientes características:

  - Fibra Óptica: Multimodo 50um OM3, OFNR
  - Marca: Panduit, Newlink
  - Distancia Máxima: 220m
  - Conector: SC a ST, LC a ST.

- **Core**

  El equipo core conecta a los equipos de distribución, este se conectada al Patch panel de fibra de backbone mediante el siguiente medio:

  - Fibra Óptica: Patch Multimodo 50/125um
  - Marca: Siemon
  - Distancia Máxima: 3m
  - Conector: LC a LC.

  El equipo core conecta a los servidores directamente, mediante el siguiente medio:

  - Cobre: UTP Categoría 5e, 6
  - Marca: Belden, AT&T
  - Distancia Máxima: 10m
  - Conector: RJ45

- **Distribución**

  Los equipos de distribución están conectados hacia el panel de fibra de cada gabinete de cableado, mediante el siguiente medio:

  - Fibra Óptica: Patch Multimodo 62.5/125um, 50/125um
  - Marca: Siemon, Genérico
  - Distancia Máxima: 2m

  Los equipos switch o hubs de acceso están conectados hacia el Patch panel de cobre de cada gabinete de cableado, mediante el siguiente medio:

  - Cobre: UTP Categoría 5, 5e, 6
  - Marca: Belden, AT&T
  - Distancia Máxima: 90m

  Algunos equipos finales están directamente conectados al switch de distribución estos están hacia el Patch panel de cobre de cada gabinete de cableado y en el otro extremo en la placa de pared terminal, mediante el siguiente medio:

  - Cobre: UTP Categoría 5, 5e
  - Marca: Belden, AT&T
  - Distancia Máxima: 90m

- **Acceso y cascadas adicionales**

  Los equipos finales están directamente conectados hacia el Patch panel de cobre de cada gabinete de cableado y en el

otro extremo en la placa de pared terminal, mediante el siguiente medio:

- Cobre: UTP Categoría 5, 5e,
- Marca: Belden, AT&T
- Distancia Máxima: 90m

Los equipos switch o hubs que se conectan de manera irregular “cascada” están conectados hacia el Patch panel de cobre de cada gabinete de cableado, mediante el siguiente medio:

- Cobre: UTP Categoría 5, 5e,
- Marca: Belden, AT&T
- Distancia Máxima: 90m

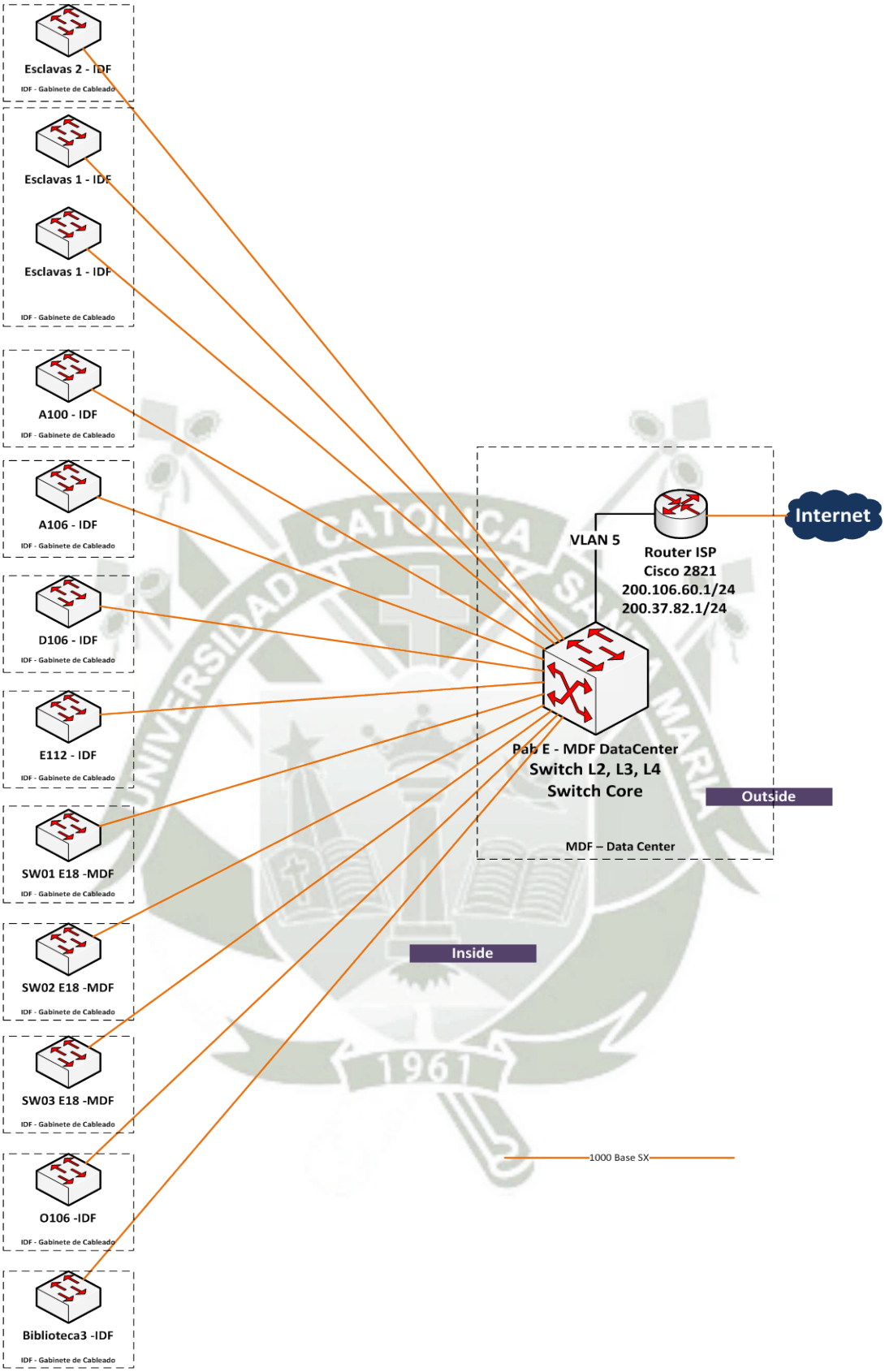

Figura 4.5-8: Cableado Data Center
Fuente: Elaboración Propia

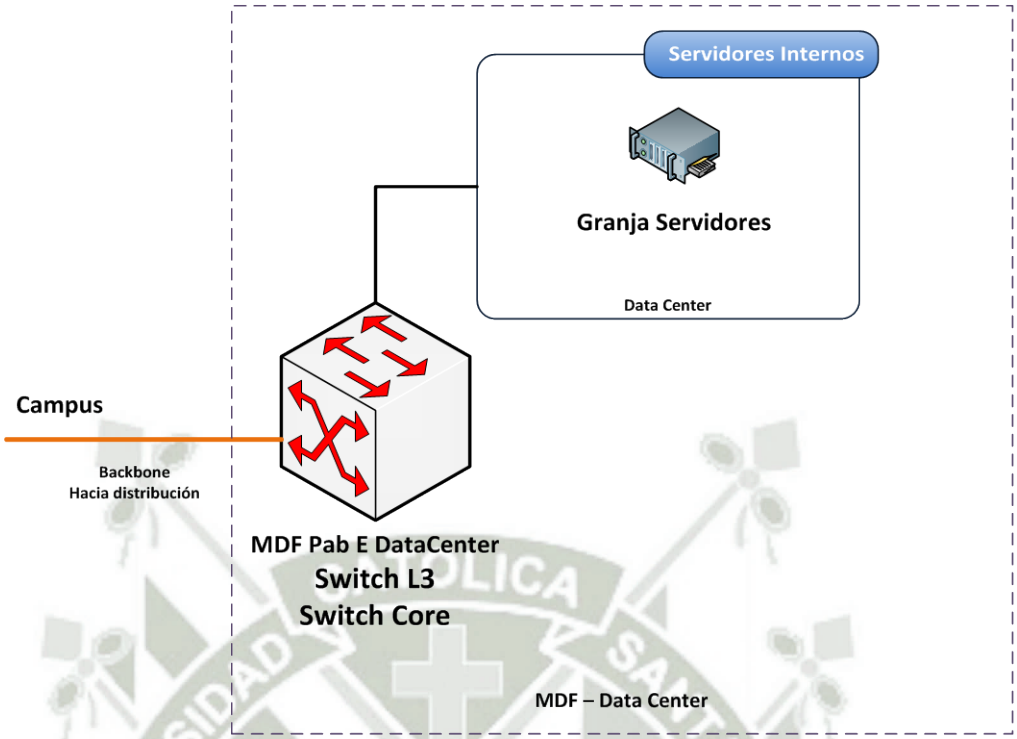

Figura 4.5-9: Cableado Data Center
Fuente: Elaboración Propia

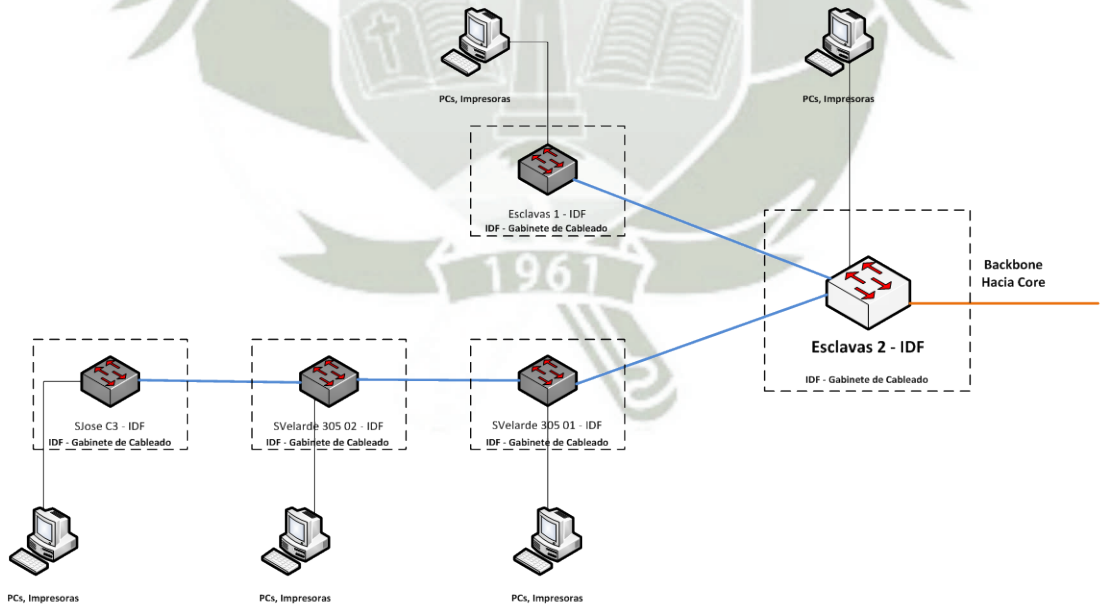

Figura 4.5-10: Cableado Campus
Fuente: Elaboración Propia

4.6. Diseño lógico propuesto

4.6.1. Topología de red

4.6.1.1. Diseño jerárquico

Enterprise

La topología para la zona Enterprise, esto incluye granja de servidores internos, los servicios publicados en la DMZ y la delimitación de las zonas indicada por el firewall.

En resumen se cuenta con las siguientes áreas:

- Granja de servidores: cuenta con los siguientes componentes:
  - Servidores Internos
  - Servidores de Seguridad
  - Servidores de Administración

- DMZ - Granja de servidores: cuenta con los siguientes componentes:
  - Servidores DMZ 1
  - Servidores DMZ 2

- Campus: está compuesta por todos los dispositivos que forman parte de la red de campus.

- WAN: cuenta con los siguientes componentes:
  - Router
  - CSU/DSU

En la siguiente figura se detalla:

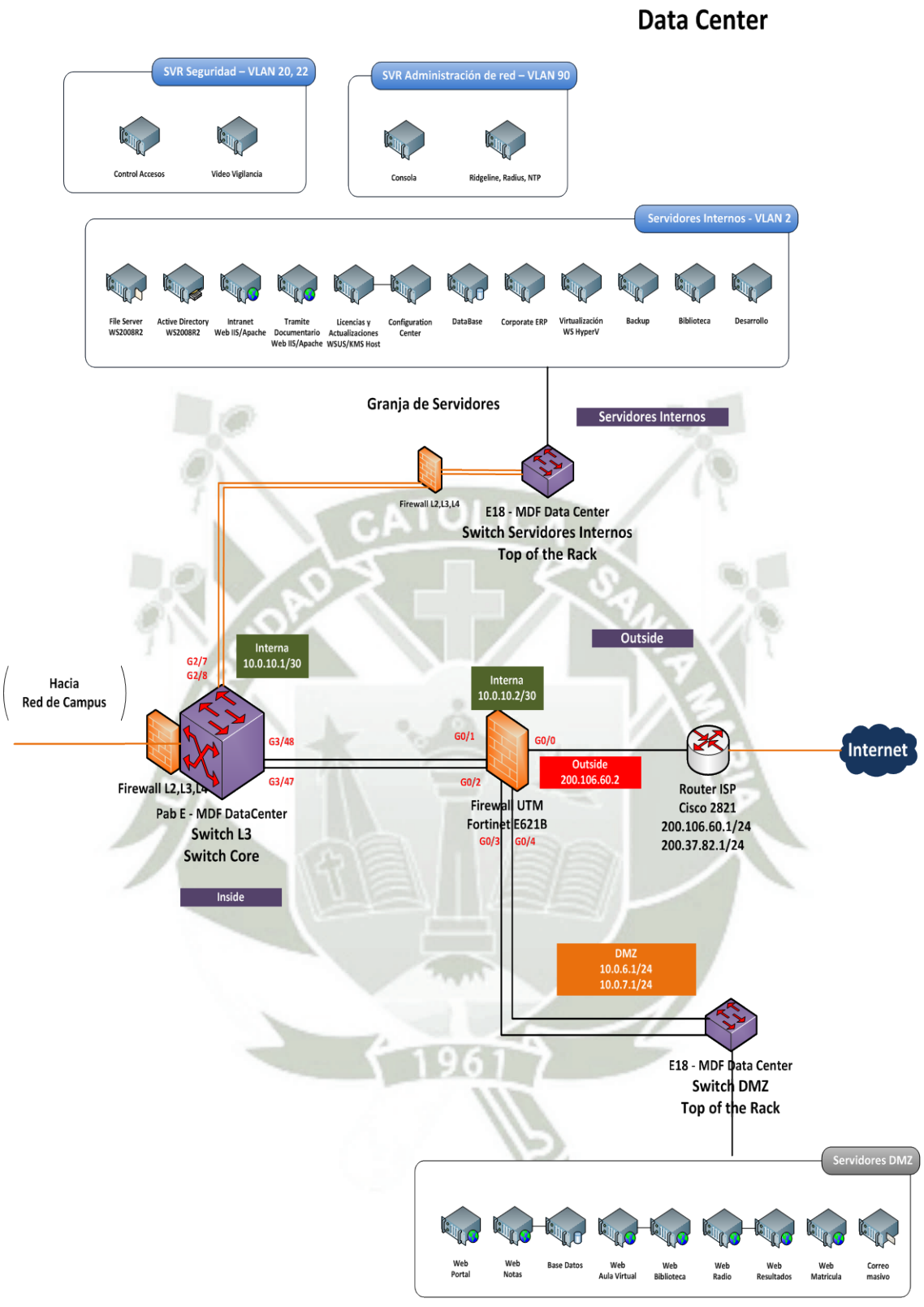

Figura 4.6-1: Diseño Enterprise
Fuente: Elaboración Propia

Campus

La topología para el campus elegida en primera instancia es la topología estrella extendida con las tres capas delimitadas (Core, Distribución y Acceso), se recomienda que sea una estrella extendida Half-Mesh el cual puede ser implementado de manera flexible sin alterar el diseño en una implementación futura.

En el siguiente grafico se presenta el diseño propuesto, el cual como se detalló en el mapa de red de la configuración anterior (red actual Mayo 2011) está dividido en las siguientes zonas:

- Zona Data Center: Incluye todos los equipos de data center.
- Zona Campus 1: Incluye los equipos que están distribuidos por los pabellones A, B, C, D, Chaminade, San Jose D3.
- Zona Campus 2: Incluye los equipos que están distribuidos por los pabellones E, F, G, H, I, O.
- Zona Campus 3: Incluye los equipos que están distribuidos por los pabellones Biblioteca, L, R, S.
- Zona Campus Esclavas: Incluye los equipos que están distribuidos por los pabellones Esclavas Nivel 1, Esclavas Nivel 2, Samuel Velarde 303, Samuel Velarde 305, San Jose C3.

El detalle de las zonas presentan se muestra a continuación:

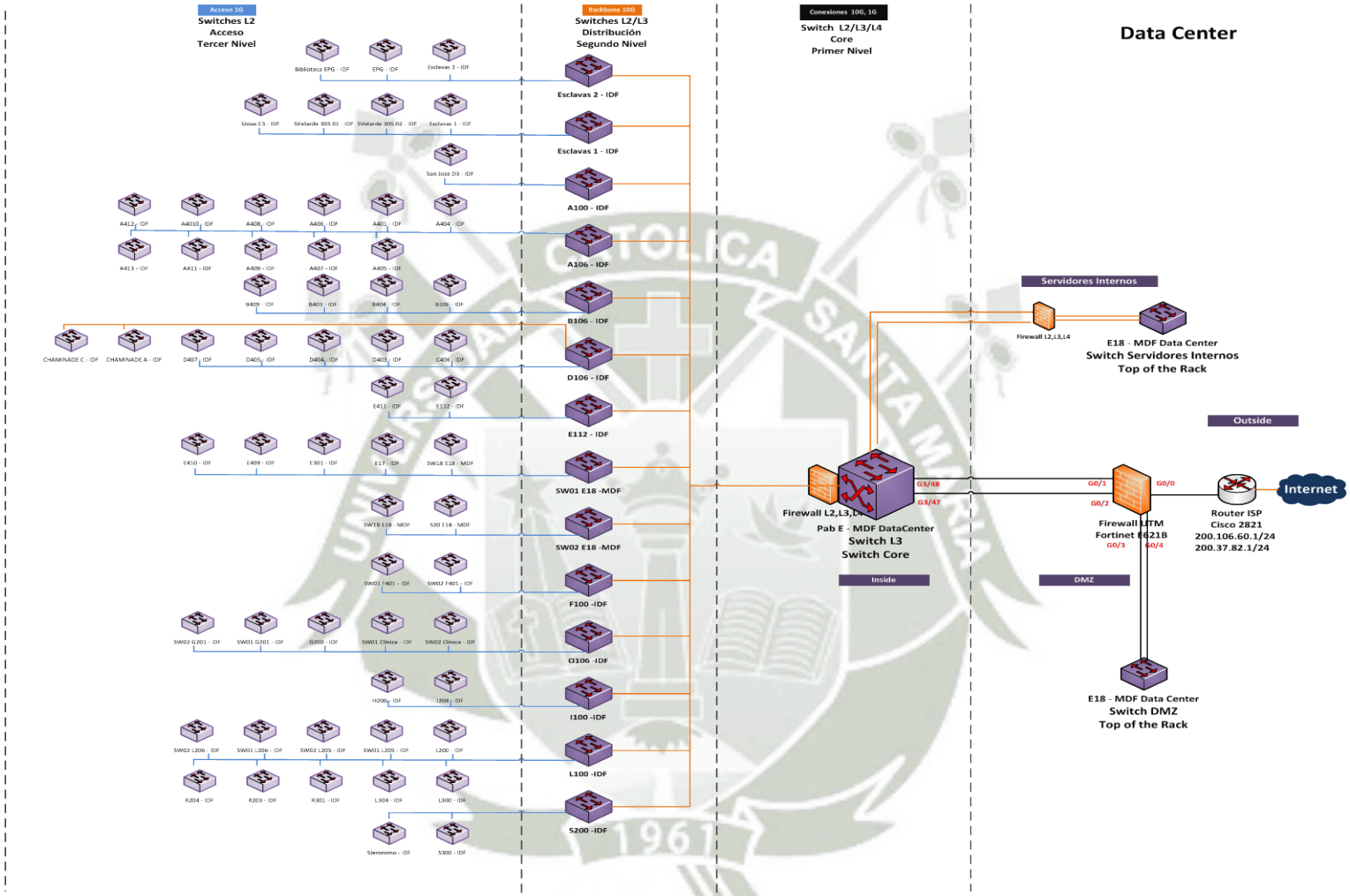

Figura 4.6-2: Diseño Campus
Fuente: Elaboración Propia

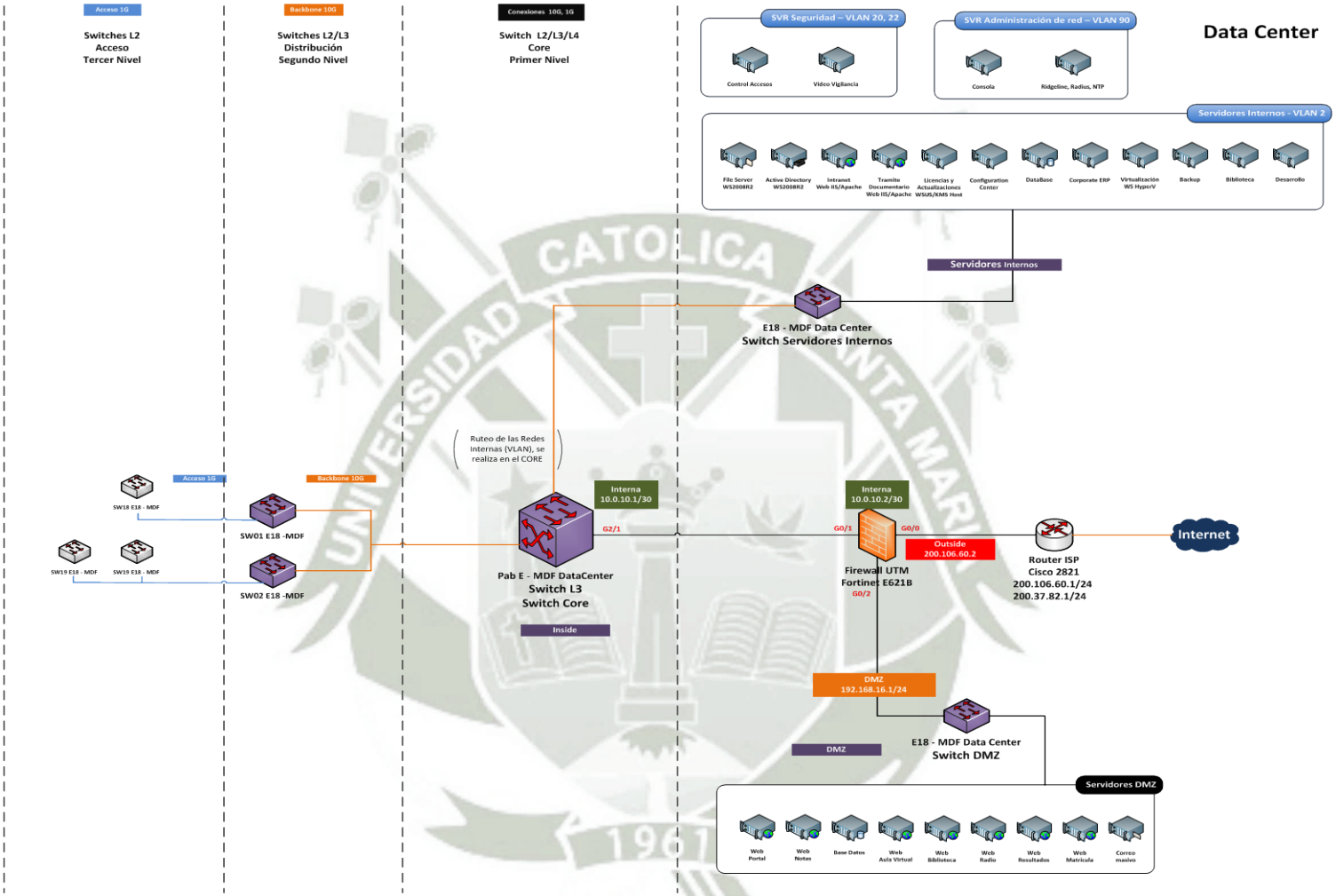

Figura 4.6-3: Diseño Zona Data Center
Fuente: Elaboración Propia

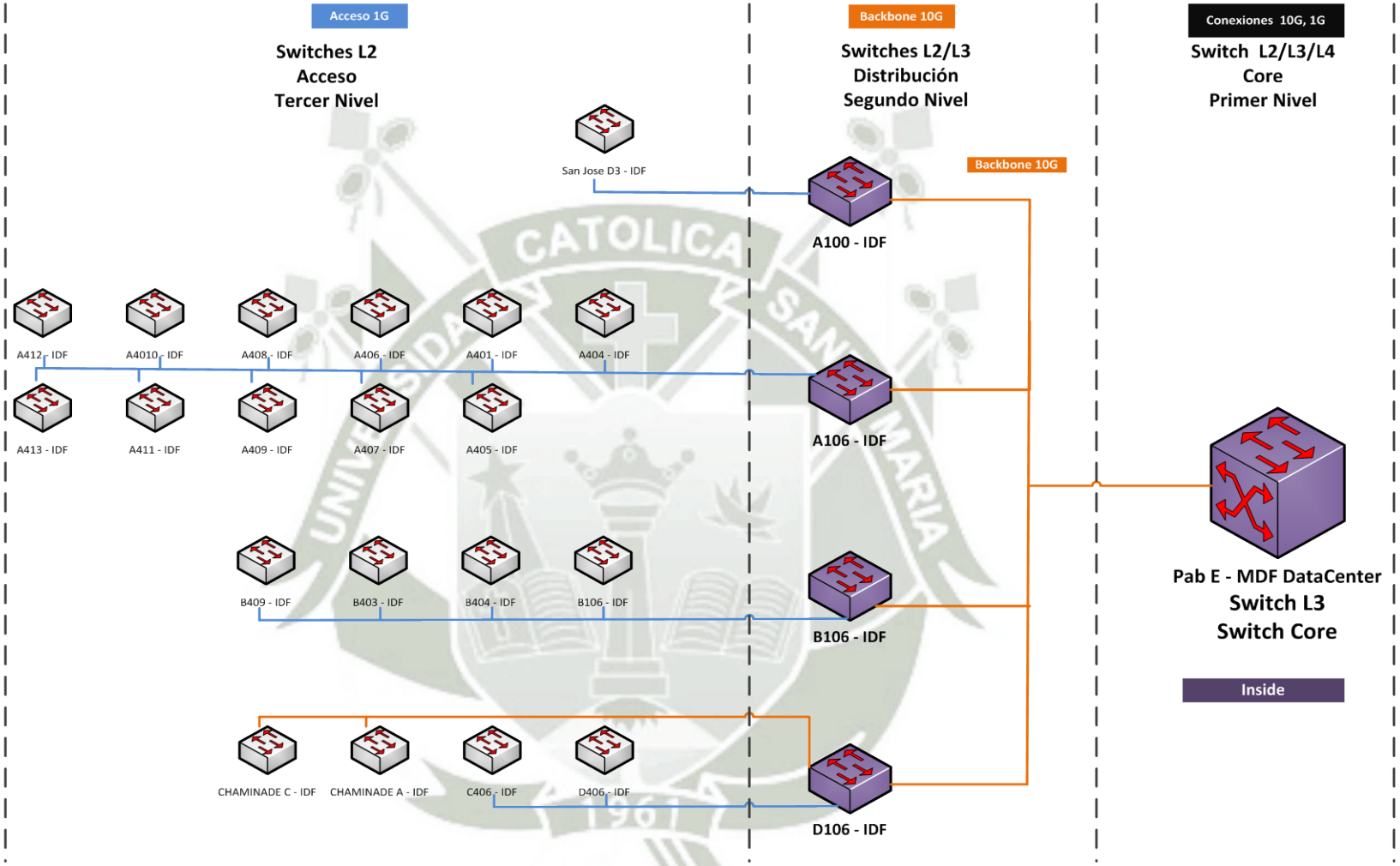

Figura 4.6-4: Diseño Zona Campus 1
Fuente: Elaboración Propia

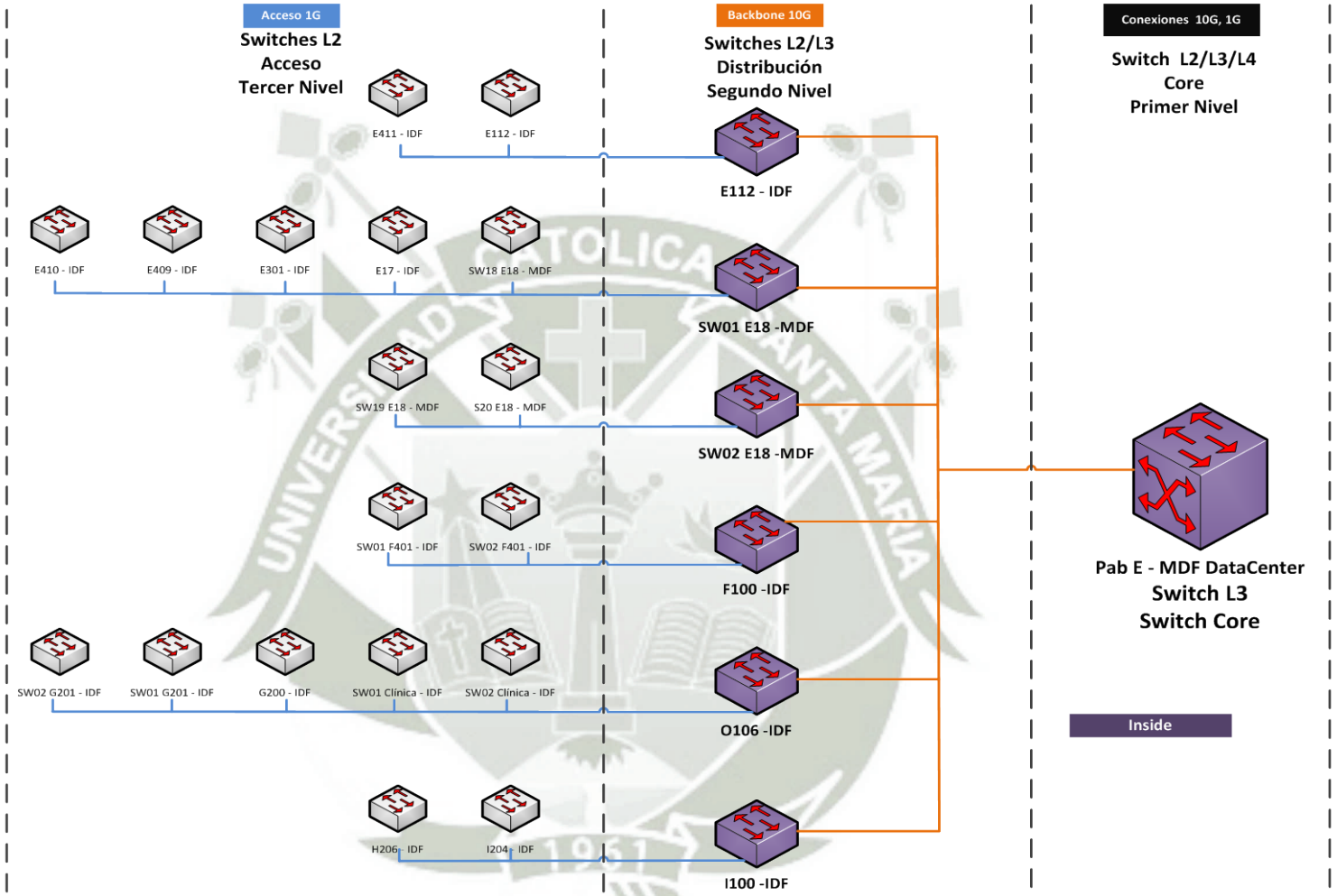

Figura 4.6-5: Diseño Zona Campus 2
Fuente: Elaboración Propia

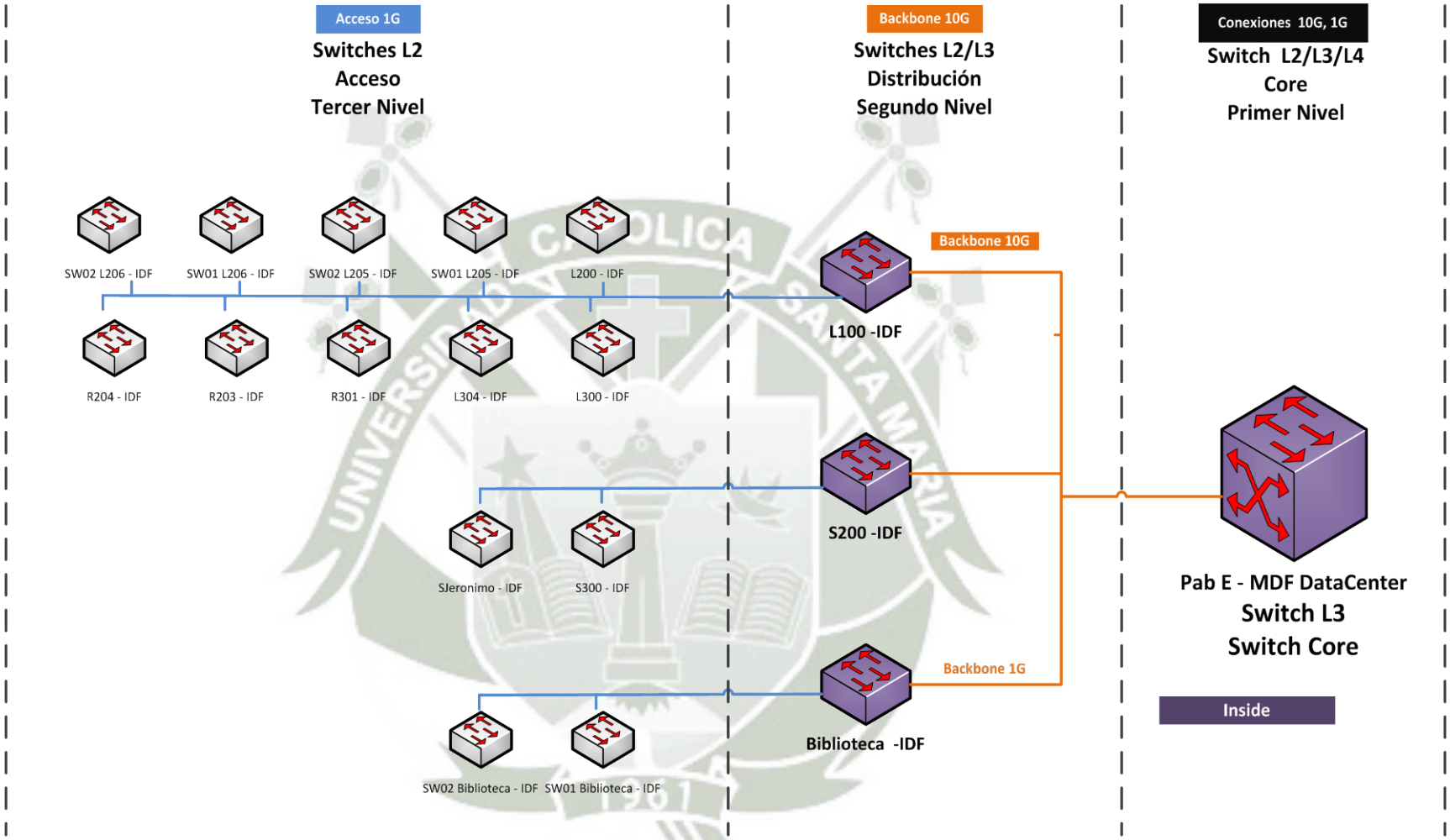

Figura 4.6-6: Diseño Zona Campus 3
Fuente: Elaboración Propia

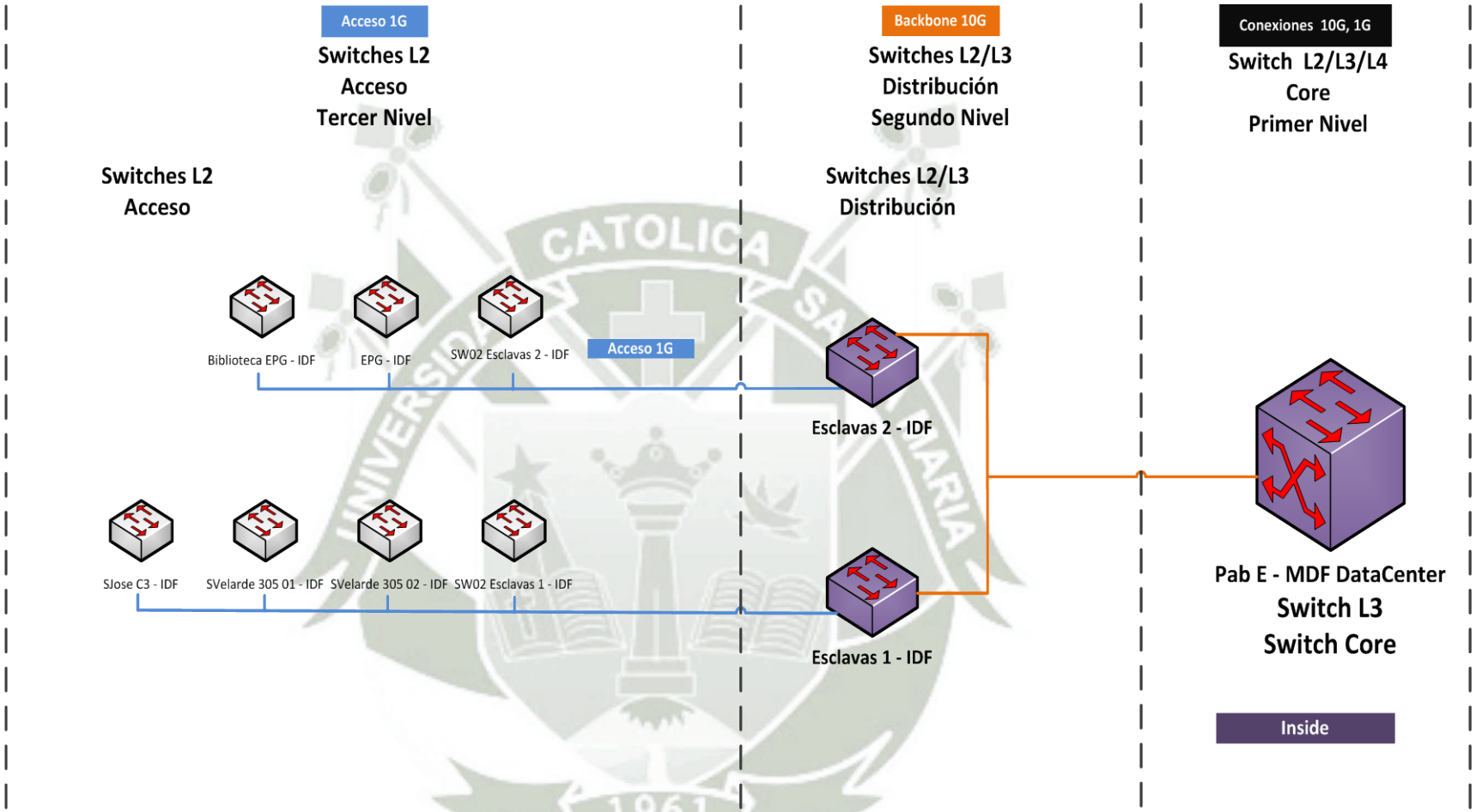

Figura 4.6-7: Diseño Zona Esclavas
Fuente: Elaboración Propia

4.6.2. Direccionamiento

Para el direccionamiento, segmentación y creación de las VLANs correspondientes, se tomaran en cuenta las áreas que llevan correspondencia unas con otras.

- Área Servidores Internos
- Área Servidores DMZ
- Área administración de Data Center
- Área administración de hardware
- Áreas Administrativas
- Áreas Laboratorios

4.6.2.1. Estructura del Modelo a implementar

Se basara en el direccionamiento privado RFC 1918 y se empleara el bloque de direcciones privadas clase A y se subneteará de acuerdo a las necesidades de la UCSM.

El modelo a implementar se basa en los siguientes parámetros, tomando en cuenta que este modelo solo se utilizara para la red Enterprise y de Campus:

- **Red a utilizar**: 10.0.0.0/8 → Clase A

- **Bloque 1**: Prefijo de red clase A
  - Único valor: 10

- **Bloque 2:** Identificador de la zona
  - Número máximo de bits: 8
  - Número máximo de zonas: 256
  - Las zonas son:

    - 0: Campus Umacollo

- 1: Campus Parque Industrial
- 2: Campus Huasacache
- 3: Instituto Confucio
- 4: Apoyo Jurídico
- 5: Museo Santuarios Andinos
- 6: Museo Arqueología
- 7: Campus Majes

- **Bloque 3**:Identificador de red o VLAN
  - Número máximo de bits: 19
  - Número máximo de redes o VLANs por zona: 224 (desde la vlan 2 hasta la vlan 224)
  - Las VLAN y sus detalla se presentaran en el siguiente punto 4.6.2.2

- **Bloque 4**: Identificador de host
  - Máxima Cantidad de bits para host: 13
  - Número máximo de host por vlan: 8190

- **Mascara de red**: Número variable según la cantidad de host necesarios.
  - Mínima cantidad de bits en mascara: 19

10	X	X	X
Identificador de Clase	***Identificador de Zona***	***Identificador de Red o VLAN***	***Identificador de Host***
Valor Único	Bits Max = 8	Bits Max = 3	Bits Max = 13

Figura 4.6-8: Estructura de direccionamiento
Fuente: Elaboración Propia

4.6.2.2. Detalle de Segmentos

El detalle de los segmentos se presenta a continuación:

- **Área Servidores Internos**: Se tienen los siguientes tipos de servidores internos:

  - **Operativos**: son todos los servicios que forman parte del Core Bussiness de la UCSM y que tienen mayor flujo de tráfico debido a que las aplicaciones se encuentran en este segmento.

Ítem	Descripción	Disp.	Nombre	Vlan	Mas.	Dir. Red
Servidores Internos						
1	Servidores Internos	**254**	SVR_Internos	80	24	10.0.80.0/24

Tabla 4.6-1: Resumen VLANs Servicios Internos
Fuente: Elaboración Propia

- **Área Servidores DMZ**: Se tienen los siguientes tipos de servidores publicados:

  - **DMZ servicios internos**: alberga los servicios publicados por la UCSM y que los administra directamente.
  - **DMZ servicios tercerizados**: alberga los servicios publicados por la UCSM y que es administrado por algún proveedor u persona fuera del área de TI.

Ítem	Descripción	Disp.	Nombre	Vlan	Mas.	Dir. Red
Servidores Publicados – DMZ						
1	Servidores DMZ 1	**254**	SVR_DMZ1	70	24	10.0.70.0/24
2	Servidores DMZ 2	**254**	SVR_DMZ2	71	24	10.0.71.0/24

Tabla 4.6-2: Resumen VLANs Servicios Publicados
Fuente: Elaboración Propia

- **Área Servicios de Seguridad**: Se tienen los siguientes tipos de servidores internos:

  - **Seguridad**: Son los servicios que registran los accesos al campus y las grabaciones de video (Cámaras IP) por la red de datos. A continuación se detalla:

    - **Control de Accesos**: Es el servicio que guardan los accesos de cada tarjeta de proximidad que es utilizada para el ingreso o salida del campus.

    - **Video Vigilancia**: Es el servicio que monitorea y graba en línea los sucesos de las diversas cámaras IP distribuidas por toda las UCSM.

Ítem	Descripción	Disp.	Nombre	Vlan	Mas.	Dir. Red
Servicios de Seguridad						
1	Control de Acceso	**14**	Seg_Control_Accesos	60	28	10.0.60.0/28
2	Cámaras 1	**254**	Seg_Camaras_1	62	24	10.0.62.0/24
		-				

Tabla 4.6-3: Resumen VLANs Servicios de Seguridad
Fuente: Elaboración Propia

- **Área de administración de hardware** : Se tienen los siguientes tipos de administración:

  - Son los servicios que administran los dispositivos de red que pueden ser administrables y que se encuentran por todo el campus de la UCSM.

- Switches
- Access Points
- Data Center
- Proyectores
- UPS

Ítem	Descripción	Disp.	Nombre	Vlan	Mas.	Dir. Red
Servicios de Administración						
1	Switches	**254**	Mgmt_Switches	30	24	10.0.30.0/24
2	Access Points	**254**	Mgmt_Aps	31	24	10.0.31.0/24
3	Data Center	**254**	Mgmt_Datacenter	32	24	10.0.32.0/24
4	Proyectores	**254**	Mgmt_Proyectores	33	24	10.0.33.0/24
5	UPS	**254**	Mgmt_Ups	34	24	10.0.34.0/24

Tabla 4.6-4: Resumen VLANs Administración
Fuente: Elaboración Propia

- **Áreas Administrativas**: Según la estructura de la UCSM se tiene:
  - Unidad Administrativa Rectorado y dependencias
  - Unidad Administrativa Vicerrectorado Académico y dependencias.
  - Unidad Administrativa Vicerrectorado Administrativo y dependencias.
  - Unidades Académicas
  - Campus:
    - Organismos Autónomos
    - Representaciones Gremiales
    - Otros Organismos
    - Reniec
    - Auditoria Externa

En el siguiente cuadro se plantean las VLANs de las áreas administrativas:

Ítem	Descripción	Act.	Adic.	Tot.	Disp.	Nombre	Vlan	Mas.	Dir. Red
Unidad Administrativa – Rectorado									
1	Rectorado	*4*	*1*	**5**	**14**	ADM_Rectorado	2900	28	10.0.221.0/28
2	Oficinas Dependientes	*58*	*6*	**64**	**254**	ADM_Rectorado_dep	2901	24	10.0.221.0/24
3	Oficina de Informática	*34*	*4*	**38**	**126**	ADM_Informatica	2902	25	10.0.222.0/25
Unidad Administrativa - Vicerrectorado Académico									
4	Vicerrectorado Académico	*7*	*1*	**8**	**14**	ADM_Vracad	2910	28	10.0.230.0/28
5	Oficinas Dependientes	*40*	*4*	**44**	**254**	ADM_Vracad_dep	2911	24	10.0.231.0/24
6	Biblioteca	*42*	*4*	**46**	**126**	ADM_Biblioteca	2913	25	10.0.233.0/25
7	Admisión	*9*	*1*	**10**	**32**	ADM_Admision	2914	27	10.0.234.0/27
8	Centro Pre Universitario	*9*	*1*	**10**	**32**	ADM_Cpu	2915	27	10.0.235.0/27
Unidad Administrativa - Vicerrectorado Administrativo									
9	Vicerrectorado Administrativo	*5*	*1*	**6**	**14**	ADM_Vradm	2920	28	10.0.250.0/28
10	Oficinas Dependientes	*56*	*6*	**62**	**254**	ADM_Vradm_dep	2921	24	10.0.251.0/24
11	Contabilidad	*15*	*2*	**17**	**62**	ADM_Contabilidad	2922	26	10.0.252.0/26
12	Impresiones	*10*	*6*	**16**	**30**	ADM_Cimpresiones	2923	27	10.0.253.0/27
Unidades Académicas									
12	Facultades Pregrado	*125*	*13*	**138**	**254**	ADM_Pregrado	2930	24	10.0.260.0/24
13	Escuela de Posgrado	*9*	*2*	**11**	**30**	ADM_Postgrado	2931	27	10.0.261.0/27
14	Institutos	*15*	*2*	**17**	**30**	ADM_Institutos	2932	27	10.0.262.0/27
15	Clínicas	*10*	*2*	**12**	**30**	ADM_Institutos	2933	27	10.0.263.0/27
Campus									
16	Organismos Autónomos	*8*	*1*	**9**	**14**	CA_OR_Autonomos	2940	27	10.0.270.0/27
17	Representaciones Gremiales	*15*	*2*	**17**	**30**	CA_OR_RG	2941	27	10.0.271.0/27
18	Otros Organismos	*3*	*1*	**4**	**14**	CA_OR_otros	2942	28	10.0.272.0/28
19	Porterías	*6*	*1*	**7**	**14**	CA_Porterias	2943	28	10.0.273.0/28
20	Reniec	*3*	*1*	**4**	**14**	CA_OR_Reniec	2944	28	10.0.274.0/28
21	Auditoria Externa	*5*	*1*	**6**	**14**	CA_OR_Auditoria	2945	28	10.0.275.0/28

Tabla 4.6-5: Resumen VLANs Administrativas
Fuente: Elaboración Propia

En los siguientes cuadros se plantean las VLANs de las áreas administrativas detalladas:

Ítem	Descripción		Jef.	Proc.	Sec.	Prac.	Imp.	Act.	Adic.	Tot.	Disp.	Nombre	Vlan
Unidad Administrativa - Rectorado													
1	**Rectorado**		1	0	2	0	1	4	1	5	14	ADM_Rectorado	2900
	1.1	Rectorado	1	0	2	0	1						
2	**Rectorado - Dependencias**		9	23	6	10	10	58	6	64	254	ADM_Rectorado_dep	2901
	2.1	Secretaria General	1	5	1	0	2						
	2.2	OF. Asesoría Jurídica	1	2	0	0	1						
	2.3	OF Auditoria Interna	1	3	0	0	1						
	2.4	OF Autoevaluación	1	4	1	0	1						
	2.5	OF Asesoría del Rectorado	1	0	0	0							
	2.6	OF. Relaciones Intl.	1	2	1	6	1						
	2.7	OF. Figura	1	5	1	4	2						
	2.8	OF. Planeamiento	1	2	1	0	1						
	2.9	OF. Seguimiento de Grad.	1	0	1	0	1						
3	**Rectorado - Dependencias**		1	20	3	6	4	34	4	38	126	ADM_Informatica	2902
	3.1	OF. Informática	1	20	3	6	4						
Unidad Administrativa - Vicerrectorado Académico													
4	**VRACAD**		1	0	4	0	2	7	1	8	14	ADM_Vracad	2910
	4.1	Vic. Académico	1	0	4	0	2						
5	**VRACAD - Dependencias**		8	7	9	6	10	40	4	44	254	ADM_Vracad_dep	2911
	5.1	Secretaria Académica	1	0	2	0	1						
	5.2	OF. Registro Académico	1	7	1	0	4						
	5.3	Desarrollo Académico	1	0	1	0	1						
	5.4	Extensión Universitaria	1	0	1	0	1						
	5.5	CICA	1	0	1	6	1						
	5.6	Cempos	1	0	1	0	0						
	5.7	Coord. de Labs. y Gab.	1	0	1	0	1						
	5.8	Tutoría Universitaria	1	0	1	0	1						
6	**VRACAD – Dependencias**		1	36	1	0	4	42	4	46	126	ADM_Biblioteca	2913
	6.1	Bibliotecas	1	36	1	0	4						
7	**VRACAD – Dependencias**		2	4	1	0	2	9	1	10	30	ADM_Admision	2914
	7.1	OF. Admisión	2	4	1	0	2						
8	**VRACAD – Dependencias**		2	4	1	0	2	9	1	10	30	ADM_Cpu	2915
	8.1	CPU	2	4	1	0	2						

Tabla 4.6-6: Detalle VLANs Administrativas 1
Fuente: Elaboración Propia

Ítem	Descripción		Jef.	Proc.	Sec.	Prac.	Imp.	Act.	Adic.	Tot.	Disp.	Nombre	Vlan
Unidad Administrativa - Vicerrectorado Administrativo													
9	**VRADM**		1	3	0	0	1	5	1	6	14	ADM_Vradm	2920
	9.1	Vic. Administrativo	1	3	0	0	1						
10	**VRADM - Dependencias**		8	25	11	3	9	56	6	62	254	ADM_Vradm	2921
	10.1	Secretaria Administrativa	1	0	1	0	1						
	10.2	OF. Presupuesto	1	1	1	0	1						
	10.3	OF. Bienestar	1	6	6	0	1						
	10.4	OF. Infraestructura	1	4	1	2	2						
	10.5	OF. Seguridad Institucional	1	1	0	0	1						
	10.6	OF. Logística	1	3	1	0	1						
	10.7	OF. Recursos Humanos	1	5	1	1	1						
	10.8	CEPROBIS	1	5	0	0	1						
11	**VRADM - Dependencias**		1	11	1	0	2	15	2	17	62	ADM_Contabilidad	2922
	12.1	OF. Contabilidad	1	11	1	0	2						
12	**VRADM - Dependencias**		1	1	0	0	8	10	6	16	30	ADM_Cimpresiones	2923
	11.1	Impresiones	1	1	0	0	8						
Unidad Académicas													
13	**Pregrado**		53	12	40	5	15	125	13	138	254	ADM_Pregrado	2930
	13.1	Fac. de CS. Contables	3	1	2	0	1						
	13.2	FCEA	4	1	4	1	1						
	13.3	FCJP	3	1	3	0	1						
	13.4	FCTSH	9	1	7	1	2						
	13.5	Fac. de Odontología	3	1	3	0	1						
	13.6	Fac. de Obstetricia	3	1	1	1	1						
	13.7	Fac. Enfermería	3	1	1	1	1						
	13.8	FCFBB	4	1	2	0	1						
	13.9	Fac. Medicina Humana	4	1	3	1	1						
	13.10	FCIFF	7	1	6	0	3						
	13.11	FCIBQ	5	1	5	0	1						
	13.12	FAICA	5	1	3	0	1						
14	**Postgrado**		3	1	5	0	0	9	2	11	30	ADM_Postgrado	2931
	14.1	Escuela de Postgrado	3	1	5	0	0						
15	**Institutos**		3	3	3	3	3	15	2	17	30	ADM_Postgrado	2932
	15.1	Informática	1	1	1	1	1						
	15.2	Idiomas	1	1	1	1	1						
	15.3	Confucio	1	1	1	1	1						
16	**Clínicas**		2	4	0	2	2	10	2	12	30	ADM_Postgrado	2933
	16.1	Odontológica	1	2	0	1	1						
	16.2	Veterinaria	1	2	0	1	1						

Tabla 4.6-7: Detalle VLANs Administrativas 2
Fuente: Elaboración Propia

Ítem	Descripción		Jef.	Proc.	Sec.	Prac.	Imp.	Act.	Adic.	Tot.	Disp.	Nombre	Vlan
Campus													
17	**Organismos Autónomos**		2	3	1	1	1	8	1	9	30	CA_OR_Autonomos	2940
	17.1	Comité Electoral	1	0	1	1	1						
	17.2	Tribunal de Honor	1	3	0	0	0						
18	**Representaciones Gremiales**		3	5	4	0	3	15	2	17	30	CA_OR_RG	2941
	18.1	ADUCA	1	4	2	0	1						
	18.2	SUTNDUCSM	1	0	1	0	1						
	18.3	SADUC	1	1	1	0	1						
19	**Otros Organismos**		0	3	0	0	0	3	1	4	14	CA_OR_otros	2942
	19.1	AISEC	0	1	0	0	0						
	19.2	LIBUM	0	1	0	0	0						
	19.3	ACAP	0	1	0	0	0						
	19.3	Cafetería	0	0	0	0	0						
20	**Porterías**		0	6	0	0	0	6	1	7	14	CA_Porterias	2943
	20.1	Porterías	0	6	0	0	0						
21	**Reniec**		0	2	0	0	1	3	1	4	14	CA_OR_Reniec	2944
	21.1	Reniec	0	2	0	0	1						
22	**Auditoria Externa**		1	4	0	0	0	5	1	6	14	CA_OR_Auditoria	2945
	22.1	Auditoria Externa	1	4	0	0	0						

Tabla 4.6-8: Detalle VLANs Administrativas 3
Fuente: Elaboración Propia

- **Áreas de Laboratorios o Académicas**: Según la estructura de la UCSM se tiene las siguientes áreas académicas:
  - Ciencias Sociales
  - Ciencias Jurídicas y Empresariales
  - Ciencias de la Salud
  - Ciencias e ingenierías
  - Escuela de Postgrado
  - Campus
  - Otras Áreas

  En el siguiente cuadro se plantean las VLANs de las áreas de laboratorios o académicas:

Ítem	Descripción	Act.	Adic.	Tot.	Disp.	Nombre	Vlan	Mas.	Dir. Red
Ciencias Sociales									
1	**Fac. Cs. Sociales**	*91*	*21*	**112**	**254**	ACAD_fctsh	2951	24	10.0.191.0/24
	FCTSH								
					-				
Ciencias Jurídicas Empresariales									
2	**Fac. Cs. Jurídicas Empresar.**	*109*	*21*	**130**	**254**	ACAD_cje	2953	24	10.0.193.0/24
	FCCF								
	FCEA								
	FCJP								
					-				
Ciencias de la Salud									
3	**Fac. Cs de la Salud**	*21*	*21*	**42**	**254**	ACAD_cs	2954	24	10.0.194.0/24
	Facultad de Enfermería								
	Facultad de Medicina								
	Facultad de Odontología								
	FCFBB								
	Facultad de Obstetricia								
					-				
Ciencias e Ingenierías									
4	FCIBQ	*21*	*21*	**42**	**254**	ACAD_fcibq	2956	24	10.0.206.0/24
5	FAICA	*56*	*10*	**66**	**254**	ACAD_faica	2957	24	10.0.207.0/24
6	P.P Ing. Industrial, Minas	*64*	*21*	**85**	**254**	ACAD_ppindustrial	2958	24	10.0.208.0/24
7	P.P Ing. de Sistemas	*117*	*0*	**117**	**254**	ACAD_ppsistemas	2959	24	10.0.209.0/24
8	P.P. Ing. Mecánica	*91*	*21*	**112**	**254**	ACAD_ppmecanica	2960	24	10.0.200.0/24
9	P.P. Ing. Electrónica	*77*	*21*	**98**	**254**	ACAD_ppelectronica	2961	24	10.0.201.0/24
					-				
Escuela de Postgrado									
10	Escuela de Post Grado	*34*	*21*	**55**	**126**	ACAD_epg	2963	25	10.0.203.0/25
					-				
Campus									
11	Aulas Campus	*120*	*12*	**132**	**254**	ACAD_Aulas	2964	24	10.0.204.0/24
12	SUM	*12*	*0*	**12**	**30**	CA_Sum	2965	27	10.0.205.0/27
13	Auditorios	*6*	*2*	**8**	**14**	CA_Auditorios	2966	28	10.0.206.0/28
					-				
Otras Áreas									
14	Biblioteca Virtual	*62*	*10*	**72**	**126**	ACAD_bvirtual	2971	25	10.0.201.0/25
15	Estadística	*25*	*2*	**27**	**62**	ACAD_estadistica	2972	26	10.0.202.0/26
16	Proyecto Mercurio	*14*	*2*	**16**	**30**	ACAD_pmercurio	2973	27	10.0.203.0/27
17	CICA	*14*	*2*	**16**	**30**	ACAD_cica	2974	27	10.0.204.0/27
18	Internos FCFBB	*14*	*2*	**16**	**30**	ACAD_in_fcfbb	2975	27	10.0.205.0/27
					-				
Institutos									
19	Informática	*42*	*21*	**63**	**254**	ACAD_iinformatica	2981	24	10.0.201.0/24
20	Instituto de Idiomas	*66*	*66*	**132**	**254**	ACAD_iidiomas	2982	24	10.0.202.0/24

Tabla 4.6-9: Resumen VLANs Laboratorios o Académicas
Fuente: Elaboración Propia

En los siguientes cuadros se plantean las VLANs de las áreas académicas detalladas:

Ítem	Descripción	Coo.	Doc.	Alu.	Imp.	Act.	*Adic.*	Tot.	Disp.	Nombre	Vlan
Ciencias Sociales											
1	FCTSH	2	4	85	0	91	*21*	112	254	ACAD_fctsh	2951
	P.P. Comunicación Social	1	2	40	0						
	P.P. Teología	0	0		0						
	P.P. Psicología	0	1	20	0						
	P.P. Publicidad	1	1	25	0						
	P.P. Educación	0	0	0	0						
	P.P. Trabajo Social	0	0	0	0						
	P.P. Turismo y Hotelería	0	0	0	0						
Ciencias Jurídicas Empresariales											
2	Fac. Jurídicas y Empresariales	0	5	104	0	109	*21*	130	254	ACAD_cje	2953
	FCCF										
	P.P. Contabilidad	0	2	44	0						
	FCCA										
	P.P. Administración	0	1	20	0						
	P.P Ing. Comercial	0	1	20	0						
	FCJP										
	P.P. Derecho	0	1	20	0						
Ciencias de la Salud											
3	Fac. Cs. De la Salud	0	1	20	0	21	*21*	42	254	ACAD_cdls	2954
	Fac. de Enfermería										
	P.P. Enfermería	0	0	0	0						
	Fac. de Medicina Humana										
	P.P. Medicina Humana	0	0	0	0						
	Fac. de Odontología										
	P.P. Odontología	0	0	0	0						
	FCFBB										
	P.P. Ing. Biotecnológica	0	0	0	0						
	P.P. Farmacia	0	1	20	0						
	Fac. de Obstetricia										
	P.P. Obstetricia	0	0	0	0						
Ciencias e Ingenierías											
4	FCIBQ	0	1	20	0	21	*21*	42	254	ACAD_fcibq	2956
	P.P. Ing. Agronómica	0	0	0	0						
	P.P. Veterinaria	0	0	0	0						
	P.P. Ing. Alimentaria	0	1	20	0						
5	FAICA	2	2	50	2	56	*10*	66	254	ACAD_faica	2957
	P.P. Arquitectura	1	1	25	1						
	P.P. Ing. Civil	1	1	25	1						
	P.P. Ing. Ambiental	0	0	0	0						
	FCIFF										
6	P.P. Ing. Industrial y Minas	1	3	60	0	64	*21*	85	254	ACAD_ppindustrial	2958
	P.P. Ing. Industrial	1	3	60	0						
	P.P. Ing. de Minas	0	0	0	0						
7	P.P Ing. de Sistemas	2	8	107	0	117	*0*	117	254	ACAD_ppsistemas	2959
	P.P Ing. de Sistemas	2	8	107	0						
8	P.P. Ing. Mecánica	1	6	84	0	91	*21*	112	254	ACAD_ppmecanica	2960
	P.P. Ing. Mecánica	1	6	84	0						
9	P.P. Ing. Electrónica	1	4	72	0	77	*21*	98	254	ACAD_ppelectronica	2961
	P.P. Ing. Electrónica	1	4	72	0						

Tabla 4.6-10: Detalle VLANs Académicas 1
Fuente: Elaboración Propia

Ítem	Descripción	Coo.	Doc.	Alu.	Imp.	Act.	*Adic.*	Tot.	Disp.	Nombre	Vlan
Escuela de Post Grado											
10	Escuela de Posgrado	0	4	30	0	34	*21*	55	126	ACAD_epg	2963
	EPG	0	4	30	0						
Campus											
11	Aulas Campus - PC	0	120	0	0	120	*12*	132	254	ACAD_aulas	2964
12	SUM	0	12	0	0	12	*2*	14	30	CA_sum	2965
13	Auditorios	0	6	0	0	6	*2*	8	14	CA_auditorios	2166
Otras Áreas											
14	Biblioteca Virtual	1	1	60	0	62	*10*	72	126	ACAD_bvirtual	2971
15	Estadística	0	1	24	0	25	*2*	27	62	ACAD_estadistica	2972
16	Proyecto Mercurio	1	1	12	0	14	*2*	16	30	ACAD_mercurio	2973
17	CICA	0	1	12	0	13	*2*	15	30	ACAD_cica	2974
18	Laboratorios Internos FCFBB	8	0	0	2	10	*4*	14	30	ACAD_in_fcfbb	2975
Institutos											
19	Informática	0	2	40	0	42	*21*	63	254	ACAD_iinformatica	2981
20	Idiomas	0	2	64	0	66	*66*	132	254	ACAD_iidiomas	2982

Tabla 4.6-11: Detalle VLANs Académicas 2
Fuente: Elaboración Propia

4.6.2.3. Asignación

- **Dinámica**: Se recomienda que se realice el direccionamiento dinámico para las siguientes redes:
  - Administrativas
  - Académicas o Laboratorios

  Siempre y cuando se tenga un mecanismo de autenticación configurada e implementada como:

  - 802.1X
  - Netlogin
  - Identity Management
  - Servidor DHCP autenticado.
  - Active Directory y Radius
  - Autenticación, autorización y contabilización en el servicio de destino.

En caso de que no se cuente con los mecanismos de seguridad, se recomienda utilizar el direccionamiento estático.

- **Estático**: Se recomienda que se realice el direccionamiento estático para las siguientes redes:

  - Servidores Internos
  - Servidores Publicados
  - Servicios de Seguridad
  - Servicios de administración

  Además se recomienda que se aplique mecanismos de seguridad como:

  - 802.1X
  - Netlogin
  - Identity Management
  - Servidor DHCP autenticado.
  - Active Directory y Radius

4.6.3. Nombramiento

4.6.3.1. Modelo de VLAN

Los nombres de las VLANs son referenciales en algunas marcas esta se manejan mediante ID y en otras se manejan mediante el nombre.

Se propone para cada VLAN se asigne un nombre de acuerdo a un sufijo según la función principal, más el nombre del área u organismo, a continuación se detalla.

- **Prefijo: ACAD (ej. red Académica o Laboratorios)**
- **ID: epg (ej. Escuela de postgrado)**

- ACAD = Académica o Laboratorios
- ADM = Administrativa
- CA = Campus
- Mgmt = Administración
- SEG = Seguridad
- Wifi = Inalámbrica

En las tablas 4.6.2.2 se especifican todos los nombres de las VLAN creadas.

4.6.3.2. Modelo de Host

Para otorgar seguridad y evitar dar mucha información acerca de la ubicación del host, de la función que realiza o de la pertenencia, se propone para cada dispositivo PC se le asigne un nombre de acuerdo a un sufijo más un ID o secuencia correlativa, a continuación se detalla:

- **Prefijo: UCSM**
- **ID: 00000**

Donde los cinco ceros indican el correlativo, se tiene un crecimiento de hasta 99999 PCs.

Adicionalmente se recomienda que cada una de estos host forme parte del dominio correspondiente y se autentiquen mediante el mismo.

4.6.3.3. Modelo de dispositivos de red

Se propone para cada dispositivo Switch se le asigne un nombre de acuerdo a un sufijo más ID del Switch (Marca y modelo) y el último octeto de la dirección IP de administración del mismo, a continuación se detalla:

- **Prefijo: SW**
- **ID: X460 (ej. Extreme X460)**
- **IP: 10 (ej. 10.0.90.10/24)**

4.6.3.4. Modelo de servidores internos y DMZ

Se propone para cada dispositivo que brinde algún determinado servicio se le asigne un nombre de acuerdo a un sufijo más un ID del proceso principal que realice y una secuencia correlativa, a continuación se detalla:

- **Prefijo: SVR**
- **ID: DC (ej. controlador de dominio)**
- **Correlativo: 01**

Donde los dos ceros indican el correlativo, se tiene un crecimiento de hasta 99 servidores por servicio.

Adicionalmente se recomienda que cada una de estos servidores forme parte del dominio correspondiente y se autentiquen mediante el mismo.

4.6.4. Protocolos

4.6.4.1. Switching

- **Redundancia de enlaces**
  - IEEE 802.1ad

- **Etiquetado de tramas**
  - IEEE 802.1q

- **Prevención de loops en anillos**
  - IEEE 802.1w
  - IEEE 802.1d
  - ELRP
  - EAPS, EPSR

- **Seguridad**
  - Autenticación, Autorización y contabilización
    - IEEE 802.1x, complementado con Radius y Active Directory
    - Netlogin, complementado con 802.1x, Radius y Active Directory
    - Identity Management, complementado con netlogin, 802.1x, Radius y Active Directory
  - Implementación de ACL por VLAN

- **Calidad de servicio**
  - IEEE 802.1p
  - RFC 2475 – DiffServ Functions
  - RFC 2474 – DiffServ Precedence
  - RFC 2598 – DiffServ EF

- RFC 2597 – DiffServ AF

- **Energía**
  - POE – IEEE 802.3af
  - POE+ – IEEE 802.3at

4.6.4.2. Routing

En la implementación del direccionamiento se emplearon direcciones IPv4, solo con ruteo y funcionalidades IPv4 es suficiente.

- **Rutas directamente conectadas**

  La lista de las rutas directamente conectadas se muestra en la siguiente tabla:

Ori	Destino	Gateway	Métrica
d	10.0.2.0/24	10.0.2.1	1
d	10.0.7.0/24	10.0.7.1	1
d	10.0.20.0/28	10.0.20.1	1
d	10.0.22.0/24	10.0.22.1	1
d	10.0.90.0/24	10.0.90.1	1
d	10.0.91.0/24	10.0.91.1	1
d	10.0.92.0/24	10.0.92.1	1
d	10.0.93.0/24	10.0.93.1	1
d	10.0.94.0/24	10.0.94.1	1
d	10.0.100.0/28	10.0.100.1	1
d	10.0.101.0/24	10.0.101.1	1
d	10.0.102.0/25	10.0.102.1	1
d	10.0.110.0/28	10.0.110.1	1
d	10.0.111.0/24	10.0.111.1	1
d	10.0.113.0/25	10.0.113.1	1
d	10.0.114.0/27	10.0.114.1	1
d	10.0.115.0/27	10.0.115.1	1
d	10.0.120.0/28	10.0.120.1	1
d	10.0.121.0/24	10.0.121.1	1
d	10.0.122.0/26	10.0.122.1	1
d	10.0.123.0/27	10.0.123.1	1
d	10.0.130.0/24	10.0.130.1	1
d	10.0.131.0/27	10.0.131.1	1
d	10.0.132.0/27	10.0.132.1	1
d	10.0.133.0/27	10.0.133.1	1
d	10.0.140.0/27	10.0.140.1	1
d	10.0.141.0/27	10.0.141.1	1
d	10.0.142.0/28	10.0.142.1	1
d	10.0.143.0/28	10.0.143.1	1
d	10.0.144.0/28	10.0.144.1	1
d	10.0.145.0/28	10.0.145.1	1
d	10.0.151.0/24	10.0.151.1	1
d	10.0.153.0/24	10.0.153.1	1
d	10.0.154.0/24	10.0.154.1	1
d	10.0.156.0/24	10.0.156.1	1
d	10.0.157.0/24	10.0.157.1	1
d	10.0.158.0/24	10.0.158.1	1
d	10.0.159.0/24	10.0.159.1	1
d	10.0.160.0/24	10.0.160.1	1
d	10.0.161.0/24	10.0.161.1	1
d	10.0.163.0/25	10.0.163.1	1
d	10.0.164.0/24	10.0.164.1	1
d	10.0.165.0/27	10.0.165.1	1
d	10.0.166.0/28	10.0.166.1	1
d	10.0.171.0/25	10.0.171.1	1
d	10.0.172.0/26	10.0.172.1	1
d	10.0.173.0/27	10.0.173.1	1
d	10.0.174.0/27	10.0.174.1	1
d	10.0.175.0/27	10.0.175.1	1
d	10.0.181.0/24	10.0.181.1	1
d	10.0.182.0/24	10.0.182.1	1

Tabla 4.6-12: Detalle rutas directamente conectadas
Fuente: Elaboración Propia

- **Ruteo Estático**

  - Ruta default:
    - 0.0.0.0/0.0.0.0 → 10.0.10.2
    - Métrica → 1

- **Ruteo Dinámico**

  - OSPF, cuando se unan las distintas sedes de la UCSM a través de radio enlaces, fibra óptica, VPN etc. El identificador de cada área es el que sumarizara las rutas según el valor. Ver punto 4.6.2.1.

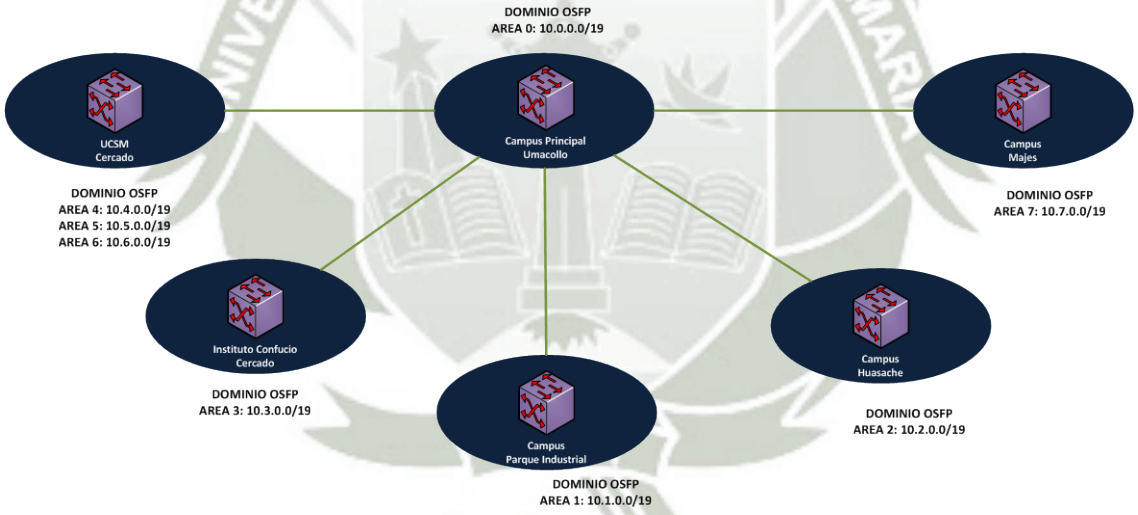

Figura 4.6-9: Enrutamiento entre sucursales
Fuente: Elaboración Propia

4.6.4.3. Administración

- Modelo de administración:
  - En banda: en todos los equipos administrables, se creara una VLAN para esta administración.
  - Fuera de banda: en equipos que tengan soporte para la administración fuera de banda se utilizara este acceso en caso de fallas en la administración en banda.
- SNMPv1,v2 en equipos heredados.
- SNMPv3 en infraestructura implementada.
- RMON de acuerdo a cada fabricante y del equipo si es que lo soporta, se debe tener en cuenta las MIB propietarias de cada marca y universales.
- CLI, en los equipos que soporten un CLI no basado en menús, se recomienda un CLI con soporte que brinde seguridad SSH2, en caso contrario utilizar telnet. En el peor de los casos utilizar la administración directa hacia el equipo utilizando un cable de consola serial, RJ45.
- Añadir mecanismos de seguridad a la administración mediante un servidor RADIUS o TACAS+ para la administración de cuentas para el acceso a los dispositivos de comunicación: switches, routers, access points.
- Integrar SNMPv1,v2, v3 al sistema de administración de red: Ridgeline v3.1

4.6.5. Seguridad

4.6.5.1. Políticas

La implementación de las políticas de seguridad se dará utilizando el mecanismo de firewall, a continuación se detalla:

- **Capa 2**
  - ACL: filtrado de paquetes a través de filtro de MAC Address por VLAN, puerto o dirección del flujo.
  - MAC Address: Se crearan políticas para que solo una dirección MAC se pueda conectar a un dispositivo, en caso de violación de la misma se creara una acción que apagara el puerto afectado y se dispara un evento en el sistema de logs.

- **Capa 3**
  - ACL: filtrado de paquetes determinado por dirección ip de origen destino, esto se puede realizar por VLAN, puerto del switch o dirección del flujo.

- **Capa 4**
  - ACL: filtrado de paquetes por medio a través del protocolo y el puerto TCP/UDP por VLAN, puerto del switch o dirección del flujo.

Estas políticas de seguridad pueden aplicarse en todos los equipos Extreme implementados:

- X440 Acceso
- X450 Acceso
- X460 Distribución
- X650 Granja de Servidores
- Black Diamond 8800 Core

Se recomienda la implementación de un servidor RADIUS y que a su vez este jale los usuarios y grupos del Controlador de Dominio Active Directory, para aplicar autenticación, autorización y contabilización.

- **Capa 7**
  - Syslog: por cada violación de alguna política de seguridad el equipo dispara un evento que se reflejara en el servidor syslog. Para esto es necesario la implementación del servicio en el servidor de administración de red.

4.6.6. Calidad de Servicio – QoS

Se deben tener en claro las 8 colas de calidad de servicio a implementar, para el caso de la UCSM se aplicara:

- DiffServ
- IEEE 802.1p
- IPTOS
- DSCP

La calidad de servicio se puede aplicar por puerto o vlan en todos los equipos Extreme implementados:

- X440 Acceso
- X450 Acceso
- X460 Distribución
- X650 Granja de Servidores
- Black Diamond 8800 Core

Las ocho colas de calidad de servicio se detallan en la siguiente tabla:

Nivel	Prioridad Tipo de tráfico	qos profile
0	Best effort	qp0
1	Tareas de fondo	qp1
2	Estándar	qp2
3	Carga excelente	qp3
4	Carga controlada	qp4
5	Video	qp5
6	Voz	qp6
7	Tráfico reservado para el control de red	qp7

Tabla 4.6-13: Perfiles de QoS
Fuente: Elaboración Propia

- Se aplicarán las colas de prioridad de la siguiente manera:

  - **QP0**: Trafico de la red Académica
  - **QP1**: Trafico de la red Administrativa y de administración de hardware
  - **QP2**: Tráfico de servicios publicados
  - **QP3**: Tráfico de servicios internos
  - **QP4**: Tráfico de base de datos
  - **QP5**: Tráfico de video
  - **QP6**: Tráfico de voz
  - **QP7**: Tráfico de protocolos de control de red

4.7. Diseño Físico Propuesto

4.7.1. Diseño

A continuación se detalla los aspectos más importantes:

- **Topología**: Estrella extendida.

- **Jerárquico**: se delimitan claramente las tres capas de red para la red de campus: Core, Distribución, Acceso. Además para la red Enterprise se delimitan las granjas de servidores interna y los servicios publicados en la DMZ.

- **Redundancia**: solo a nivel de Core con supervisoras redundantes y agregación de enlaces, a nivel de equipos "top of the rack" enlaces redundantes.

- **Seguridad**:
  - El MDF se encuentra protegido por puertas de acceso con llave adicionalmente la puerta principal del MDF tiene una llave que solo tienen los Administradores.
  - Todos los IDF se encuentran en lugares que poseen seguridad física en la primera puerta, como en los gabinetes.

- **Mantenimiento**: a los equipos se les proveerá mantenimiento físico como lógico. Físicamente cada 3 meses se realizara la limpieza de gabinetes así como de los "fans" de los dispositivos para evitar problemas ocasionados por el polvo. Lógicamente se instalara los firmware que provean actualizaciones críticas de software debido a brechas de seguridad o errores en algunos procesos.

4.7.2. Cableado de LAN

4.7.2.1. Tipo de cables

El cableado de la LAN propuesto se presenta a continuación:

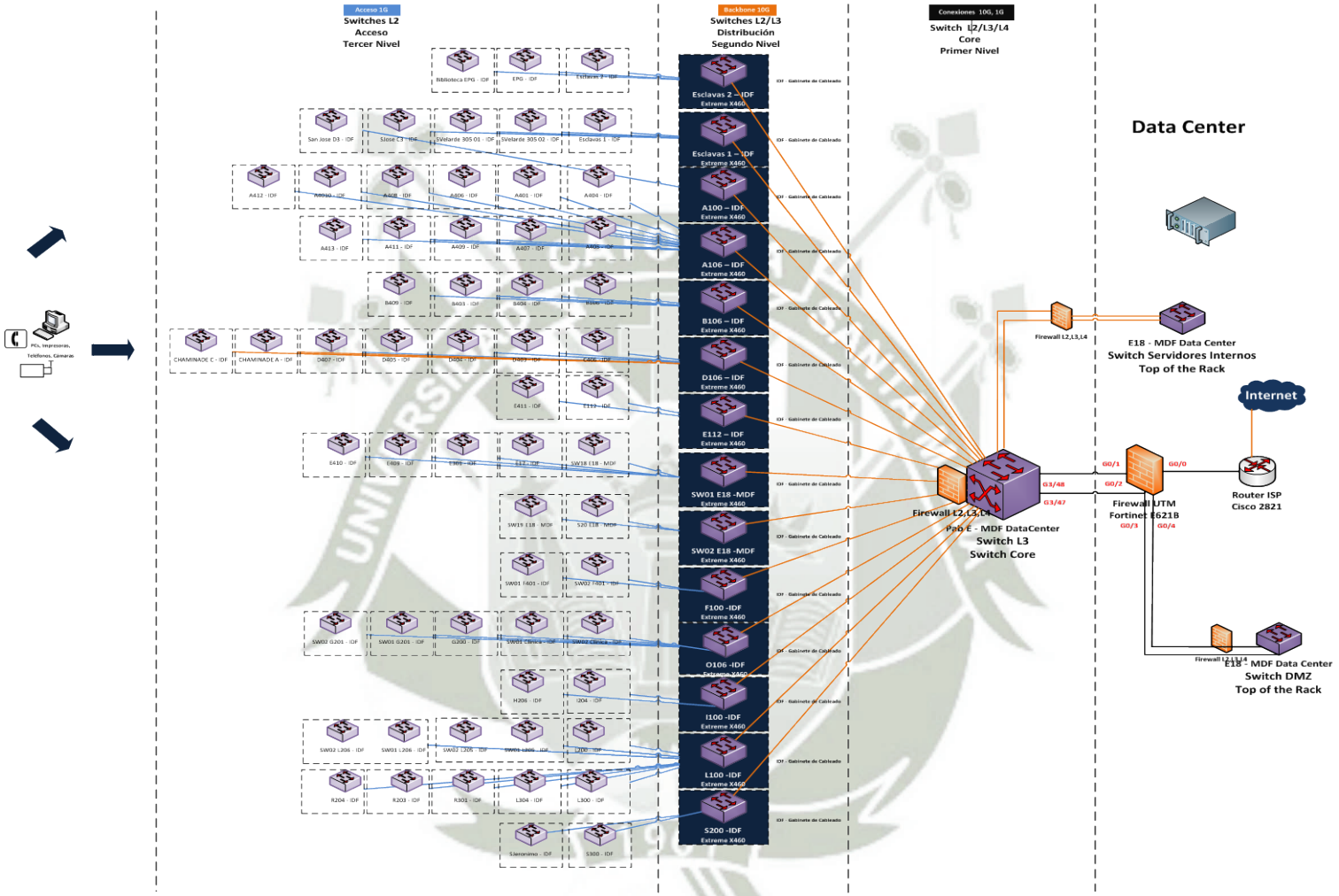

Figura 4.7-1: Diseño Físico Campus
Fuente: Elaboración Propia

- **Backbone**

  La fibra óptica negra tendida en el campus de la UCSM debe tener las siguientes características para cumplir con el requerimiento de 10G:

  - Fibra Óptica: Multimodo 50um OM3
  - Marca: Panduit u otras
  - Distancia Máxima: 300m

    Conector: ST a ST

En la siguiente Figura se detalla:

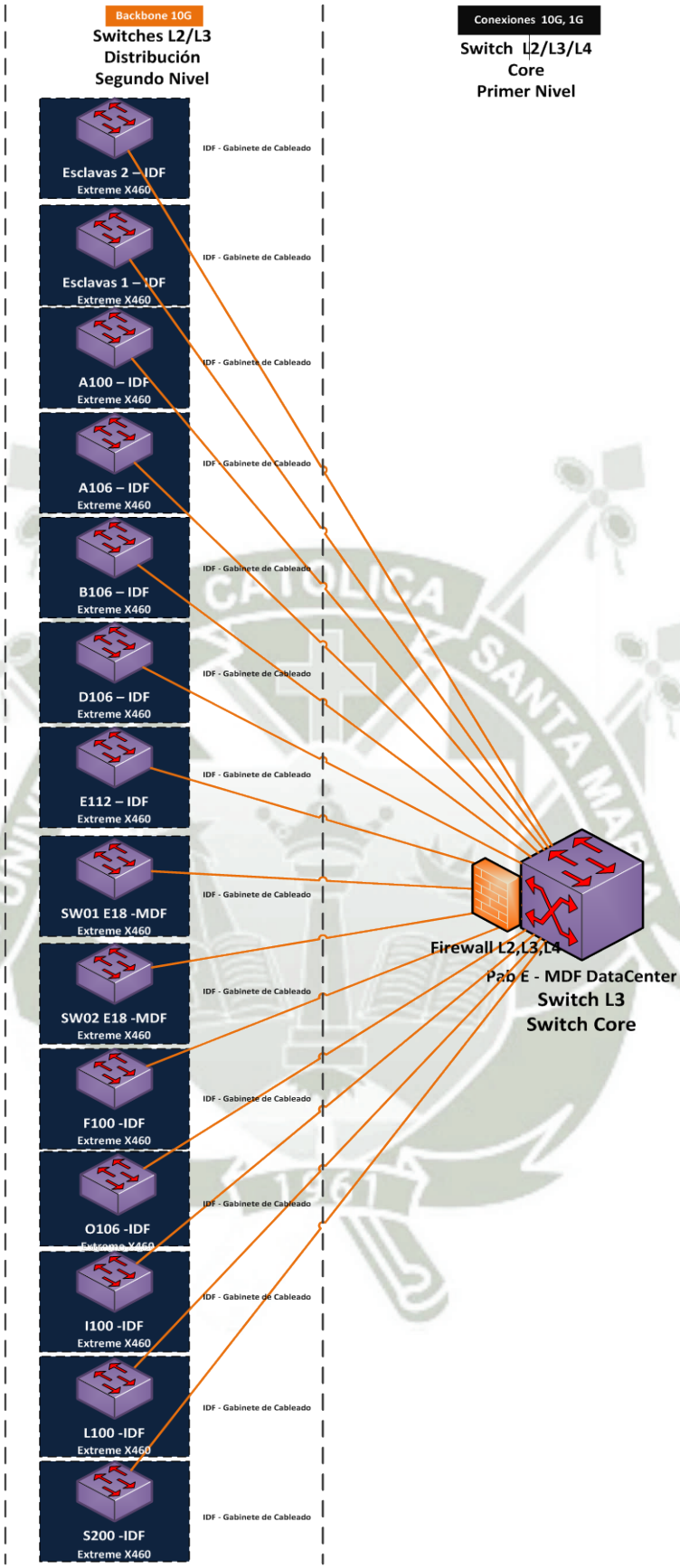

Figura 4.7-2: Diseño Físico Campus Backbone
Fuente: Elaboración Propia

- **Core**

  El equipo core conecta a los equipos de distribución, este se conectada al Patch panel de fibra de backbone mediante el siguiente medio:

  - Fibra Óptica: Patch Multimodo 50/125um
  - Marca: Panduit u otras
  - Distancia Máxima: 3m
  - Conector: LC a LC.

- **Granja de servidores**

  El equipo "top of the rack" que conecta a granja de servidores por un enlace agregado de 10G BaseSR, mediante el siguiente medio:

  - Fibra Óptica: Patch Multimodo 50/125um
    - Marca: Panduit u otras
    - Distancia Máxima: 10m
    - Conector: LC a LC

  - Cobre: Conexión hacia los servidores, al menos UTP Categoría 6, recomendable UTP Categoría 6a.
    - Marca: Belden u otras.
    - Distancia Máxima: 90m
    - Patch Cord: máximo 10 m
    - Conector: RJ45

  En la siguiente Figura se detalla el diseño de Core y Granja de servidores:

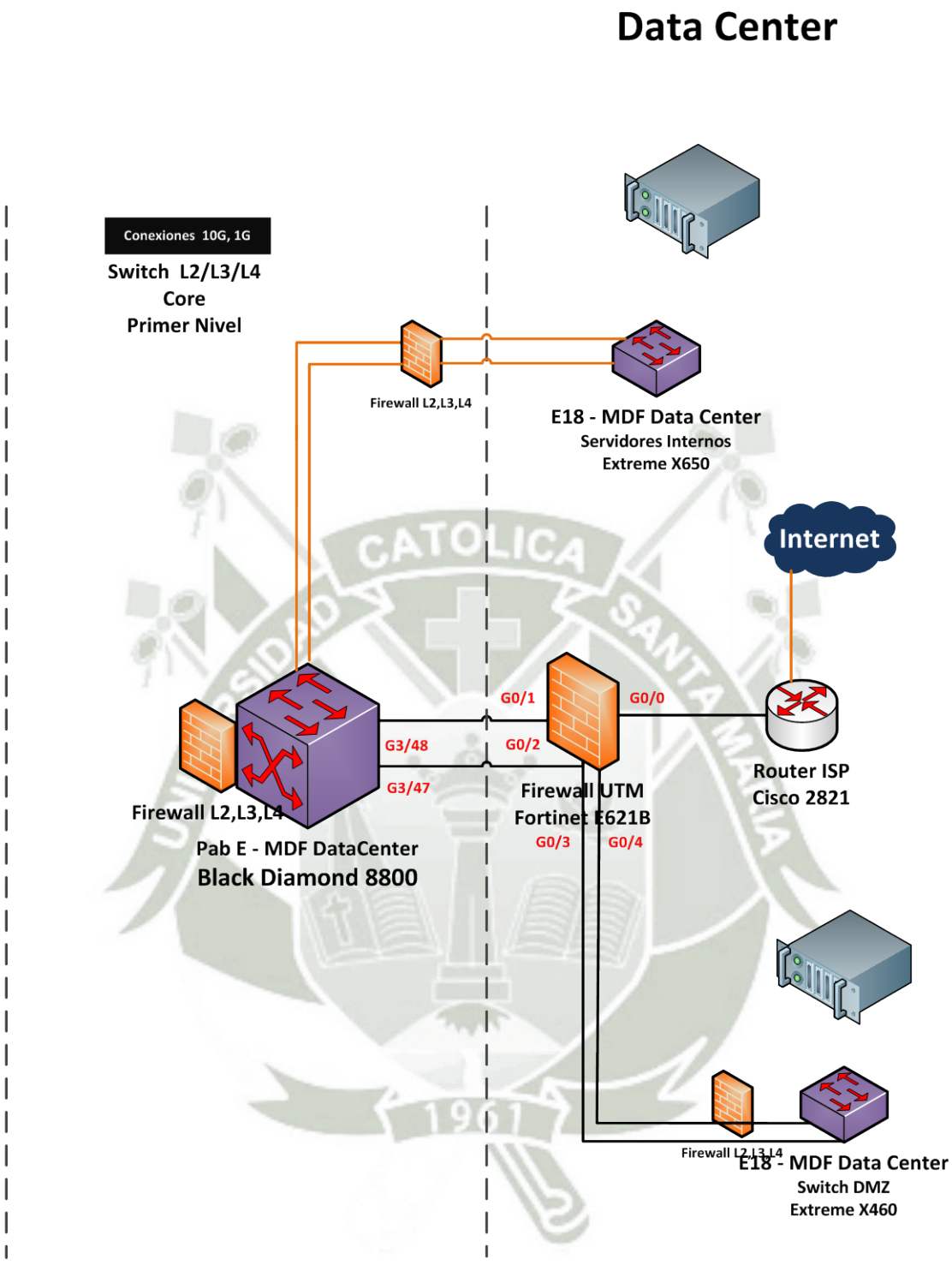

Figura 4.7-3: Diseño Físico Core
Fuente: Elaboración Propia

- **Distribución**

  Los equipos de distribución están conectados hacia el panel de fibra de cada gabinete de cableado, mediante el siguiente medio:

  - Fibra Óptica: Multimodo 50um OM3
  - Marca: Panduit u otras
  - Distancia Máxima: 300m
  - Conector: ST a ST
  - Patch de Fibra: maximo 2 m
  - Conector: LC a LC

  Los equipos switch o hubs de acceso que estén conectados hacia el Patch panel de cobre de cada gabinete de cableado, deben tener al menos las siguientes características:

  - Fibra Óptica: Multimodo 50um OM3
    - Marca: Panduit u otras
    - Distancia Máxima: 300m
    - Conector: ST a ST
    - Patch de Fibra: máximo 2 m
    - Conector: LC a LC

  - Cobre: Al menos UTP Categoría 5e, recomendable UTP Categoría 6 o 6a.
    - Marca: Belden u otras.
    - Distancia Máxima: 90m
    - Patch Cord: máximo 5m
    - Conector: RJ45

  De ser necesario que algunos equipos finales están directamente conectados al switch de distribución estos

deben estar conectados hacia el Patch panel de cobre de cada gabinete de cableado y en el otro extremo en la placa de pared terminal, mediante el siguiente medio:

- Cobre:
  - UTP Categoría 5e para PCs e impresoras cámaras de video,
  - UTP Categoría 6: para cámaras y telefonía IP.
- Marca: Belden u otras.
- Distancia Máxima: 90m

- **Acceso**

  Los equipos finales están directamente conectados hacia el Patch panel de cobre de cada gabinete de cableado y en el otro extremo en la placa de pared terminal, mediante el siguiente medio:

  - Cobre:
    - UTP Categoría 5e para PCs e impresoras
    - UTP Categoría 6: para cámaras IP y telefonía IP.
  - Marca: Belden u otras.
  - Distancia Máxima: 90m

  En la siguiente figura se detalla las capas de distribución acceso:

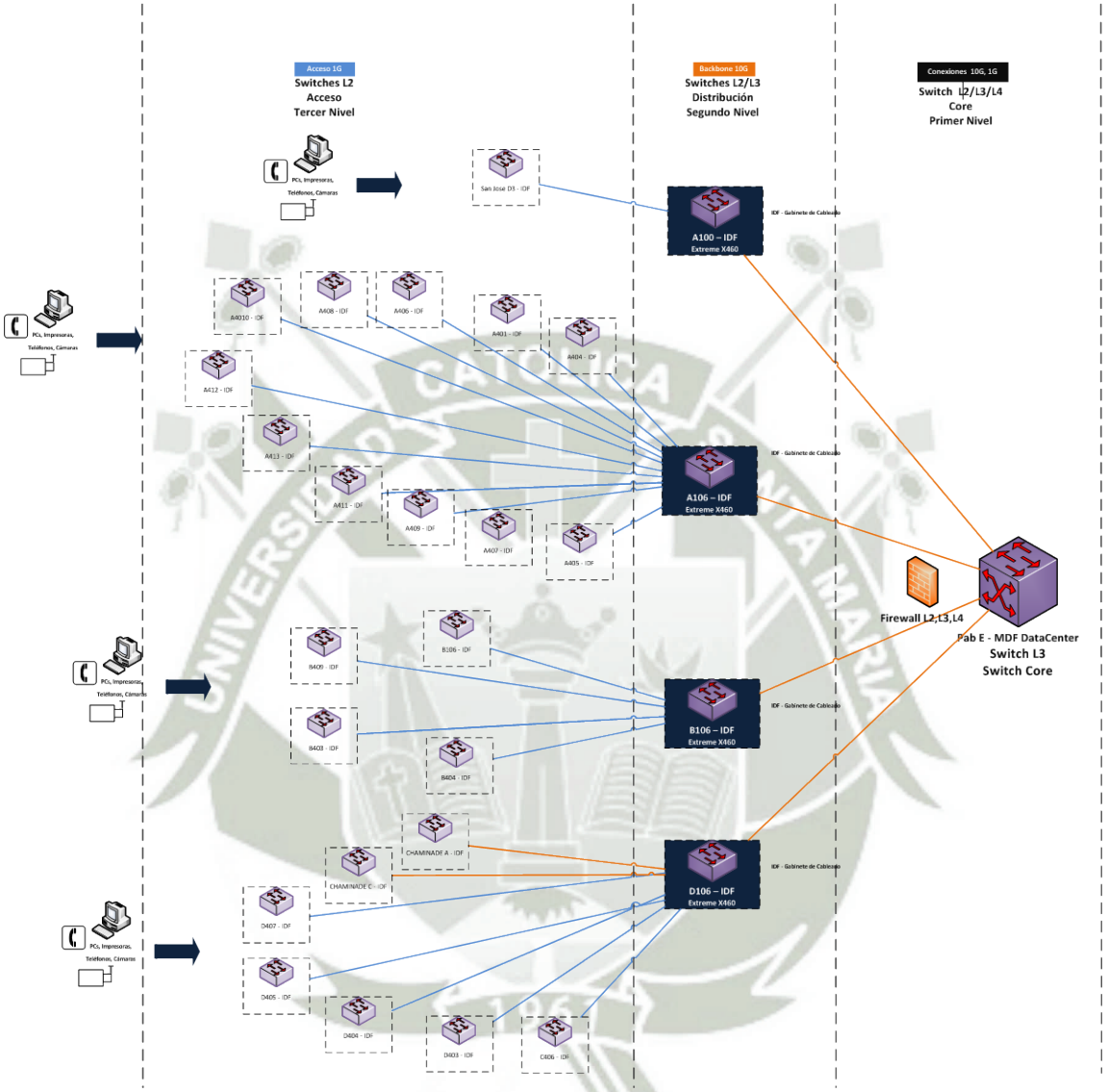

Figura 4.7-4: Diseño Físico Zona Campus 1
Fuente: Elaboración Propia

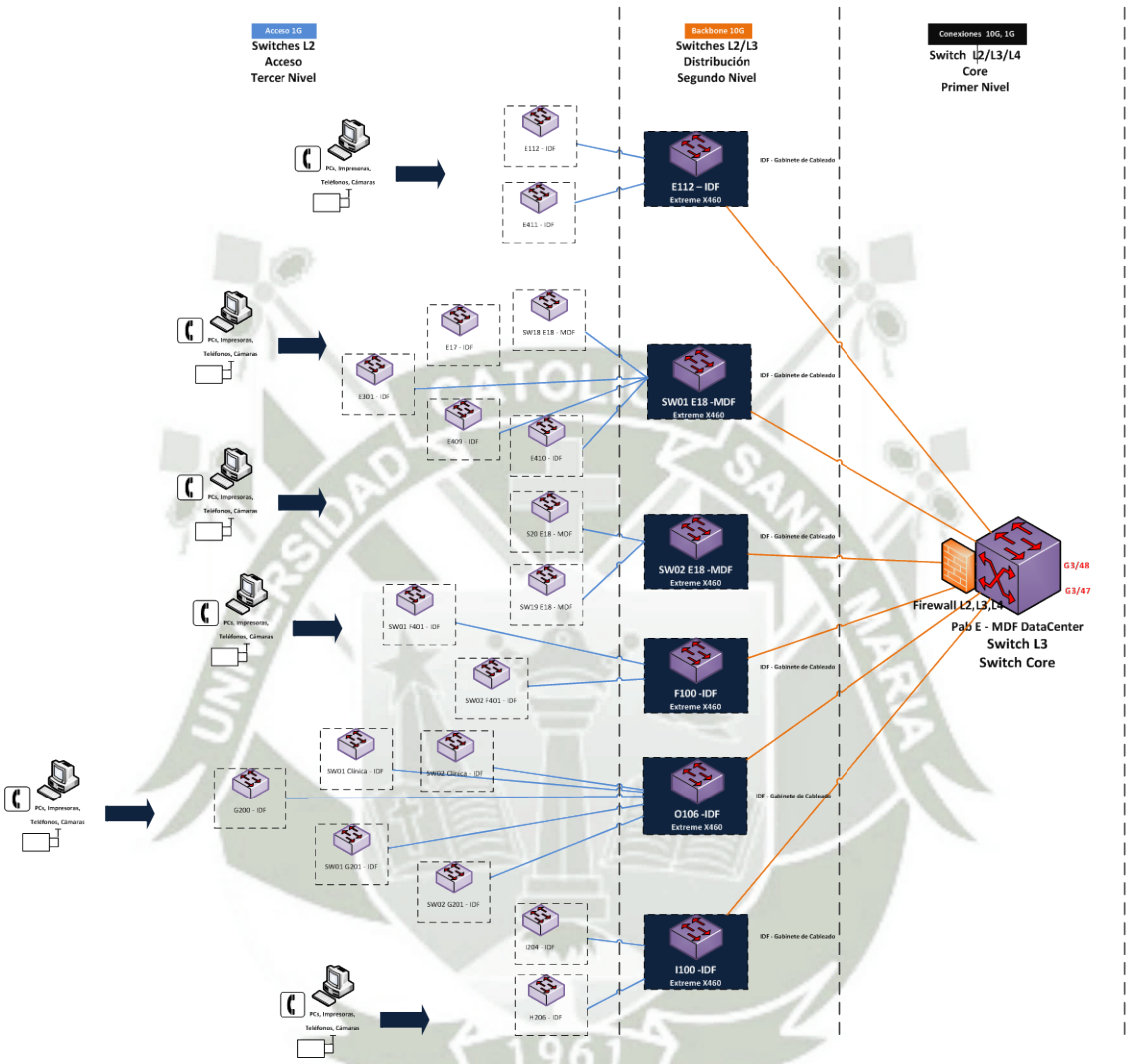

Figura 4.7-5: Diseño Físico Zona Campus 2
Fuente: Elaboración Propia

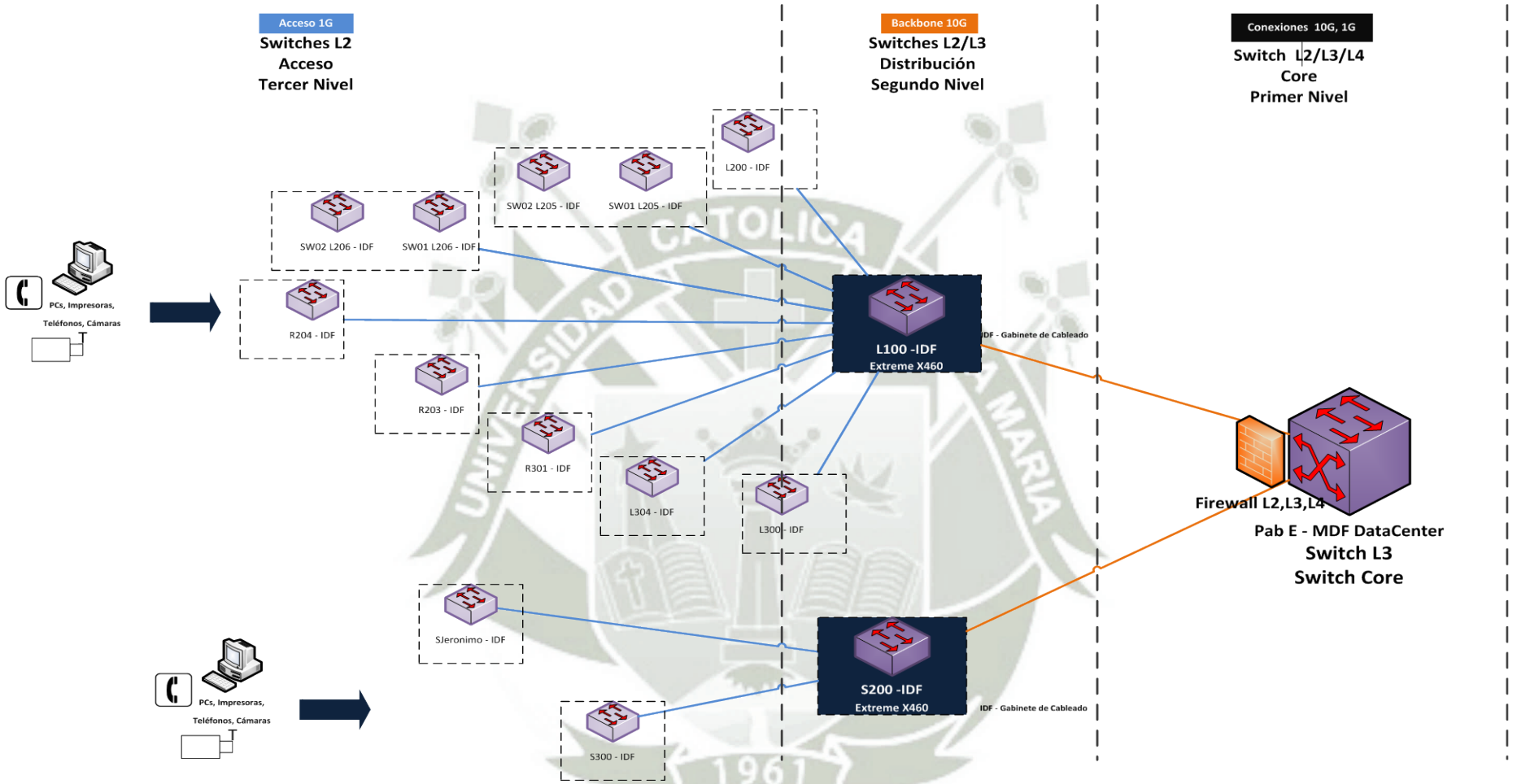

Figura 4.7-6: Diseño Físico Zona Campus 3
Fuente: Elaboración Propia

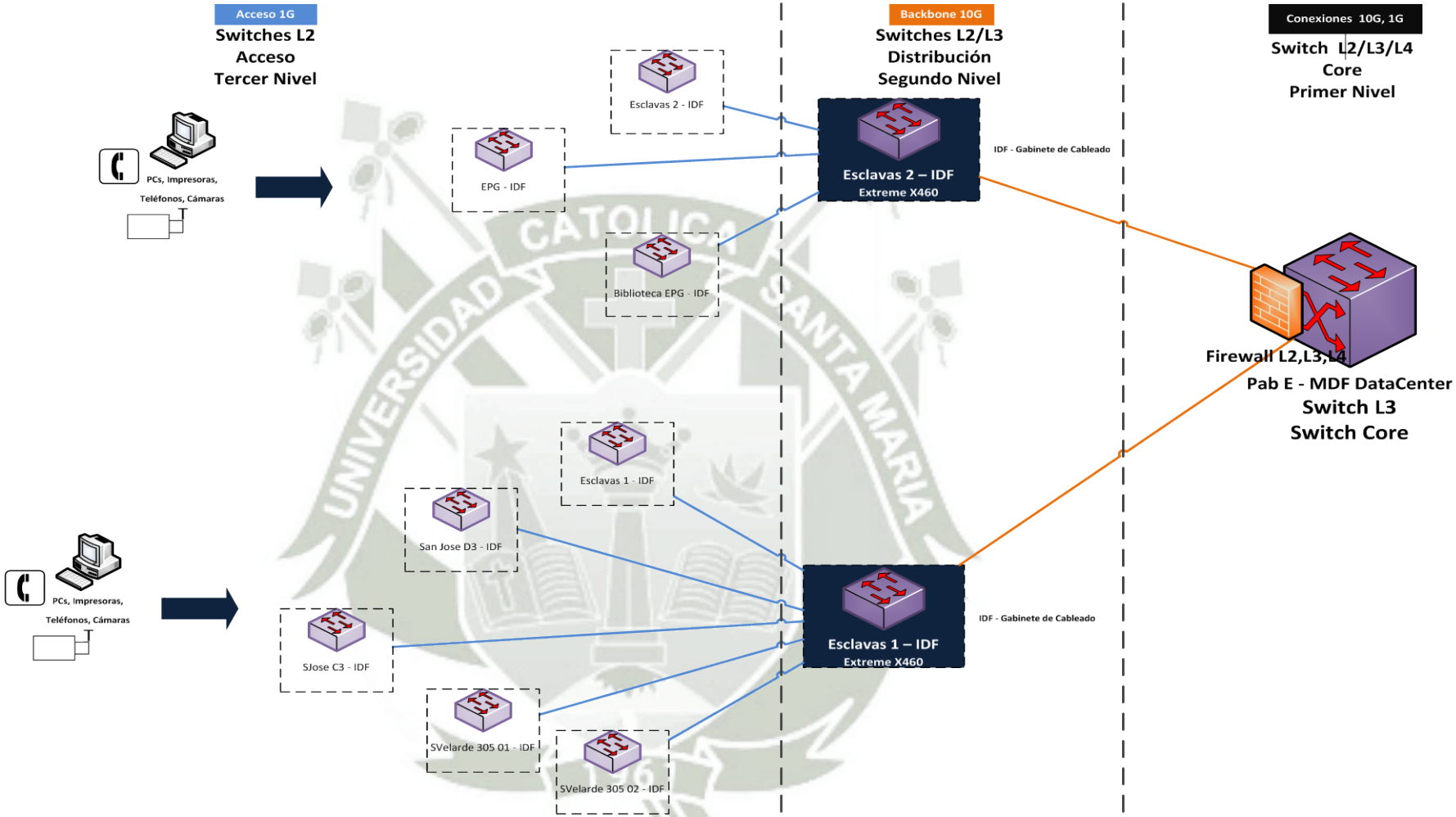

Figura 4.7-7: Diseño Físico Zona Campus Esclavas
Fuente: Elaboración Propia

4.7.3. Dispositivos

4.7.3.1. Tecnologías

4.7.3.1.1. LAN

Dentro de las tecnologías LAN se encuentran implementadas las siguientes:

- 10 Gigabit Ethernet BaseT
- 10 Gigabit Ethernet BaseSR
- Gigabit Ethernet BaseT
- Gigabit Ethernet BaseSX

4.7.3.1.2. WAN

Actualmente el enlace WAN es un circuito digital de 34 Mbps de ancho de banda, siendo el proveedor de Telefónica del Perú.

La conexión se realiza mediante el router Cisco 2821 y el CSU/DSU M1000 Huawey siendo el medio que por el cual llega la señal: fibra óptica.

4.7.3.2. Características

Los equipos instalados con sus principales características se detallan a continuación:

- **Equipo de Core: Extreme Black Diamond 8800**

  - Máxima capacidad del equipo: 3.8 Tbps
  - Máxima Velocidad por puerto según slot:
    - Slot 1 y 2: 8 puertos 10 Gbps full duplex BaseSR.
    - Slot 3: 48 puertos 1 Gbps full duplex BaseSX.
    - Slot 5: Supervisora MM128
    - Slot 6: Supervisora MM128
  - Escalabilidad:
    - Tecnológica: Soporta 40Gbps, solo cambiar tarjeta en slot.
    - Slot libres: 5, la cantidad de puertos máximos adicionales pueden ser:
      - 5 * 2 40Gbps = 10 puertos 40Gbps.
      - 5 * 8 10Gbps = 40 puertos 10Gbps.
      - 5 * 48 1Gbps = 240 puertos 1Gbps.
  - Tiempo de convergencia al conectar el dispositivo: 32 ms

- **Equipo de Granja de servidores:**

  - **Equipo 1: Extreme X650-24t**
    - Máxima capacidad del equipo: 224-448
    - Máxima Velocidad por puerto:
      - Equipada: 24 puertos 10 Gbps BaseT.
      - Tarjeta Opcional: 8 puertos 10 Gbps BaseSR.
    - Escalabilidad:
      - Tecnológica: Soporta 40Gbps, solo cambiar vim en slot posterior.

- Slot libres: 1, la cantidad de puertos máximos adicionales pueden ser:
  - 1 * 2 40Gbps = 2 puertos 40Gbps.
  - 1 * 8 10Gbps = 8 puertos 10Gbps.
- Apilamiento: Es posible.

- Tiempo de convergencia al conectar el dispositivo: 32 ms

- **Equipo de Distribución:**

  - **Equipo 1: Extreme X460-24P**
    - Máxima capacidad del equipo: 176-328 Gbps
    - Máxima Velocidad por puerto:
      - Equipada: 24 puertos 10/100/1000 Mbps BaseT.
      - Tarjeta Opcional: 2 puertos 10 Gbps full duplex BaseSR.
    - Funcionalidad POE: Si POE Clases 1, 2, 3, 4.
    - Apilamiento: Es posible.
    - Tiempo de convergencia al conectar el dispositivo: 600 ms

  - **Equipo 2: Extreme X460-48P**
    - Máxima capacidad del equipo: 176-328 Gbps
    - Máxima Velocidad por puerto:
      - Equipada: 48 puertos 10/100/1000 Mbps BaseT.
      - Tarjeta Opcional: 2 puertos 10 Gbps full duplex BaseSR.
    - Funcionalidad POE: Si POE Clases 1, 2, 3, 4.

- Apilamiento: Es posible.
- Tiempo de convergencia al conectar el dispositivo: 600 ms

- **Equipo de Acceso:**

Se recomienda la implementación de los siguientes equipos en la capa de acceso para la unificación de la red bajo un solo sistema operativo y la administración sea más transparente.

- **Equipo 1: Extreme X440-24 t/P**
  - Máxima capacidad del equipo: 64-136 Gbps
  - Máxima Velocidad por puerto:
    - Equipada: 24 puertos 10/100/1000 Mbps BaseT, cuatro de los cuales son combo pueden trabajar en BaseT o BaseSX.
  - Funcionalidad POE: En el modelo P.
  - Apilamiento: Es posible.
  - Tiempo de convergencia al conectar el dispositivo: 800 ms

- **Equipo 2: Extreme X440-48 t/P**
  - Máxima capacidad del equipo: 64-136 Gbps
  - Máxima Velocidad por puerto:
    - Equipada: 48 puertos 10/100/1000 Mbps BaseT, cuatro de los cuales son combo pueden trabajar en BaseT o BaseSX.
  - Funcionalidad POE: En el modelo P.
  - Apilamiento: Es posible.

- Tiempo de convergencia al conectar el dispositivo: 800 ms

En los equipos de acceso se tiene una amplia gama de equipos administrables y no administrables, el detalle de todos los equipos de acceso se explica en el punto 4.7.3.3

4.7.3.3. Resumen de equipos implementados

A continuación se detalla la lista de los equipos implementados:

Ítem	Ubicación	ID	Marca	Modelo	#Port	Adm.	Dirección	Nombre	Estado
Nivel Core									
	Core								
1	Switch Core	x	Extreme	BD8810	64	si	10.0.130.x/24	x	instalado
Nivel Distribución									
	Distribución								
1	A 100	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
2	A	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
3	B	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
4	D	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
5	E	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
6	F	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
7	I	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
8	L	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
9	O	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
10	S	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
11	Esclavas 1	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
12	Esclavas 2	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
13	Chaminade - A	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
14	Chaminade - C	x	Extreme	X460	24	si	10.0.130.x/24	x	instalado
Nivel Data Center									
	Distribución								
1	Servidores 10G	x	Extreme	X650	24	si	10.0.130.x/24	x	instalado
2	Switch 1	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
3	Switch 2	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
4	Switch 3	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
5	Switch DMZ	x	Extreme	X350	24	si	10.0.130.x/24	x	instalado
	Blade								
1	Blade sw 1	x	BNT	GbESM	20	si	10.0.130.x/24	x	instalado
2	Blade sw 2	x	BNT	GbESM	20	si	10.0.130.x/24	x	instalado
Nivel Acceso									
	Pabellón E								
1	E20 - SW01 Redes	x	HP	HPv1910	20	si	10.0.130.x/24	x	instalado
2	E21 - SW01 Impresiones	x	DLink	DL3526	24	si	10.0.130.x/24	x	instalado
3	E113 - SW02 Tesorería	x	Extreme	X450	48	si	10.0.130.x/24	x	instalado
4	E416 - SW01 Tutoría	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
5	E301 - SW01 CPU	x	Satra	S24P	24	no	-	x	instalado

6	E213 - SW01 Electrónica	x	Satra	S24P	24	no	-	x	instalado
7	E17 - SW01 Aulas	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
8	E17 - SW02 Aulas	x	-	-	48	-	-	-	ampliación
9	E406 - SW01 Idiomas 01	x	DLink	DL48P	48	si	10.0.130.x/24	x	instalado
10	E406 - SW02 Idiomas 02	x	DLink	DL48P	48	si	10.0.130.x/24	x	instalado
11	E406 - SW01 Idiomas 03	x	-	-	48	-	-	-	ampliación
12	E406 - SW01 Idiomas 04	x	-	-	48	-	-	-	ampliación
	Pabellón F								
13	F401 - SW01	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
14	F401 - SW02	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
15	F100 - Aulas	x	-	-	48	-	-	-	ampliación
	Pabellón I, H								
16	I 100	x	-	-	48	-	-	-	ampliación
17	H-I Aulas, Labs	x	-	-	48	-	-	-	ampliación
18	I Lab Psicología	x	Satra	S24P	24	-	-	x	instalado
19	H Lab Mercurio	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
	Pabellón G								
20	G200 - SW01 Estadística	x	Satra	S24P	24	no	-	x	instalado
21	G201 - SW01 Bib. Virtual	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
22	G201 - SW02 Bib. Virtual	x	Satra	S24P	24	no	-	x	instalado
	Pabellón O								
23	O - SW01 Clínica	x	Extreme	X440	24	si	10.0.130.x/24	x	instalado
24	O - SW02 Clínica	x	Extreme	X440	24	si	10.0.130.x/24	x	instalado
25	O405 - SW01 Aulas	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
26	O405 - SW02Aulas	x	-	-	48	-	-	-	ampliación
27	O - SW01 Lab	x	-	-	48	-	-	-	ampliación
	Pabellón S								
28	S - Tercer Piso	x	3Com	3C2426	26	si	10.0.130.x/24	x	instalado
29	S - Caseta San Jerónimo	x	Extreme	x440	24	si	10.0.130.x/24	x	instalado
	Pabellón L								
30	L200 - Coordinación	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
31	L204 - Lab 1,2	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
32	L204 - Lab 1,2	x	Satra	S24P	24	no	-	x	instalado
33	L205- Lab 3,4	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
34	L205- Lab 3,4	x	-	-	24	-	-	-	ampliación
35	L300 - Coordinación	x	Satra	S24P	24	no	-	x	instalado
36	L304 - Lab 1,2,3	x	Satra	S24P	24	no	-	x	instalado
37	L304 - Lab 1,2,3	x	-	-	48	-	-	-	ampliación
38	L304 - Lab 1,2,3	x	-	-	48	-	-	-	ampliación
	Pabellón R								
39	R101 - Lab	x	-	-	48	-	-	-	ampliación
40	R203 - CEDIM	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
41	R203 - CEDIM	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
42	R201 - Automatizacion	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
43	R201 - Automatizacion	x	-	-	48	-	-	-	ampliación
44	R303 - Industrial	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
45	R303 - Industrial	x	-	-	24	-	-	-	ampliación
	Biblioteca								
46	Biblioteca SW01	x	Extreme	X440	24	si	10.0.130.x/24	x	instalado
47	Biblioteca SW01	x	Extreme	X440	24	si	10.0.130.x/24	x	instalado
48	Biblioteca SW01	x	-	-	24	si	10.0.130.x/24	-	ampliación
	Pabellón A								
49	A - Piso 1	x	-	-	48	-	-	-	ampliación
50	A - Aulas 01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
51	A - Aulas 02	x	-	-	48	-	-	-	ampliación
52	A - Lab	x	-	-	24	-	-	-	ampliación

53	A - Lab A401	x	Satra	S24P	24	no	-	x	instalado
54	A - Lab A405	x	Extreme	X440	24	si	10.0.130.x/24	x	instalado
55	A - Lab A406	x	Satra	S24P	24	no	-	x	instalado
56	A - Lab A407	x	Satra	S24P	24	no	-	x	instalado
57	A - Lab A408	x	Satra	S24P	24	no	-	x	instalado
58	A - Lab A409	x	Satra	S24P	24	no	-	x	instalado
59	A - Lab A410	x	Satra	S24P	24	no	-	x	instalado
60	A - Lab A411	x	Satra	S24P	24	no	-	x	instalado
61	A - Lab A412	x	Satra	S24P	24	no	-	x	instalado
62	A - Lab A413	x	Satra	S24P	24	no	-	x	instalado
	Pabellón B								
63	B - Piso 1	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
64	B - Aulas 01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
65	B - Aulas 02	x	-	-	48	-	-	-	ampliación
66	B - Lab B407	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
67	B - Lab B409	x	DLink	DL48P	48	no	-	x	instalado
	Pabellón C								
68	C - Piso 1	x	-	-	48	-	-	-	ampliación
69	C - Aulas 01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
70	C - Aulas 02	x	-	-	48	-	-	-	ampliación
71	C - Lab	x	-	-	24	-	-	-	ampliación
	Pabellón D								
72	D - Piso 1	x	-	-	48	-	-	-	ampliación
73	D - Aulas 01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
74	D - Aulas 02	x	-	-	48	-	-	-	ampliación
75	D - Lab	x	-	-	24	-	-	-	ampliación
76	D - Lab 404	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
77	D - Lab 405	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
78	D - Lab 407	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
	Esclavas								
79	Esclavas 1 - SW01	x	Extreme	X460	48	si	10.0.130.x/24	x	instalado
80	Esclavas 1 - SW02 EPG	x	Alcatel	6248	48	si	10.0.130.x/24	x	instalado
81	Esclavas 1 - SW03	x	-	-	24	si	10.0.130.x/24	-	ampliación
82	Esclavas 2 - SW01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
83	Esclavas 2 - SW02 EPG Aulas	x	Extreme	X440P	24	si	10.0.130.x/24	x	instalado
84	Esclavas 3 - SW03	x	-	-	24	-	-	-	ampliación
	Samuel Velarde 303, 305								
85	SVelarde 305 - SW01	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
86	SVelarde 305 - SW02	x	Satra	S24P	24	si	10.0.130.x/24	x	instalado
87	SVelarde 305 - SW03	x	-	-	24	-	-	-	ampliación
	San Jose C3, D3								
88	San Jose C3 01	x	Alcatel	6248	48	si	10.0.130.x/24	x	ampliación
89	San Jose C3 02	x	-	-	24	-	-	-	ampliación
90	San Jose D3 01	x	3Com	3C2250	50	si	10.0.130.x/24	x	instalado
91	San Jose D3 02	x	-	-	24	-	-	-	ampliación
	Pabellón Chaminade								
92	Chaminade - SW01 Aulas	x	HP	HPv1910	48	si	10.0.130.x/24	x	instalado
93	Chaminade - SW01 Lab	x	-	-	24	-	-	-	ampliación

Tabla 4.7-1: Equipos Implementados
Fuente: Elaboración Propia

4.8. Resultados de las pruebas

4.8.1. Resumen de protocolos de pruebas

Los equipos involucrados en éste Protocolo de Pruebas son:

SWITCH DE CORE - BLACK DIAMONT 8800 10 SLOTS			
PN	**NOMBRE**	**DESCRIPCION**	**CANT.**
41011	BD 8810 10- Slot Chassis	BlackDiamond 8810 10-Slot Chassis	1
60020	700W/1200W 100-240V PSU	700W/1200W 100-240VAC Power Supply Unit	3
41231	BD 8900-MSM128	Management Switch Module	2
41311	BD 8800 Core License	BlackDiamond 8800 ExtremeWare XOS Core software upgrade	1
41631	BD 8900-10G8X-xl	8-port 10GBASE-X, XFP	1
10110	SR XENPAK Module	10 Gigabit Ethernet XENPAK, 850nm, MMF 300m, SC connector	2
41517	BD 8800 G48Tc	BlackDiamond 8800 48-port 10/100/1000BASE-T RJ-45, optional POE Card	1
10088	Pwr Cord,10A,NEMA L6-15P,C13,RA	Pwr Cord,10A,NEMA L6-15P,IEC320-C13,Right Angle	3

SWITCH DE DISTRIBUCIÓN - SUMMIT X460 48 PORT 10/100/1000 PoE, PoE+			
PRODUCT NUMBER	**PRODUCT NAME**	**PRODUCT DESCRIPTION**	**QTY**
16404	Summit X460-48p	48 10/100/1000BASE-T PoE, 4 100/1000BASE-X unpopulated SFP, XGM3 slot, Stacking module slot, AC PSU with one unpopulated PSU slot, Fan module, ExtremeXOS Edge License	2
16117	XGM3-2SF	Option card, two unpopulated 10 Gigabit SFP+ slots, compatible with Summit X460	2
10301	SR SFP+ Module	10 Gigabit Ethernet SFP+ module, 850nm, MMF 26-300m link, LC Connector	2

4.8.1.1. Introducción al protocolo de pruebas

Los laboratorios mencionados a continuación se trabajarán en un esquema acumulativo, o sea cuando se realice el LAB 3 por ejemplo, debe mantenerse las configuraciones de los LABs 1 y 2, por lo tanto para cuando se realice el último laboratorio se debe tener todo los LABs anteriores funcionando conjuntamente.

LAB 1

➔ **Descripción del LAB 1:**

Existen dos anillos lógicos “anillo 1” y “anillo 2”, en donde se deben configurar 10 vlans que pasan sólo por el “anillo 1" y otras 10 vlans distintas circulan sólo en el “anillo 2". A su vez existirán 2 vlans que pasarán por todos los switches o sea por los dos anillos. Estas dos vlans deben llamarse Voz y Data, otras vlans pueden tener cualquier nombre.

Se instalarán dos PCs, uno en el switch 1 y otro en el switch 3, lo mismo se hará con dos telefonos IP, tal como se muestra en el diagrama. Los PCs utilizarán la vlan Data y los teléfonos la vlan Voz. Se transmitirá entre los PCs un video y ping constantemente. Con los teléfonos se establecerá una llamada.

Esquema Planteado:

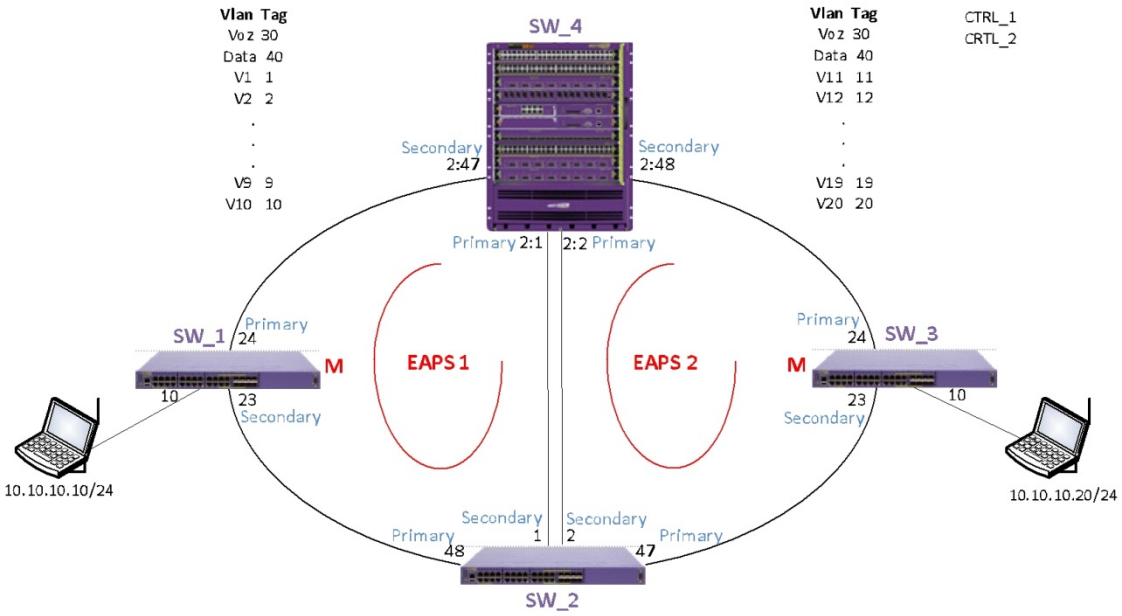

Figura 4.8-1: Esquema laboratorio de pruebas
Fuente: Elaboración Propia

➔ **Objetivo del LAB 1: Redundancia**

Se realizarán cortes de todos los enlaces, pero no más de uno a la vez, y no debe haber pérdidas de los servicios de voz y video o retardos superiores a 50 ms entre los distintos dispositivos.

➔ **Resultado del LAB 1: OK**

➔ **Configuraciones LAB 1:**

SW_1:

unconfigure switch all
configure snmp sysName SW_1
configure vlan "Default" delete ports all
configure vlan "Default" tag 1000
create vlan voz
create vlan data
create vlan v1
create vlan v2
create vlan v3

create vlan v4
create vlan v5
create vlan v6
create vlan v7
create vlan v8
create vlan v9
create vlan v10
create vlan CTRL_1
configure vlan voz tag 30
configure vlan data tag 40
configure vlan v1 tag 1
configure vlan v2 tag 2
configure vlan v3 tag 3
configure vlan v4 tag 4
configure vlan v5 tag 5
configure vlan v6 tag 6
configure vlan v7 tag 7
configure vlan v8 tag 8
configure vlan v9 tag 9
configure vlan v10 tag 10
configure vlan CTRL_1 tag 100
configure vlan CTRL_2 tag 200
configure vlan voz add ports 16
configure vlan data add ports 10
configure vlan voz add ports 23 tagged

configure vlan voz add ports 24 tagged
configure vlan data add ports 23 tagged
configure vlan data add ports 24 tagged
configure vlan v1 add ports 23,24 tagged
configure vlan v2 add ports 23,24 tagged
configure vlan v3 add ports 23,24 tagged
configure vlan v4 add ports 23,24 tagged
configure vlan v5 add ports 23,24 tagged
configure vlan v6 add ports 23,24 tagged
configure vlan v7 add ports 23,24 tagged
configure vlan v8 add ports 23,24 tagged
configure vlan v9 add ports 23,24 tagged
configure vlan v10 add ports 23,24 tagged
configure vlan CTRL_1 add ports 23,24 tagged
create eaps
configure eaps "EAPS_1" mode master
configure eaps "EAPS_1" add control "CTRL_1"
configure eaps "EAPS_1" primary port 24
configure eaps "EAPS_1" secondary port 23
configure eaps "EAPS_1" add protected vlan voz
configure eaps "EAPS_1" add protected vlan data
configure eaps "EAPS_1" add protected vlan v1
configure eaps "EAPS_1" add protected vlan v2
configure eaps "EAPS_1" add protected vlan v3
configure eaps "EAPS_1" add protected vlan v4
configure eaps "EAPS_1" add protected vlan v5
configure eaps "EAPS_1" add protected vlan v6
configure eaps "EAPS_1" add protected vlan v7
configure eaps "EAPS_1" add protected vlan v8

configure eaps "EAPS_1" add protected vlan v9
configure eaps "EAPS_1" add protected vlan v10
enable eaps
enable eaps EAPS_1

SW_2:

Configure snmp sysname SW_2
configure default delete ports all
Configure default tag 1000
Create vlan v1
Create vlan v2
Create vlan v3
Create vlan v4
Create vlan v5
Create vlan v6
Create vlan v7
Create vlan v8
Create vlan v9
Create vlan v10
Create vlan v11
Create vlan v12
Create vlan v13
Create vlan v14
Create vlan v15
Create vlan v16
Create vlan v17
Create vlan v18
Create vlan v19
Create vlan v20
Create vlan voz
Create vlan data
Configure vlan voz tag 30
Configure vlan data tag 40
Configure v1 tag 1
Configure v2 tag 2
Configure v3 tag 3
Configure v4 tag 4
Configure v5 tag 5
Configure v6 tag 6
Configure v7 tag 7
Configure v8 tag 8
Configure v9 tag 9
Configure v10 tag 10
Configure v11 tag 11
Configure v12 tag 12
Configure v13 tag 13
Configure v14 tag 14
Configure v15 tag 15
Configure v16 tag 16
Configure v17 tag 17
Configure v18 tag 18
Configure v19 tag 19
Configure v20 tag 20

#creando enlace de agregacion

Enable sharing 1 grouping 1,2 algorithm address-based L3_L4 lacp
Configure v1 add ports 1,48 tagged
Configure v2 add ports 1,48 tagged
Configure v3 add ports 1,48 tagged
Configure v4 add ports 1,48 tagged
Configure v5 add ports 1,48 tagged
Configure v6 add ports 1,48 tagged
Configure v7 add ports 1,48 tagged
Configure v8 add ports 1,48 tagged
Configure v9 add ports 1,48 tagged
Configure v10 add ports 1,48 tagged
Configure v11 add ports 1,47 tagged
Configure v12 add ports 1,47 tagged
Configure v13 add ports 1,47 tagged
Configure v14 add ports 1,47 tagged
Configure v15 add ports 1,47 tagged
Configure v16 add ports 1,47 tagged
Configure v17 add ports 1,47 tagged
Configure v18 add ports 1,47 tagged
Configure v19 add ports 1,47 tagged
Configure v20 add ports 1,47 tagged
Configure voz add ports 1,47,48 tagged
Configure data add ports 1,47,48 tagged

#configurando EAPS
Create vlan CTRL_1
Configure CTRL_1 tag 100
Configure CTRL_1 add ports 1,48 tagged
Create eaps EAPS_1
Configure EAPS_1 mode transit
y
Configure EAPS_1 add control CTRL_1
Configure EAPS_1 primary port 48
Configure EAPS_1 secondary port 1
Configure EAPS_1 add protected v1
Configure EAPS_1 add protected v2
Configure EAPS_1 add protected v3
Configure EAPS_1 add protected v4
Configure EAPS_1 add protected v5
Configure EAPS_1 add protected v6
Configure EAPS_1 add protected v7
Configure EAPS_1 add protected v8
Configure EAPS_1 add protected v9
Configure EAPS_1 add protected v10
Configure EAPS_1 add protected voz
Configure EAPS_1 add protected datos
Create vlan CTRL_2
Configure CTRL_2 tag 200
Configure CTRL_2 add ports 1,47 tagged
y
Create eaps EAPS_2
Configure EAPS_2 mode transit
y
Configure EAPS_2 add control CTRL_2
Configure EAPS_2 primary port 47
Configure EAPS_2 secondary port 1
Configure EAPS_2 add protected v11

Configure EAPS_2 add protected v12
Configure EAPS_2 add protected v13
Configure EAPS_2 add protected v14
Configure EAPS_2 add protected v15
Configure EAPS_2 add protected v16
Configure EAPS_2 add protected v17
Configure EAPS_2 add protected v18

Configure EAPS_2 add protected v19
Configure EAPS_2 add protected v20
Configure EAPS_2 add protected voz
Configure EAPS_2 add protected datos
Enable eaps
Enable EAPS_1
Enable EAPS_2
#Shared Port
create eaps shared-port 1
configure eaps shared-port 1 link-id 10
configure eaps shared-port 1 mode partner

SW_3

unconfigure switch all
configure snmp sysName SW_3
configure vlan "Default" delete ports all
configure vlan "Default" tag 1000
create vlan voz
create vlan data
create vlan v11
create vlan v12
create vlan v13
create vlan v14
create vlan v15
create vlan v16
create vlan v17
create vlan v18
create vlan v19
create vlan v20
create vlan CTRL_1
create vlan CTRL_2
configure vlan voz tag 30
configure vlan data tag 40
configure vlan v11 tag 11
configure vlan v12 tag 12
configure vlan v13 tag 13
configure vlan v14 tag 14
configure vlan v15 tag 15
configure vlan v16 tag 16
configure vlan v17 tag 17
configure vlan v18 tag 18
configure vlan v19 tag 19
configure vlan v20 tag 20
configure vlan CTRL_1 tag 100
configure vlan CTRL_2 tag 200
configure vlan voz add ports 16
configure vlan data add ports 10
configure vlan voz add ports 23 tagged
configure vlan voz add ports 24 tagged

configure vlan data add ports 23 tagged
configure vlan data add ports 24 tagged
configure vlan v11 add ports 23,24 tagged
configure vlan v12 add ports 23,24 tagged
configure vlan v13 add ports 23,24 tagged
configure vlan v14 add ports 23,24 tagged
configure vlan v15 add ports 23,24 tagged
configure vlan v16 add ports 23,24 tagged
configure vlan v17 add ports 23,24 tagged
configure vlan v18 add ports 23,24 tagged
configure vlan v19 add ports 23,24 tagged
configure vlan v20 add ports 23,24 tagged
configure vlan CTRL_2 add ports 23,24 tagged
create eaps EAPS_2
configure eaps "EAPS_2" mode master
configure eaps "EAPS_2" add control "CTRL_2"
configure eaps "EAPS_2" primary port 24
configure eaps "EAPS_2" secondary port 23
configure eaps "EAPS_2" add protected vlan voz
configure eaps "EAPS_2" add protected vlan data
configure eaps "EAPS_2" add protected vlan v11
configure eaps "EAPS_2" add protected vlan v12
configure eaps "EAPS_2" add protected vlan v13
configure eaps "EAPS_2" add protected vlan v14
configure eaps "EAPS_2" add protected vlan v15
configure eaps "EAPS_2" add protected vlan v16
configure eaps "EAPS_2" add protected vlan v17
configure eaps "EAPS_2" add protected vlan v18
configure eaps "EAPS_2" add protected vlan v19
configure eaps "EAPS_2" add protected vlan v20
enable eaps
enable eaps_2

SW_4:

Configure snmp sysname SW_4
configure default delete ports all
Configure default tag 1000
Create vlan v1
Create vlan v2
Create vlan v3
Create vlan v4
Create vlan v5
Create vlan v6
Create vlan v7
Create vlan v8
Create vlan v9
Create vlan v10
Create vlan v11
Create vlan v12
Create vlan v13
Create vlan v14
Create vlan v15
Create vlan v16
Create vlan v17
Create vlan v18
Create vlan v19
Create vlan v20

Create vlan voz
Create vlan data
Configure vlan voz tag 30
Configure vlan data tag 40
Configure v1 tag 1
Configure v2 tag 2
Configure v3 tag 3
Configure v4 tag 4
Configure v5 tag 5
Configure v6 tag 6
Configure v7 tag 7
Configure v8 tag 8
Configure v9 tag 9
Configure v10 tag 10
Configure v11 tag 11
Configure v12 tag 12
Configure v13 tag 13
Configure v14 tag 14
Configure v15 tag 15
Configure v16 tag 16
Configure v17 tag 17
Configure v18 tag 18
Configure v19 tag 19
Configure v20 tag 20

#creando enlace de agregacion
Enable sharing 1 grouping 2:1,2:2 algorithm address-based L3_L4 lacp
Configure v1 add ports 2:1,2:47 tagged
Configure v2 add ports 2:1,2:47 tagged
Configure v3 add ports 2:1,2:47 tagged
Configure v4 add ports 2:1,2:47 tagged
Configure v5 add ports 2:1,2:47 tagged
Configure v6 add ports 2:1,2:47 tagged
Configure v7 add ports 2:1,2:47 tagged
Configure v8 add ports 2:1,2:47 tagged
Configure v9 add ports 2:1,2:47 tagged

Configure v10 add ports 2:1,2:47 tagged
Configure v11 add ports 2:1,2:48 tagged
Configure v12 add ports 2:1,2:48 tagged
Configure v13 add ports 2:1,2:48 tagged
Configure v14 add ports 2:1,2:48 tagged
Configure v15 add ports 2:1,2:48 tagged
Configure v16 add ports 2:1,2:48 tagged
Configure v17 add ports 2:1,2:48 tagged
Configure v18 add ports 2:1,2:48 tagged
Configure v19 add ports 2:1,2:48 tagged
Configure v20 add ports 2:1,2:48 tagged
Configure voz add ports 2:1,2:47,2:48 tagged
Configure data add ports 2:1,2:47,2:48 tagged

#configurando EAPS
Create vlan CTRL_1
Configure CTRL_1 tag 100
Configure CTRL_1 add ports 2:1,2:47 tagged
Create eaps EAPS_1
Configure EAPS_1 mode transit

y
Configure EAPS_1 add control CTRL_1
Configure EAPS_1 primary port 2:1
Configure EAPS_1 secondary port 2:47
Configure EAPS_1 add protected v1
Configure EAPS_1 add protected v2
Configure EAPS_1 add protected v3
Configure EAPS_1 add protected v4
Configure EAPS_1 add protected v5
Configure EAPS_1 add protected v6
Configure EAPS_1 add protected v7
Configure EAPS_1 add protected v8
Configure EAPS_1 add protected v9
Configure EAPS_1 add protected v10
Configure EAPS_1 add protected voz
Configure EAPS_1 add protected data
Create vlan CTRL_2
Configure CTRL_2 tag 200
Configure CTRL_2 add ports 2:1,2:48 tagged
y
Create eaps EAPS_2
Configure EAPS_2 mode transit
y
Configure EAPS_2 add control CTRL_2
Configure EAPS_2 primary port 2:1
Configure EAPS_2 secondary port 2:48
Configure EAPS_2 add protected v11
Configure EAPS_2 add protected v12
Configure EAPS_2 add protected v13
Configure EAPS_2 add protected v14
Configure EAPS_2 add protected v15
Configure EAPS_2 add protected v16
Configure EAPS_2 add protected v17
Configure EAPS_2 add protected v18
Configure EAPS_2 add protected v19
Configure EAPS_2 add protected v20
Configure EAPS_2 add protected voz
Configure EAPS_2 add protected data
Enable eaps
Enable EAPS_1
Enable EAPS_2

#Shared Port (Solución de Problema de EAPs en un enlace compartido)
create eaps shared-port 2:1
configure eaps shared-port 2:1 link-id 10
configure eaps shared-port 2:1 mode controller
configure eaps shared-port 2:1 segment-timeout expiry-action

Lab 2

➔ **Descripción del LAB 2:**

Manteniendo la configuración del LAB 1, se deberá realizar una configuración tal que en los switches 1 y 3 al conectar un PC y un

teléfono, el switch debe automáticamente asignar la vlan al puerto, asignar calidad de servicio al puerto (sólo en el caso que sea el teléfono) y enviar logs describiendo el proceso. Las vlans de datos y Voz deben tener sólo asignados los puertos de enlaces.

➔ **Objetivo: Flexibilidad y Disponibilidad**

Se conectará un teléfono genérico que utiliza el protocolo LLDP en algunos de los puertos del switch. Se espera que al conectar los dispositivos el switch (en este caso al telefono) en los puertos de 6 a 9 los reconozca y cargue la configuración al dispositivo y cuando se desconecten la configuración realizada debe desconfigurarse automáticamente por parte del switch.

Este protocolo es estándar por lo tanto basta con que se tenga un equipo con soporte de LLDP y el switch reconocerá el tipo de dispositivo que se está conectando.

➔ **Resultado: OK**

➔ **Configuraciones**

Para este fin se le cargo 2 scripts al switch Extreme como se muestra a continuación via comando:

```
SW_3.17 # ls
                                                    Jul
-rw-r--r--  1 root    0      3806 19     01:26 Detectado_Telefono.xsf
                                                    Jul     01:36
-rw-r--r--  1 root    0      3702 19     No_Detectado_Telefono.xsf
-rw-rw-     1
rw-         root      0    136762 Jul 19 01:37 primary.cfg
```

SW_3

```
enable lldp ports all
create upm profile Telefono_Detectado
load script Detectado_Telefono.xsf
create upm profile Telefono_No_Detectado
load script No_Detectado_Telefono.xsf
configure upm event device-detect profile Telefono_Detectado ports 6-9
```

configure upm event device-undetect profile Telefono_No_Detectado ports 6-9

Lab 3

➔ **Descripción del LAB 3:**

Manteniendo la configuración del LAB 1 y LAB 2, se deberá realizar una configuración para comprobar la existencia de 8 colas de calidad de servicio, por lo cual a la vlan de datos se le asignará alguno de los 8 perfiles de QoS (uno a la vez), mientras por la vlan de voz se satura el ancho de banda. Los enlaces deben ser configurados a 10 Mbps a excepción del link agregación. Para esta párte del laboratorio se debe configurar lo siguiente en todos los switchs:

➔ **Objetivo: Calidad de Servicio en las ocho colas**

Los 8 perfiles de QoS asignados a la vlan de datos deben permitir que el video transmitido no sufra pérdida de la Figura o retardo que imposibiliten ver el video normalmente.

Se puede observar las 8 colas via comando:

```
SW_3.75 # show qosprofile
    QP1   Weight =  1    Max Buffer Percent = 100
    QP2   Weight =  1    Max Buffer Percent = 100
    QP3   Weight =  1    Max Buffer Percent = 100
    QP4   Weight =  1    Max Buffer Percent = 100
    QP5   Weight =  1    Max Buffer Percent = 100
    QP6   Weight =  1    Max Buffer Percent = 100
    QP7   Weight =  1    Max Buffer Percent = 100
    QP8   Weight =  1    Max Buffer Percent = 100
SW_3.76 #
```

Se satura un enlace mediante un software y se comprueba que la calidad de la voz, el video y la comunicación ICMP no se pierda dependiendo del QoS que se le asigne

➔ **Resultado: OK**

➔ **Configuraciones**

create qosprofile qp2
configure dot1p type 1 qosprofile qp2
configure diffserv examination code-point 8 qosprofile qp2
configure diffserv examination code-point 9 qosprofile qp2
configure diffserv examination code-point 10 qosprofile qp2
configure diffserv examination code-point 11 qosprofile qp2
configure diffserv examination code-point 12 qosprofile qp2
configure diffserv examination code-point 13 qosprofile qp2
configure diffserv examination code-point 14 qosprofile qp2
configure diffserv examination code-point 15 qosprofile qp2
create qosprofile qp3
configure dot1p type 2 qosprofile qp3
configure diffserv examination code-point 16 qosprofile qp3
configure diffserv examination code-point 17 qosprofile qp3
configure diffserv examination code-point 18 qosprofile qp3
configure diffserv examination code-point 19 qosprofile qp3
configure diffserv examination code-point 20 qosprofile qp3
configure diffserv examination code-point 21 qosprofile qp3
configure diffserv examination code-point 22 qosprofile qp3
configure diffserv examination code-point 23 qosprofile qp3
create qosprofile qp4
configure dot1p type 3 qosprofile qp4
configure diffserv examination code-point 24 qosprofile qp4
configure diffserv examination code-point 25 qosprofile qp4
configure diffserv examination code-point 26 qosprofile qp4
configure diffserv examination code-point 27 qosprofile qp4
configure diffserv examination code-point 28 qosprofile qp4
configure diffserv examination code-point 29 qosprofile qp4
configure diffserv examination code-point 30 qosprofile qp4
configure diffserv examination code-point 31 qosprofile qp4
create qosprofile qp5
configure dot1p type 4 qosprofile qp5
configure diffserv examination code-point 32 qosprofile qp5
configure diffserv examination code-point 33 qosprofile qp5
configure diffserv examination code-point 34 qosprofile qp5
configure diffserv examination code-point 35 qosprofile qp5
configure diffserv examination code-point 36 qosprofile qp5
configure diffserv examination code-point 37 qosprofile qp5
configure diffserv examination code-point 38 qosprofile qp5
configure diffserv examination code-point 39 qosprofile qp5
create qosprofile qp6
configure dot1p type 5 qosprofile qp6
configure diffserv examination code-point 40 qosprofile qp6
configure diffserv examination code-point 41 qosprofile qp6
configure diffserv examination code-point 42 qosprofile qp6
configure diffserv examination code-point 43 qosprofile qp6
configure diffserv examination code-point 44 qosprofile qp6
configure diffserv examination code-point 45 qosprofile qp6
configure diffserv examination code-point 46 qosprofile qp6
configure diffserv examination code-point 47 qosprofile qp6
create qosprofile qp7

configure dot1p type 6 qosprofile qp7
configure diffserv examination code-point 48 qosprofile qp7
configure diffserv examination code-point 49 qosprofile qp7
configure diffserv examination code-point 50 qosprofile qp7
configure diffserv examination code-point 51 qosprofile qp7
configure diffserv examination code-point 52 qosprofile qp7
configure diffserv examination code-point 53 qosprofile qp7
configure diffserv examination code-point 54 qosprofile qp7
configure diffserv examination code-point 55 qosprofile qp7
enable dot1p replacement ports all
enable diffserv examination ports all
enable diffserv replacement ports all

 # aplicando la calidad de servicio a la vlan VOZ qp6
Configure vlan voz qosprofile qp5

Lab 4

➔ **Descripción del LAB 4:**

Manteniendo la configuración del LAB 1, LAB 2 y LAB 3, se deberá realizar una configuración para capturar el tráfico de entrada y salida del puerto donde está el PC 2 o del Teléfono IP 2 y enviar esta captura de tráfico al switch 1 donde está el PC 1 con un programa de sniffer para visualizar lo capturado. La información de mirroring debe enviar el trafico del puerto X, ser enviado al puerto de monitoreo. Colocando un sniffer en un computador se realiza la captura del tráfico que circula por un puerto o una vlan, esta característica se puede activar para que la captura se realice en forma remota.

➔ **Objetivo: Troubleshooting**

Debe ser posible capturar el tráfico en el PC 1 ubicado en el switch 1 y no debe haber cortes del tráfico recibido cuando se realicen desconexiones de los cables de enlace del switch 1 y 3 , en la prueba se desconectará un cable a la vez.

➔ **Resultado: OK**

➔ **Configuraciones:**

SW_1
create vlan sniffer
configure vlan sniffer tag 30 remote-mirroring #remote mirroring#
configure vlan sniffer add ports 23,24 tagged
SW_2
create vlan sniffer
configure vlan sniffer tag 30 remote-mirroring #remote mirroring#
configure vlan sniffer add ports 48,1,47 tagged
SW_3
create vlan sniffer
configure vlan sniffer tag 30 remote-mirroring #remote mirroring#
configure vlan sniffer add ports 23,24 tagged
configure mirroring mode enhanced
enable mirroring to port-list 1,24 loopback-port 21 remote-tag 30
configure mirroring add port 12
configure mirroring add port 13
configure mirroring add port 14
configure mirroring add port 15
configure "LAB_2" add protected "internalMirrorLoopback"
SW_4
create vlan sniffer
configure vlan sniffer tag 30 remote-mirroring #remote mirroring#
configure vlan sniffer add ports 2:47,2:48,2:1 tagged

Lab 5

➔ **Descripción del LAB 5:**

Manteniendo la configuración del LAB 1, LAB 2, LAB 3 y LAB 4, se deberá comprobar que el sistema operativo utilizado en los switches de core y borde es modular y permite el reinicio de procesos. Se debe reiniciar los siguientes procesos: Spanning-tree (SPT) o EAPS según sea el protocolo utilizado en capa 2 para evitar el loop, OSPF y telnet. Para éste laboratorio se debe adicionar una comunicación de OSPF del tipo punto a punto entre todos los equipos a excepción del enlace utilizado como link aggregation. Se crearán dos vlans que serán conocidas mediante el protocolo OSPF, por lo tanto una existirá sólo en el switch 1 y otra en el switch 3. Se comprobará mediante traceroute que efectivamente la comunicación entre las dos vlans es posible sólo mediante el enrutamiento de OSPF. El PC 1

pertenecerá a una de las vlans y el PC 2 a la otra, entre ellos se transmitirá una comunicación de video y un ping. Se establecerá una llamada a traves de la vlan de capa 2 llamada “Voz”.

➔ **Objetivo: Redundancia y disponibilidad**

Se realizará el reinicio de procesos como OSPF, EAPS o SPT y telnet, no debe existir pérdida de los servicios de Voz y Video. Para este fin se debe reiniciar los procesos, veamos que procesos se puede reiniciar:

```
SW_3.76 # restart process ?
  class         Process of the same class
  <name>        Process name
    "bgp"       "dot1ag"      "eaps"        "ethoam"
    "exsshd"    "isis"        "lldp"        "netLogin"
    "ospf"      "snmpMaster"  "snmpSubagent"  "telnetd"
    "tftpd"     "thttpd"      "vrrp"        "xmld"

SW_3.76 # restart process
SW_3.76 # restart process ospf  // reinicia el proceso ospf
```

➔ **Resultado: OK**

➔ **Configuraciones:**

 # OSPF #
SW_1
create vlan routing_1
create vlan routing_2
create vlan router_id
configure routing_1 ipaddress 192.168.1.2/30
configure routing_2 ipaddress 192.168.2.2/30
configure router_id ipaddress 1.1.1.1/32
configure routing_1 add port 1
configure routing_2 add port 24
enable loopback-mode vlan router_id
enable ipforwarding
configure ospf add routing_1 area 0.0.0.0 link-type point-to-point
configure ospf add routing_2 area 0.0.0.0 link-type point-to-point
configure ospf add router_id area 0.0.0.0 link-type point-to-point passive

configure ospf routerid 1.1.1.1
enable ospf
configure ospf restart both
configure ospf vlan all restart-helper both

SW_2
create vlan routing_1
create vlan routing_2
create vlan router_id
configure routing_1 ipaddress 192.168.2.5/30
configure routing_2 ipaddress 192.168.2.1/30
configure router_id ipaddress 2.2.2.2/32
configure routing_1 add port 24
configure routing_2 add port 25
enable loopback-mode vlan router_id
enable ipforwarding routing_1
enable ipforwarding routing_2
enable ipforwarding router_id
configure ospf add routing_1 area 0.0.0.0 link-type point-to-point
configure ospf add routing_2 area 0.0.0.0 link-type point-to-point
configure ospf add router_id area 0.0.0.0 link-type point-to-point passive
configure ospf routerid 2.2.2.2
enable ospf
configure ospf restart both
configure ospf vlan all restart-helper both

SW_3
create vlan routing_1
create vlan routing_2
create vlan router_id
configure routing_1 ipaddress 192.168.1.6/30
configure routing_2 ipaddress 192.168.2.6/30
configure router_id ipaddress 3.3.3.3/32
configure routing_1 add port 24
configure routing_2 add port 1
enable loopback-mode vlan router_id
enable ipforwarding routing_1
enable ipforwarding routing_2
enable ipforwarding router_id
configure ospf add routing_1 area 0.0.0.0 link-type point-to-point
configure ospf add routing_2 area 0.0.0.0 link-type point-to-point
configure ospf add router_id area 0.0.0.0 link-type point-to-point passive
configure ospf routerid 3.3.3.3
enable ospf
configure ospf restart both
configure ospf vlan all restart-helper both

SW_4
create vlan routing_1
create vlan routing_2
create vlan router_id
configure routing_1 ipaddress 192.168.1.1/30
configure routing_2 ipaddress 192.168.1.5/30
configure router_id ipaddress 4.4.4.4/32
configure routing_1 add port 5:1
configure routing_2 add port 2:48
enable loopback-mode vlan router_id

enable ipforwarding
configure ospf add routing_1 area 0.0.0.0 link-type point-to-point
configure ospf add routing_2 area 0.0.0.0 link-type point-to-point
configure ospf add router_id area 0.0.0.0 link-type point-to-point passive
configure ospf routerid 4.4.4.4
enable ospf
configure ospf restart both
configure ospf vlan all restart-helper both

Lab 6

➔ **Descripción del LAB 6:**

Manteniendo la configuración del LAB 1, LAB 2, LAB 3, LAB 4 y LAB 5, se deberá realizar un Failover entre las tarjetas de administración o supervisoras manteniendo en ése momento una comunicación de capa 3 (OSPF) y capa 2 (SPT o EAPS). Para la comunicación de capa 3 se utilizarán las dos vlans creadas en el laboratorio anterior y que son conocidas mediante el protocolo OSPF. El PC 1 pertenecerá a una de las vlans y el PC 2 a la otra, entre ellos se transmitirá una comunicación de video y un ping. Se establecerá una llamada a través de la vlan de capa 2 llamada “Voz”.

➔ **Objetivo: Redundancia en supervisora sin perder ningún paquete.**

Esta prueba es física y en laboratorio y es totalmente transparente la actualización. Se realizará el failover de las tarjetas supervisoras y no debe existir pérdida de los servicios de Voz y Video.

➔ **Resultado: OK**

Lab 7

➔ **Descripción del LAB 7:**

Manteniendo la configuración del LAB 1, LAB 2, LAB 3, LAB 4, LAB 5 y LAB 6, se deberá realizar un upgrade de software en las tarjetas de administración o supervisoras manteniendo en ése momento una comunicación de capa 3 (OSPF) y capa 2 (SPT o EAPS). Para la comunicación de capa 3 se utilizarán las dos vlans creadas en el laboratorio anterior y que son conocidas mediante el protocolo OSPF. El PC 1 pertenecerá a una de las vlans y el PC 2 a la otra, entre ellos se transmitirá una comunicación de video y un ping. Se establecerá una llamada a traves de la vlan de capa 2 llamada “Voz”.

➔ **Objetivo: Disponibilidad**

Se realizará el upgrade de software de las tarjetas supervisoras y no debe existir pérdida de los servicios de Voz y Video. Esta prueba también consiste con la manipulación de los equipos y se puede observar que no se requiere de baja de ningún servicio y es totalmente transparente.

➔ **Resultado: OK**

Capítulo 5

Validaciones

5.1. Comprobación de la Hipótesis

Se concluye que la aplicación de los estándares IEEE 802.3ae, IEEE802.3an, IEEE 802.3ab permite mejorar la velocidad de la transmisión minimizando los inconvenientes generados por la latencia, throughput o convergencia, además de la aplicación del modelo jerárquico el cual permite la aplicación adecuada de calidad de servicio, otorga flexibilidad y seguridad de la red en la UCSM.

5.2. Validación de indicadores

5.2.1. Variable independiente

- Red de datos IP alineado a los estándares IEEE 802.3ae, IEEE802.3an, IEEE 802.3ab.

5.2.1.1. Indicadores

- Throughput
- Latencia
- Priorización
- Convergencia

5.2.1.2. Metodología para la validación

Se realizará una evaluación cualitativa y cuantitativa del escenario según el estándar 10G.

Este punto incluye resultados de la evaluación realizada por un laboratorio certificado internacionalmente Ixia.

5.2.1.3. Indicador throughput

Se pondrá en marcha el test de throughput RFC 2544.

- **Objetivo:** Para identificar el performance del switch 10GE en cuanto al data plane en el reenvío de tráfico. La IETF RFC 2544 define una prueba metodología para esta caracterización, divididos en los siguientes tres pruebas:

  - La prueba de back-to-back determina cómo el DUT responde a diferentes cantidades de frames con la mínima brecha permitida por la especificación del protocolo.
  - La prueba de perdida de frames determina como el DUT responde a los streams con cargas diferentes.
  - La prueba de throughput encuentra la tasa más alta en la cual el DUT puede reenviar frames.

- **Configuración:** Al menos dos puertos 10GE son requeridos para esta prueba. La aplicación Ixia's IxScriptmate puede ser usada para ejecutar RFC 2544.

- **Parámetros:** Seleccionar el par de puertos, modo y tamaño del frame y numero de bucles.

En la figura 5.2-1 se muestra la configuración del laboratorio con los parámetros establecidos.

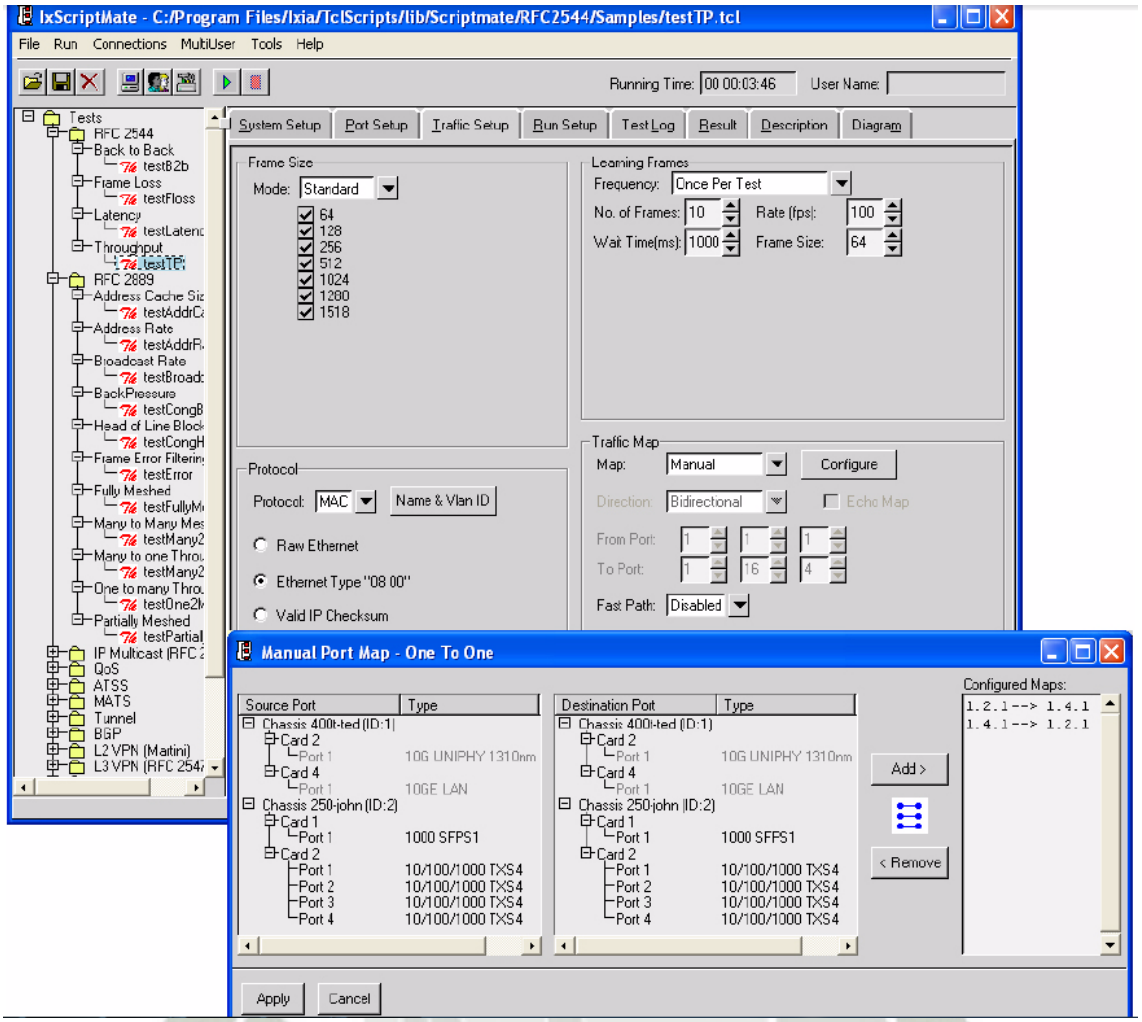

Figura 5.2-1: Indicador throughput
Fuente: IXIA Tools

- **Metodología:** Esta prueba debe incluir varios puertos de prueba para que coincida con la densidad del puerto del DUT. Idealmente, la prueba debe inundar el tráfico a cada puerto de entrada del DUT. Un número de Módulos de carga Ixia estarán conectados a la DUT. IxScriptMate de Ixia se utiliza para realizarla prueba de referencia RFC 2544.

- **Resultados:** En la figura 5.2-2 se muestran los resultados de la prueba donde se observan las tasas de throughput, en frames por segundo, obtenidas para cada tamaño de frame. Los

resultados también muestran la tasa de throughput promedio para todas las pruebas.

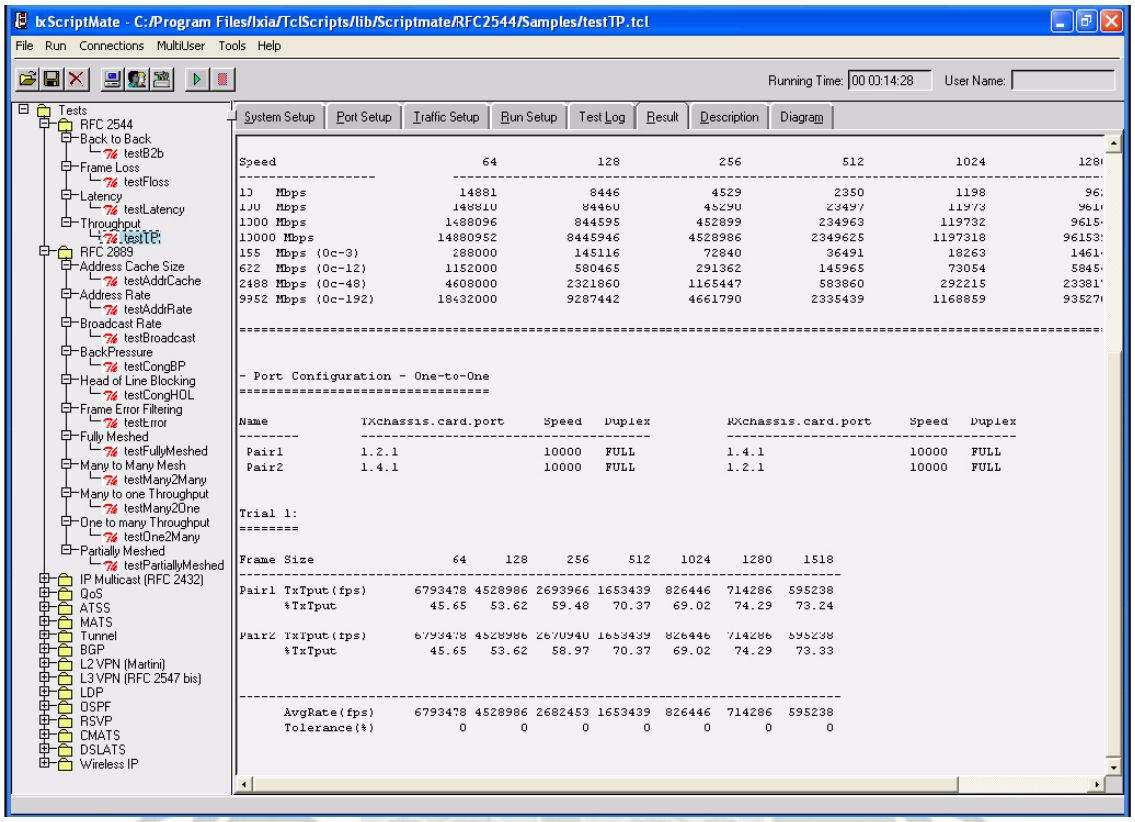

Figura 5.2-2: Indicador throughput 1
Fuente: IXIA Tools

5.2.1.4. Indicador latencia

Se pondrá en marcha el test de latencia RFC 2544.

- **Objetivo:** Para determinar la latencia del DUT, y cuanto varia con diferentes tamaños de frame.

En esta prueba, los frames serán transmitidos por un tiempo determinado. Uno por segundo, el test etiqueta un frame y lo trasmite a medio camino durante un periodo de tiempo. El test compara los tiempos registrados de los frames etiquetados

cuando este fue transmitido con el tiempo registrado cuando fue recibido. La diferencia de estos dos es la latencia.

- Configuración: Al menos dos puertos 10GE son requeridos para esta prueba, en conjunto con el IxScriptmate para la prueba de RFC2544. La latencia será medida en ambas direcciones.

- Parámetros: Seleccionar el par de puertos, modo y tamaño del frame y numero de bucles.

- Metodología:

- Los paquetes serán enviados hacia el DUT de cada modulo 10GE empezando con el menor tamaño de frame seleccionado, por un intervalo de tiempo de prueba elegido.
- La latencia promedio es medida.
- Los dos pasos anteriores se repetirán, utilizando tamaños de frames elegidos por un intervalo hasta que se llegue al tamaño máximo de frame seleccionado.

- Resultados: En la figura 5.2-3 se muestran los resultados de la prueba donde se observa la latencia en nanosegundos (ns) obtenidas para cada tamaño de frame y par de puertos. Los resultados también muestran la latencia promedio entre pares de puertos.

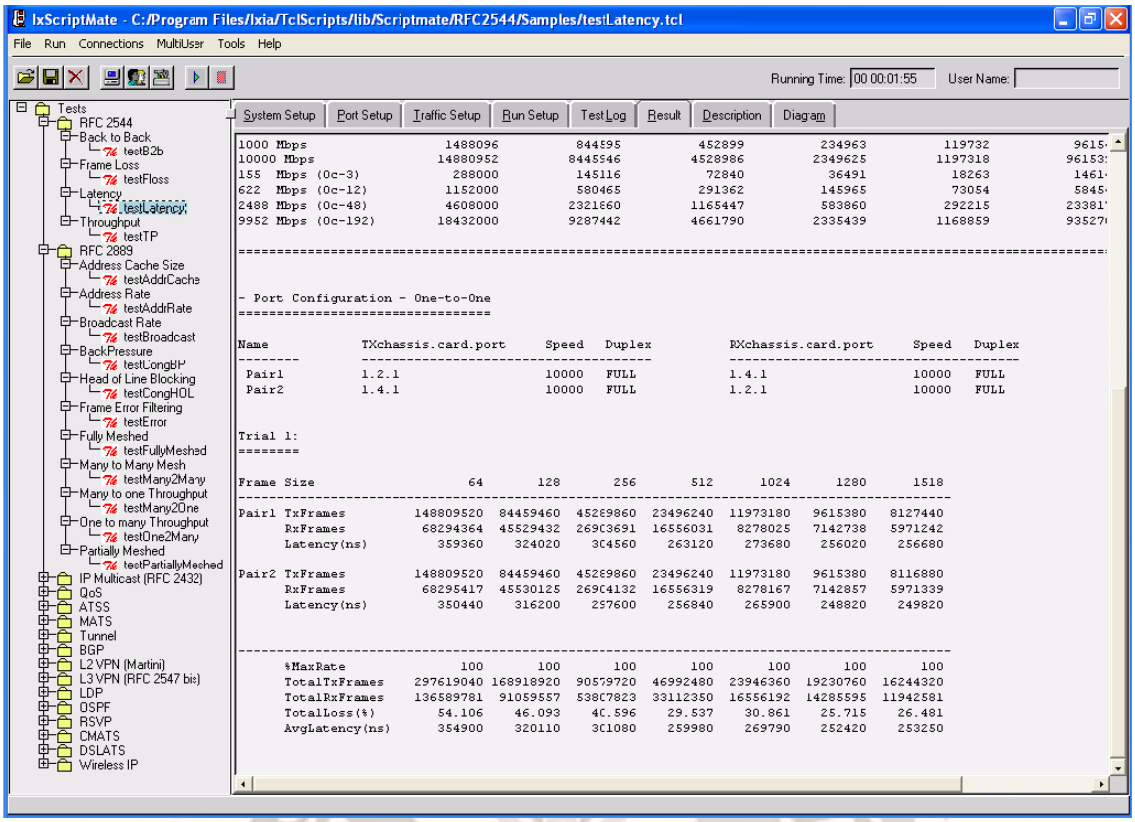

Figura 5.2-3: Indicador latencia
Fuente: IXIA Tools

5.2.1.5. Indicador priorización

- **Objetivo:** Para determinar la tasa máxima en el cual el DUT puede reenviar frames correctamente de acuerdo a las configuraciones de prioridad.

Esta prueba realiza una configuración en la cual varios puertos, cada uno con diferente prioridad, envía tráfico hacia un único puerto. El puerto receptor será sobrecargado para probar la recepción de frames con alta prioridad.

Este test soporta frames en MAC e IP; los bits de prioridad pueden ser especificados en la precedencia IP o en la cabecera de 802.1p. Latencia puede ser opcionalmente calculada por nivel de prioridad. Los resultados son: las tasas de transmisión y

recepción por prioridad, porcentaje de perdida y opcionalmente latencia para cada prioridad por puerto

- Configuración: Al menos dos puertos 10GE son requeridos para esta prueba, en conjunto con el IxScriptmate QoS Many-to-One test- En el test, un probador de puerto 10GE Ixia y dos probadores de puerto Ixia 1GE son conectados al DUT todo el tráfico dirigido hacia un único puerto 10GE en el DUT.

- Parámetros: Seleccionar los tres puertos, tamaño del frame. Parámetros QoS para cada puerto y numero de iteraciones.

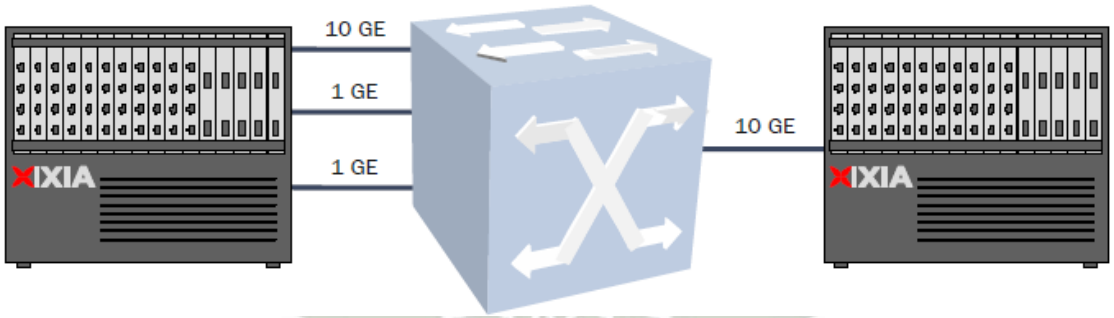

Figura 5.2-4: Indicador priorización 1
Fuente: IXIA Tools

- Metodología:

- Paquetes serán enviados hacia todos los puertos. Varios streams con variados parámetros de QoS serán enviados a puerto de egreso.

- El total de frames recibidas, latencia y reenvío de frames son medidos por prioridad.
- Los dos pasos anteriores se repetirán, utilizando tamaños de frames seleccionados por un intervalo hasta que se llegue al tamaño máximo de frame seleccionado.

- Resultados: En la figura 5.2-5 se muestran los resultados de la prueba donde se observa la latencia en nanosegundos (ns) obtenidas para cada tamaño de frame y par de puertos. Los resultados también muestran la latencia promedio entre pares de puertos.

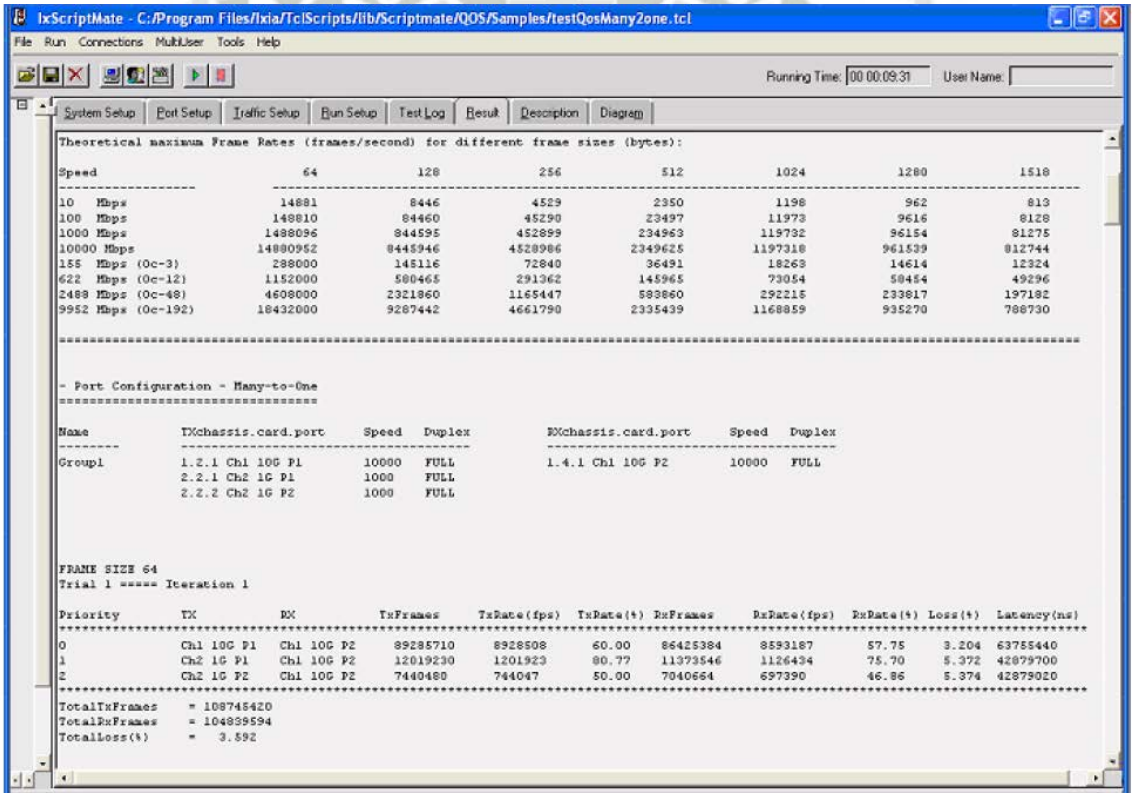

Figura 5.2-5: Indicador priorización 2
Fuente: IXIA Tools

5.2.1.6. Indicador convergencia

- Objetivo: Verificar la habilidad del switch L3 de cambiar entre rutas preferidas y menos preferidas en sus puertos 10GE cuando las rutas preferidas están caídas y re-publicadas. El test de la función de control plane en el MM del DUT 10GE.

En estas pruebas, dos puertos 10GE simulan routers OSFP, el router 1 y router. Ambos routers publican los mismos prefijos de rutas hacia la red simulada. A pesar de las rutas publicadas el router 1 tendrá métricas menores (costo menor), el cual debe causar al DUT de reenviar el tráfico desde este router 1 en vez del router 2. Después de publicar las rutas, el puerto transmisor inicia la transmisión de streams de paquetes hacia una dirección la cual está en la ruta publicada. El DUT debe reenviar todos los paquetes por la ruta con la métrica más baja router 1. Después de un intervalo de tiempo transcurrido, el puerto receptor simula la caída de las rutas del router 1. El DUT debería detectar que la ruta preferida cayó y cambiar a las rutas del router 2. Luego el router 1 re-publica sus rutas. El DUT debería de nuevo detectar el cambio y redireccionar el tráfico para utilizar el router 1 de nuevo.

- Configuración: Este puerto utiliza tres puertos de prueba uno transmite y dos reciben. Un probador de puerto Ixia (actúa como puerto transmisor) y dos Ixia 10GB probadores de puerto (puerto 1 y 2 actúan como receptores) conectados al DUT. Los puertos receptores simularan OSPF routers. El tráfico es unidireccional. El DUT debe tener tres puerto utilizados con dos puertos habilitados para OSPF routers. Todos los puertos deben tener configurada una IP y tener subnets únicas para comunicarse hacia los puertos en prueba.

- Resultados: En la figura 5.2-6 se muestran los resultados de la prueba donde se observa el promedio de convergencia para todas las rutas. En la siguiente figura muestra los resultados de la prueba para convergencia OSFP en IxScriptMate. Adicionalmente el tiempo de convergencia, también indica la cantidad de paquetes perdidos por la convergencia.

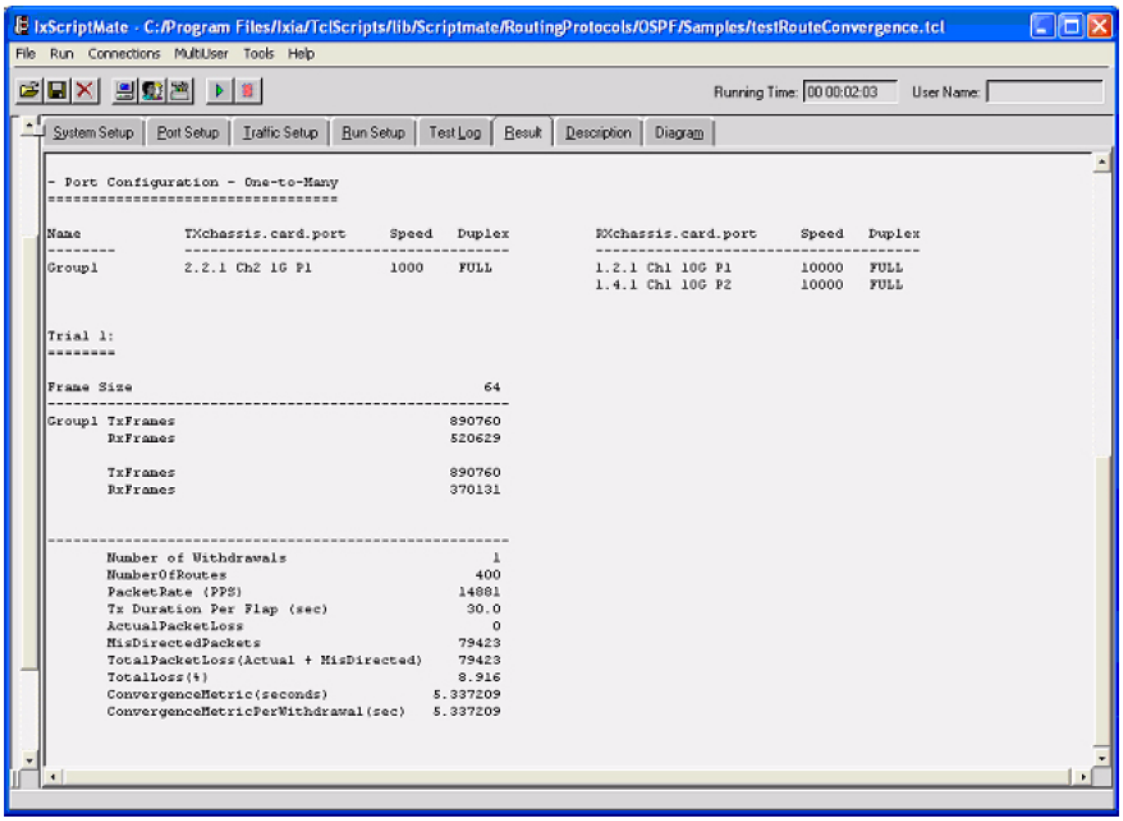

Figura 5.2-6: Indicador convergencia
Fuente: IXIA Tools

5.2.2. Variable dependiente

- Modelo de implementación Jerárquico en la red de datos IP.

5.2.2.1. Indicadores

- Escalabilidad
- Flexibilidad
- Calidad de Servicio
- Seguridad

5.2.2.2. Metodología para la validación

Se realizara una evaluación cualitativa de la aplicación de metodología en la UCSM.

5.2.2.3. Indicador escalabilidad

Si permite aplicarse a la infraestructura de red actual y a su posible expansión física y lógica además que considere diversas aplicaciones de datos sin perder su funcionalidad.

Escalabilidad física

- Objetivo: Crecimiento físico de la red, de crecer el campus de la UCSM en infraestructura ya sea con la adición de nuevos pabellones, laboratorios u otros ambientes, el modelo presentado lo soporta.

Se realizaran los siguientes escenarios supuestos:

- El tamaño del campus, crecerá en cuatro pabellones.
- Se agregaran 10 nuevos laboratorios a un pabellón actual.

- Configuración: Para el primer escenario, al menos dos puertos 10GE son requeridos para agregar un pabellón adicional o distribución (uno en el equipo de core, otro en el equipo de distribución). Para el segundo escenario, al menos dos puertos 1GE son requeridos para agregar un equipo de acceso (un puerto en el equipo de distribución y otro puerto en el equipo de acceso o laboratorio).

A priori se conoce que la escalabilidad de los equipos en capa de Core y Distribución:

- **Equipo de core: Black Diamond 8810**
  - **Escalabilidad:**
    - Máxima capacidad del equipo: 3.8 Tbps
    - Tecnológica: Soporta 40Gbps, solo cambiar tarjeta en slot.
    - Slot libres: 5, la cantidad de puertos máximos adicionales pueden ser:
      - 5 * 2 40Gbps = 10 puertos 40Gbps.
      - 5 * 8 10Gbps = 40 puertos 10Gbps.
      - 5 * 48 1Gbps = 240 puertos 1Gbps.
    - Agregación backbone: Hasta 8 puertos similares. Entonces:
      - BW = 8 * Velocidad de puerto

- **Equipo de distribución: Extreme X460-24P**
  - **Escalabilidad:**
    - Máxima capacidad del equipo: 176-328 Gbps
    - Densidad de puertos
      - Equipada con: 24 puertos 10/100/1000 Mbps BaseT.

        - Tarjeta Opcional: 2 puertos 10 Gbps full duplex BaseSR.
    - Agregación backbone: Hasta 20Gbps
    - Agregación enlace de acceso: Hasta 8Gbps
    - Apilamiento: Es posible.

- **Equipo de distribución: Extreme X460-48P**
    - **Escalabilidad**
        - Máxima capacidad del equipo: 176-328 Gbps
        - Densidad de puertos
            - Equipada con: 24 puertos 10/100/1000 Mbps BaseT.
            - Tarjeta Opcional: 2 puertos 10 Gbps full duplex BaseSR.
        - Agregación backbone: Hasta 20Gbps
        - Agregación enlace de acceso: Hasta 8Gbps
        - Apilamiento: Es posible.

- Parámetros: Seleccionar la cantidad de puertos requeridos en ambos escenarios.

- Resultados: En la figura 5.2-7 y 5.2-8 se muestran los resultados de la prueba donde ser observa que el crecimiento físico es posible ya que la implementación de la metodología propone escalabilidad de la red física.

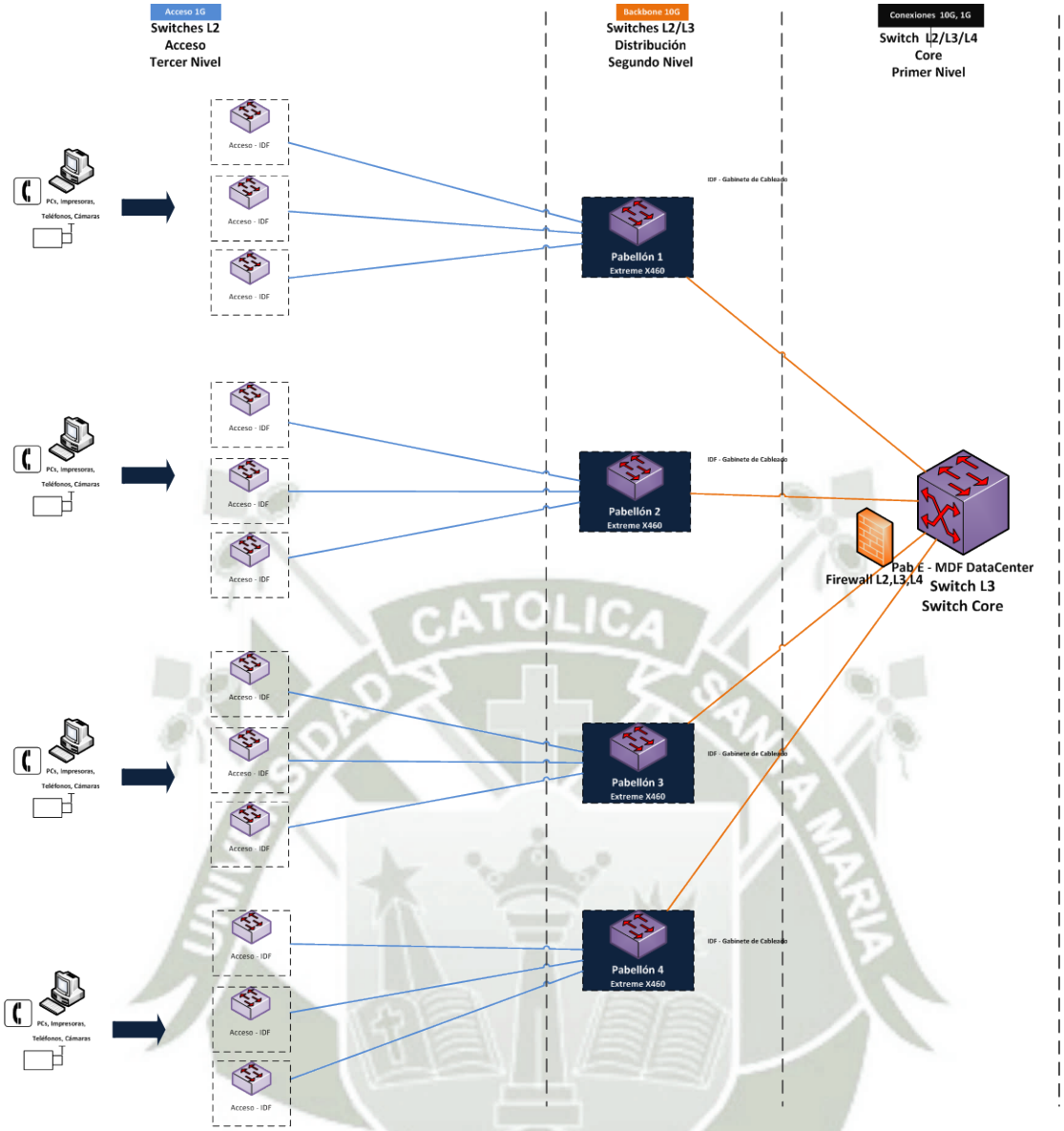

Figura 5.2-7: Indicador escalabilidad 1
Fuente: Elaboración Propia

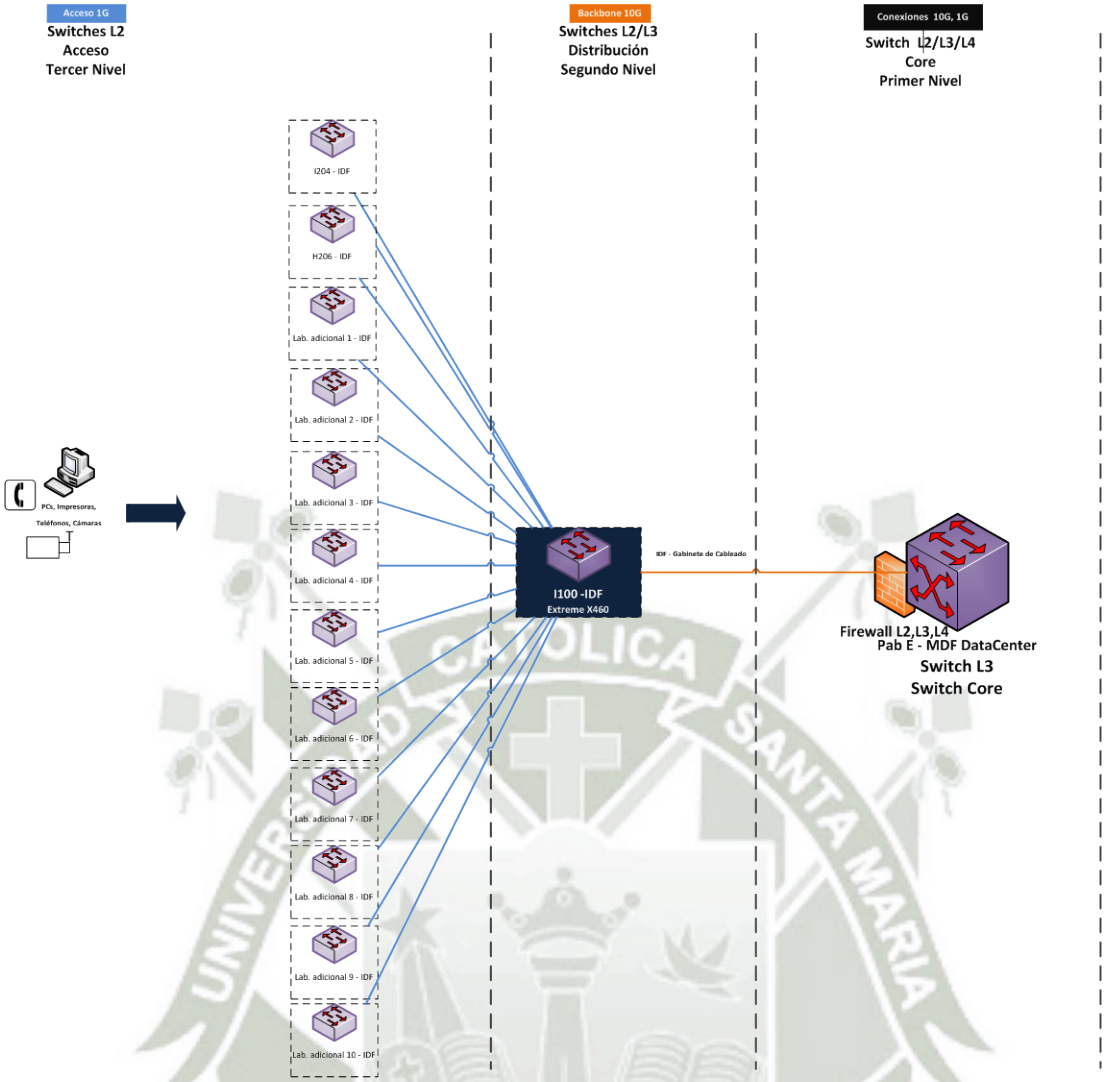

Figura 5.2-8: Indicador escalabilidad 2
Fuente: Elaboración Propia

Escalabilidad lógica

- **Objetivo:** El crecimiento físico de la red va de la mano con el crecimiento lógico de la red, para esto se requieren nuevas direcciones IP de acuerdo a la VLAN que sea afecta, el modelo presentado lo soporta.

Se realizaran los siguientes escenarios supuestos:

- Se agregaran nuevas oficinas administrativas.
- Se agregaran nuevos laboratorios de una facultad.

- **Configuración:** Para el primer escenario, se crearan dos nuevas oficinas a las unidades administrativas Rectorado, Vicerrectorado Académico y Administrativo. Para el segundo escenario, se incrementara en dos laboratorios cada Facultad.

- **Parámetros:** Seleccionar la cantidad de direcciones son requeridas en ambos escenarios.

- **Resultados:** En la tabla 5.2-1 y 5.2.2 se muestran los resultados de la prueba donde se observa que el crecimiento lógico es posible ya que la implementación de la metodología propone escalabilidad de la red lógica.

Ítem	Descripción	Act.	Adic.	Tot.	Disp.	Nombre	Vlan	Mas.	Dir. Red
Unidad Administrativa - Rectorado									
1	Rectorado	4	1	5	14	ADM_Rectorado	100	28	10.0.100.0/28
2	Oficinas Dependientes	58	6	64	254	ADM_Rectorado_dep	101	24	10.0.101.0/24
3	Oficina de Informática	34	4	38	126	ADM_Informatica	102	25	10.0.102.0/25
Unidad Administrativa - Vicerrectorado Académico									
4	Vicerrectorado Académico	7	1	8	14	ADM_Vracad	110	28	10.0.110.0/28
5	Oficinas Dependientes	40	4	44	254	ADM_Vracad_dep	111	24	10.0.111.0/24
6	Biblioteca	42	4	46	126	ADM_Biblioteca	113	25	10.0.113.0/25
7	Admisión	9	1	10	32	ADM_Admision	114	27	10.0.114.0/27
8	Centro Pre Universitario	9	1	10	32	ADM_Cpu	115	27	10.0.115.0/27
Unidad Administrativa - Vicerrectorado Administrativo									
9	Vicerrectorado Administrativo	5	1	6	14	ADM_Vradm	120	28	10.0.120.0/28
10	Oficinas Dependientes	56	6	62	254	ADM_Vradm_dep	121	24	10.0.121.0/24
11	Contabilidad	15	2	17	62	ADM_Contabilidad	122	26	10.0.122.0/26
12	Impresiones	10	6	16	30	ADM_Cimpresiones	123	27	10.0.123.0/27
Unidades Académicas									
12	Facultades Pregrado	125	13	138	254	ADM_Pregrado	130	24	10.0.130.0/24
13	Escuela de Posgrado	9	2	11	30	ADM_Postgrado	131	27	10.0.131.0/27
14	Institutos	15	2	17	30	ADM_Institutos	132	27	10.0.132.0/27
15	Clínicas	10	2	12	30	ADM_Institutos	133	27	10.0.133.0/27
Campus									
16	Organismos Autónomos	8	1	9	14	CA_OR_Autonomos	140	27	10.0.140.0/27
17	Representaciones Gremiales	15	2	17	30	CA_OR_RG	141	27	10.0.141.0/27
18	Otros Organismos	3	1	4	14	CA_OR_otros	142	28	10.0.142.0/28
19	Porterías	6	1	7	14	CA_Porterias	143	28	10.0.143.0/28
20	Reniec	3	1	4	14	CA_OR_Reniec	144	28	10.0.144.0/28
21	Auditoria Externa	5	1	6	14	CA_OR_Auditoria	145	28	10.0.145.0/28

Tabla 5.2-1: Red Administrativa escalable
Fuente: Elaboración Propia

Ítem	Descripción	Act.	Adic.	Tot.	Disp.	Nombre	Vlan	Mas.	Dir. Red
Ciencias Sociales									
1	**Fac. Cs. Sociales**	*91*	*21*	**112**	**254**	ACAD_fctsh	151	24	10.0.151.0/24
	FCTSH								
Ciencias Jurídicas Empresariales									
2	**Fac. Cs. Jurídicas Empresar.**	*109*	*21*	**130**	**254**	ACAD_cje	153	24	10.0.153.0/24
	FCCF								
	FCEA								
	FCJP								
Ciencias de la Salud									
3	**Fac. Cs de la Salud**	*21*	*21*	**42**	**254**	ACAD_cs	154	24	10.0.154.0/24
	Facultad de Enfermería								
	Facultad de Medicina								
	Facultad de Odontología								
	FCFBB								
	Facultad de Obstetricia								
Ciencias e Ingenierías									
4	FCIBQ	*21*	*21*	**42**	**254**	ACAD_fcibq	156	24	10.0.156.0/24
5	FAICA	*56*	*10*	**66**	**254**	ACAD_faica	157	24	10.0.157.0/24
6	P.P Ing. Industrial, Minas	*64*	*21*	**85**	**254**	ACAD_ppindustrial	158	24	10.0.158.0/24
7	P.P Ing. de Sistemas	*117*	*0*	**117**	**254**	ACAD_ppsistemas	159	24	10.0.159.0/24
8	P.P. Ing. Mecánica	*91*	*21*	**112**	**254**	ACAD_ppmecanica	160	24	10.0.160.0/24
9	P.P. Ing. Electrónica	*77*	*21*	**98**	**254**	ACAD_ppelectronica	161	24	10.0.161.0/24
Escuela de Postgrado									
10	Escuela de Post Grado	*34*	*21*	**55**	**126**	ACAD_epg	163	25	10.0.163.0/25
Campus									
11	Aulas Campus	*120*	*12*	**132**	**254**	ACAD_Aulas	164	24	10.0.164.0/24
12	SUM	*12*	*0*	**12**	**30**	CA_Sum	165	27	10.0.165.0/27
13	Auditorios	*6*	*2*	**8**	**14**	CA_Auditorios	166	28	10.0.166.0/28
Otras Áreas									
14	Biblioteca Virtual	*62*	*10*	**72**	**126**	ACAD_bvirtual	171	25	10.0.171.0/25
15	Estadística	*25*	*2*	**27**	**62**	ACAD_estadistica	172	26	10.0.172.0/26
16	Proyecto Mercurio	*14*	*2*	**16**	**30**	ACAD_pmercurio	173	27	10.0.173.0/27
17	CICA	*14*	*2*	**16**	**30**	ACAD_cica	174	27	10.0.174.0/27
18	Internos FCFBB	*14*	*2*	**16**	**30**	ACAD_in_fcfbb	175	27	10.0.175.0/27
Institutos									
19	Informática	*42*	*21*	**63**	**254**	ACAD_iinformatica	181	24	10.0.181.0/24
20	Instituto de Idiomas	*66*	*66*	**132**	**254**	ACAD_iidiomas	182	24	10.0.182.0/24

Tabla 5.2-2: Red Académica escalable
Fuente: Elaboración Propia

5.2.2.4. Indicador flexibilidad

Este indicador mide la capacidad del modelo para adaptarse a una nueva situación, es decir, si se adecúa a las necesidades existentes en la UCSM, y que es flexible al cambio debido a la ampliación de requerimientos técnicos o de negocio.

- **Objetivo:** La modificación de parámetros de red debido a nuevos requerimientos técnicos luego de la implementación, el modelo presentado lo soporta.

Se realizara el siguiente escenario supuesto:

- Se modificara el requerimiento de red en los laboratorios del Programa Profesional de Ing. de Sistemas.

- **Configuración:** Se subneteara la vlan asignada al programa profesional mencionado ID: 159, segmento 10.0.159.0/24, en las siguientes subredes:

- Alumnos →cantidad: 95 conexiones habilitadas.
- Docentes →cantidad: 11 conexiones habilitadas.
- Coordinación →cantidad: 2 conexiones habilitadas.

La configuración de los parámetros de subred se dan el equipo de Core, y la modificación de subred se realizan en los equipos cliente.

- **Parámetros:** Seleccionar la cantidad de direcciones son requeridas y calcular crecimiento futuro.

- **Resultados:** En la tabla 5.2-3 se muestran los resultados de la prueba donde se observa que el cambio es flexible ya que solo afecta a la vlan seleccionada entonces es posible el cambio sin

mayores problemas ya que la implementación de la metodología propone flexibilidad.

Subred	Dirección de red	Puerta de enlace	Host
Alumnos	10.0.159.0/26	10.0.159.1/26	192
Docentes	10.0.159.224/27	10.0.159.193/26	32
Coordinación	10.0.159.224/29	10.0.159.225/26	8

Tabla 5.2-3: Indicador flexibilidad
Fuente: Elaboración Propia

5.2.2.5. Indicador calidad de servicio

Este indicador muestra la aplicación de las colas de calidad de servicio establecidas según la funcionalidad de las diversas aplicaciones mapeadas según sus características.

- **Objetivo:** Identificar las colas de calidad de servicio basadas en diffserv de acuerdo a la criticidad de la aplicación, el modelo presentado lo soporta.

- **Configuración:** Se reconocen los tipos de tráfico existentes en la red implementada a continuación se detalla:

  - Trafico común
  - Trafico de la red Administrativa y de administración de hardware.
  - Tráfico de servicios publicados
  - Tráfico de servicios internos
  - Tráfico de base de datos
  - Tráfico de video

- Tráfico de voz
- Tráfico de protocolos de control de red

- Parámetros: Seleccionar la cola de prioridad de acuerdo a la aplicación.

- Resultados: En la tabla 5.2-4 se muestran los resultados de la prueba donde ser observa que la aplicación de calidad de servicio es factible ya que existen colas de prioridad específicas y estas pueden ser aplicadas de acuerdo a la necesidad de la red. Entonces es posible su aplicación ya que la implementación de la metodología propone calidad de servicio.

Nivel	Prioridad Tipo de tráfico	qos profile	Aplicado a tipo de trafico:
0	Best effort	qp0	de la red Académica
1	Tareas de fondo	qp1	de la red Administrativa y de administración de hardware.
2	Estándar	qp2	de servicios publicados
3	Carga excelente	qp3	de servicios internos
4	Carga controlada	qp4	de base de datos
5	Video	qp5	de video
6	Voz	qp6	de voz
7	Reservado para el control de red	qp7	de protocolos de control de red

Tabla 5.2-4: Indicador calidad de servicio
Fuente: Elaboración Propia

5.2.2.6. Indicador seguridad

Es la capacidad del modelo para aplicar mecanismos de seguridad para asegurar la información que viaja a través de la red, esto mediante políticas aplicadas en los equipos implementados y contar con al menos dos filtros de seguridad en la red.

- **Objetivo:** Identificar los mecanismos de seguridad desarrollados en la red implementada, la configuración de las listas de control de acceso ACL para evitar las comunicaciones no permitidas, el modelo presentado lo soporta.

- **Configuración:** Se implementara listas de control de acceso ACL y se cargaran a los equipos que las soporten en las distintas capas ya sea, acceso, distribución, core, o granja de servidores.

- **Parámetros:** Identificar las direcciones ip/mac, puertos, vlan de origen. Identificar las direcciones ip/mac, puertos, vlan de destino.

- **Resultados:** En la figura 5.2-9 se muestran los resultados de la prueba donde se observa que la seguridad de la red está cubierta debido a la implementación de ACL en los equipos propuestos. Entonces es posible su aplicación ya que la implementación de la metodología propone calidad de servicio.

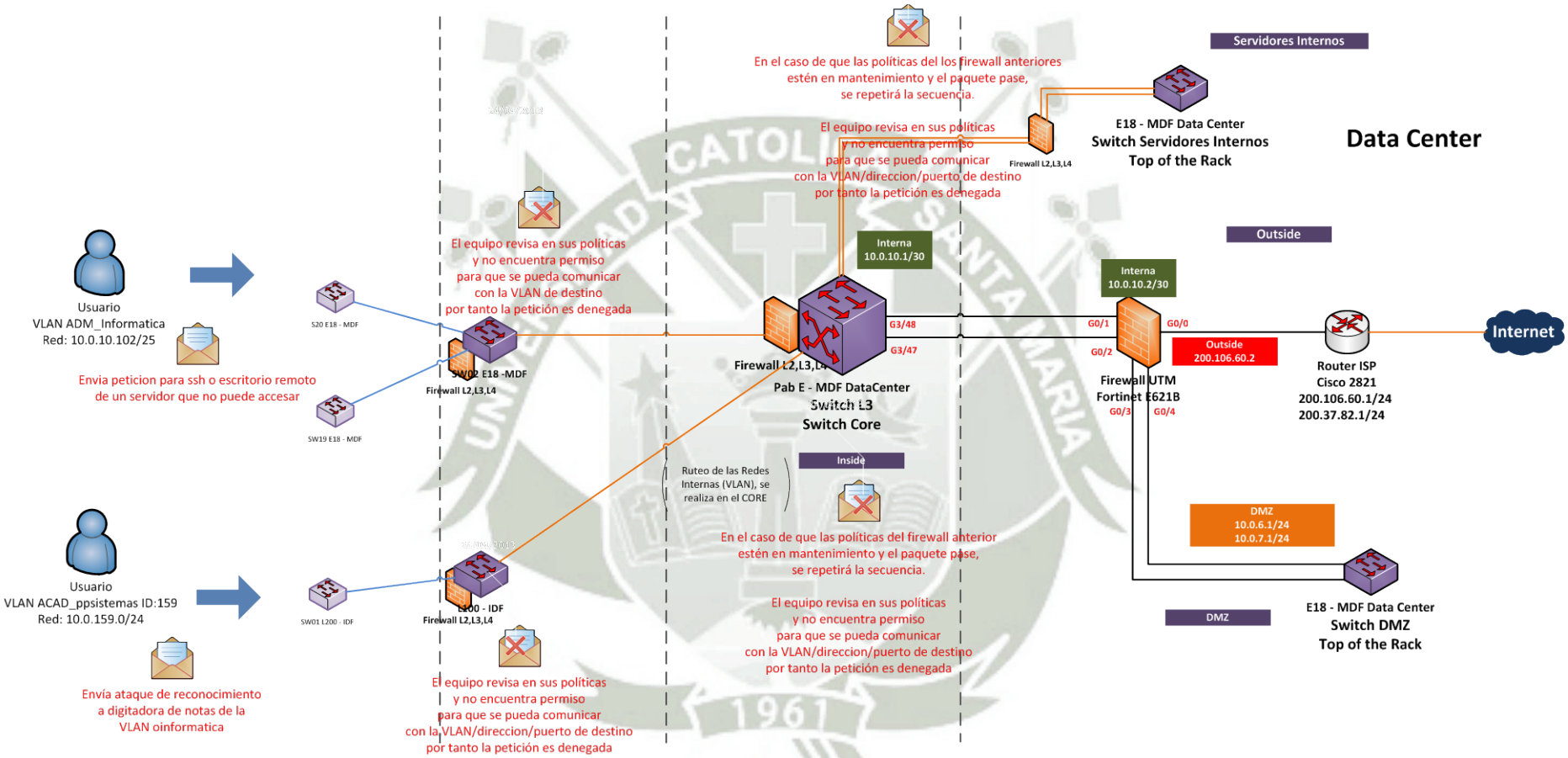

Figura 5.2-9: Indicador seguridad
Fuente: Elaboración Propia

CONCLUSIONES

1. Se logró implementar la red basada en un modelo jerárquico de acuerdo al diseño propuesto obteniendo los tres niveles de red: core, distribución y acceso permitiendo que la red sea confiable y segura.

2. El modelo de red demostró adaptarse a los requerimientos específicos que demanda una red de campo universitario utilizando el estándar IEEE 802.1q para la creación de VLAN.

3. El modelo propuesto está basado en tecnología Ethernet y se adapta perfectamente a los incrementos de velocidad propios de la evolución de la tecnología.

4. Se concluye que el modelo propuesto implementa mecanismos de seguridad debido al diseño en tres niveles implementadas por medio de ACLs. En cuanto a calidad de servicio se demuestra su efectividad con el análisis de las aplicaciones que apuntan a las ocho colas propuestas según su prioridad.

5. Se analizó las principales marcas ofrecidas en el mercado local relacionando su arquitectura con los requerimientos del modelo propuesto, concluyendo sobre su importancia en función de la escalabilidad y funcionalidad por ser las características de mayor importancia en los estándares propuestos.

6. Se analizó los protocolos de capa 2 y 3 que cumplen con los requerimientos técnicos solicitados concluyendo que si existen protocolos universales y propietarios se debe tomar en cuenta los pros y contras de cada uno de estos.

7. Se analizó las herramientas para la administración de red concluyendo que se debe optar por herramientas que se integren a la infraestructura de la organización para una mejor administración.

RECOMENDACIONES

1. Se recomienda la implementación de la metodología en cualquier empresa u organización de cualquier rubro no necesariamente educativa, siguiendo detalladamente los pasos indicados en la presente metodología. Tener en cuenta que la realización de cada paso conlleva al siguiente en tal sentido ser precavido con el levantamiento de requerimientos y en su implementación posterior.

2. El modelo presentado no implementa características de alta disponibilidad en las capas de acceso, distribución, core, granja de servidores y la red enterprise se recomienda la implementación de esta característica a la red de la UCSM.

3. El modelo presentado e implementado solo presenta la red del campus Umacollo de la UCSM, se recomienda aplicar el modelo de ser posible y factible en los otros campus y realizar su interconexión entre los mismos.

4. En la elección de la marca de los dispositivos de red como switches L2, L3, L4 se recomienda tener en cuenta la disponibilidad, soporte, garantía, documentación según el vendor que se elija, ya que todas las marcas pueden ser comercializadas localmente pero la disponibilidad, soporte, garantía y documentación puede que no sea la adecuada para el proyecto que se vaya a implementar.

BIBLIOGRAFÍA

[CCN2007] Cisco. (2007) Currícula CCNA Exploration 4.0.

[EPA2005] Encarna Pastor, "Aplicaciones Distribuidas Avanzadas, Curso de Doctorado 2004 - 2005,"

[MEF2001] Michael E. Flannagan, *Administering Cisco QoS for IP Networks*.: Syngress Publishing, 2001.

[OWE2005] Michael E. Flannagan, *Administering Cisco QoS for IP Networks*.: Syngress Publishing, 2001.

[ODE2005] Michael E. Flannagan, *Administering Cisco QoS for IP Networks*.: Syngress Publishing, 2001.

[TSZ2004] Tim Szigeti and Christina Hattingh, *End-to-End QoS Network Design*.: Cisco Press, 2004.

[POP2011] Priscilla Oppenheimer, Top-Down Network Design," 3rd ed., Cisco Press, 2011

[MOY1998] Moy, J.T., OSPF: Anatomy of an Internet Routing Protocol. Reading, Massachusetts: Addison Wesley Publishing Company, Inc., 1998.

[CLA1999] Clark, K. and K. Hamilton. Cisco LAN Switching. Indianapolis, Indiana: Cisco Press, 1999.

[SEI1998] Seifert, R. Gigabit Ethernet: Technology and Applications for High-Speed LANs. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 1998.

[SEI2008] Seifert, R. and J. Edwards The All New Switch Book: The Complete Guide to LAN Switching Technology, 2nd ed. New York, New York: John Wiley & Sons, Inc, 2008.

[DOY1998] Doyle, J. Routing TCP/IP, Volume I. Indianapolis, Indiana: Cisco Press, 1998.

[DOY2001] Doyle, J. and J. D. Carroll Routing TCP/IP, Volume II. Indianapolis, Indiana: Cisco Press, 2001.

[BUC1996] Buchanan, R. The Art of Testing Network Systems. New York, New York: John Wiley & Sons, Inc., 1996.

[FAR2002] Faraz S., Z. Aziz, J. Lui, A. Martey, and Z. Azia Troubleshooting IP Routing Protocols. Indianapolis, Indiana: Cisco Press, 2002.

[HAU2000] Haugdahl, J.S. Network Analysis and Troubleshooting. Reading, Massachusetts: Addison-Wesley Publishing Company, Inc., 2000.

[OPP2002] Oppenheimer, P. and J. Bardwell Troubleshooting Campus Networks. New York, New York: John Wiley & Sons, 2002.

[TEA2007] Teare, Diane CCDA Self-Study: Designing for Cisco Internetwork Solutions (DESGN), 2nd ed. 640-861, Indianapolis, Indiana: Cisco Press, 2007

[1] http://www.wikilearning.com/monografia/epistemologia_contable-concepto_de_modelo/12713-3

[2] http://definicion.de/modelo/

[3] http://es.wikipedia.org/wiki/Modelado

[4] http://es.wikipedia.org/wiki/Modelo_OSI

[5] http://www.cisco.com/en/US/technologies/tk543/tk766/technologies_white_paper 09186a00800a3e3f.html

[6] http://standards.ieee.org/findstds/standard/802.3-2005-Cor_2-2007.html

[7] http://standards.ieee.org/findstds/standard/802.3an-2006.html

[8] http://standards.ieee.org/findstds/standard/802.3ab-1999.html

[9] http://line-provider.com/articles/disaster-recovery-cost-of-downtime/

[10] http://line-provider.com/whitepapers/10-gigabit-ethernet-bandwidth-quotes-whitepaper/

[11] http://line-provider.com/whitepapers/optical-fiber-and-10-gigabit-ethernet/

[12] http://www.ixiacom.com/pdfs/library/white_papers/10ge.pdf

[13] http://enterprise.alcatel lucent.com/private/active_docs/omnistack_6100_brochure.pdf

[14] http://www.sistas.com.tr/PDF%5CALCATEL_LUCENT%5CIP-Networking%5COmniSwitch-6600-Family.pdf

[15] http://www.extremenetworks.com/solutions/solutions-hub.aspx

[16] http://www.extremenetworks.com/Resources/library.aspx?q=wp

ANEXOS

Anexo A: Comparación entre equipos 10Gigabit Ethernet

➔ Equipos de Core

MARCA	BROCADE	EXTREME NETWORKS	CISCO
MODELO	**BigIron RX-8**	**BlackDiamond 8810**	**CAT6509 w/sup720**
PARAMETROS FISICOS			
Medidas H/W/D (pulgadas)	12.21" x 17.45" x 22.5"	24.47" x 17.51" x 18.23"	25.3" x 17.2" x 18.2"
Unidades de Rack (RUs)	7	14	15
Total de Chassis soportado en 1 Rack	6	2	2
EQUIPAMIENTO			
Slots	13	10	9
Slots Utilizables	8	8	7
Redundancia de Motor de Switching	Si, 2 Mgmt Module Slots	Si, 2 Mgmt Module Slots	Si, utiliza slots utilizables
10/100/1000 densidad de puertos por modulo	24	24 o 48	16 o 48
SFP densidad de puertos por modulo	24	24 o 48	24 o 48
10GbE densidad de puertos por modulo	4	4 o 8 o 24	4
Numero de puertos 10Gb NO-BLOQUEANTE por modulo	4	8	2
DENSIDAD DE PUERTOS CON MM Redundante			
10/100/1000 Puertos MAX por SWITCH	384*	768	336
SFP Puertos MAX por SWITCH	192	400	336
10GbE Puertos MAX por SWITCH	32	192	32
Numero de puertos 10Gb NO-BLOQUEANTE por Switch	32	64	14
DENSIDAD DE PUERTOS CON MM Redundante			
10/100/1000 Puertos MAX por RACK	2304	1536	672
SFP Puertos MAX por RACK	1152	800	672
10GbE Puertos MAX por RACK	192	384	56
Numero de puertos 10Gb NO-BLOQUEANTE por Rack	192	128	28
OPCIONES DE FUENTE DE PODER			
fuente de poder Bays	4	6	2
Opciones AC y DC	Si	Si	Si
Redundante y Removible	Si	Si	Si
Numero mínimo de fuentes	2	2	1
Energía de salida por fuente de poder	1200W	1200W	2500W, 3000W, 4000W, 6000W
Eficiencia por fuente de poder	82%	80%	70 - 80%
PORFORMANCE			
Máxima RAM	512MB SDRAM	1GB SDRAM	512 MB DRAM

Capacidad Total de Switch	1.92 Tbps	3.8 Tbps	720 Gbps
L2 Throughput (Mpps)	570 Mpps	2.84 Tbps en L2 y L3	Hasta 400Mpps
Fabric por Modulo	48 Gbps	80 Gbps	20 Gbps
LAYER 2 SWITCHING			
Max. Numero de direcciones MAC por Switch	256k por system	512K por System	64k por system
Jumbo Frames	Si, 9k	Si	No todos los modulos soportan jumbo frames
MAC Filter	L2 MAC Filtering	L2 MAC Filtering	L2 MAC Filtering
VLANS			
Numero deVLANs	4096	4094	4095
VLAN Criterio (Basado en puerto, Basado en Protocolo, etc.)	L2: Puerto, L3: Protocol, IP Subnet	Basado en puerto, Protocolo y MAC.	Puerto
VLAN Propagation (VTP)	No	No	Si
VLAN Tagging	802.1q, Dual Mode, SAV/Q-en-Q	802.1Q, Q-en-Q	802.1q, Q-en-Q
STP			
STP por VLAN	Si	Si, pero PVST+	Si
Compatibilidad con Cisco PVST	Si	No	Si
STP fast Forwarding (STP fast, uplink fast, BB fast)	Fast Port, Fast Uplenk	Edge Safe guard, link type, restricted role	Portfast, Uplinkfast
STP enable/disable por Port / VLAN	Si	Si	Si
RSTP (802.1w)	802.1w-compatible	Si	Si
MSTP (802.1s)	Si, 17 enstances max	Si	Si
STP Alternativas			
Physical Port Redundancy	UDLD, RFN, LFS	ELRP no utiliza STP	UDLD
VSRP	Si, Hasta 256 groups	No, pero existe similar en Extreme is ESRP	No
MRP	Si, Phase I y II	No	No
Topology Groups	Si	Si	No
ESQUEMAS DE DIRECCIONAMIENTO			
Subnetting	Si	Si	Si
LAG			
802.3ad	Si	Si	Si
Numero de Puertos por Trunk Group	Hasta 8 puertos	Hasta 8 puertos	Hasta 8 puertos
Puertos Tagged soportados en Trunk Group	Si	Si	Si
Compatibilidad con Cisco EtherChannel	Si	Si	Si
MULTICAST			
IGMP	Si	Si	Si
IGMP snooping	Release 2.3	Si	Si
Stom Control	Broadcast, Multicast, Unknown Unicast	Broadcast, Multicast y Unknown Unicast	Multicast & Unicast on Gig only, Broadcast
Multicast Suppression en hardware	Si	Si	Si
Broadcast Suppression en hardware	Si	Si	Si
Rate Limiting	Si	Si	Si
QOS			

Service Policies	Si	Si	Si
Hardware Queues por puerto	4	8	2-8, depende de puerto
802.1p Honoing	Si	Si	Si
802.1p Marking	Si	Si	Si
DSCP/ TOS/ IP Prec Honoing	Si	Si	Si
DSCP/ TOS/ IP Prec Marking	Si	Si	Si
Rate Limiting / Shaping (BW allocation)	Si	Si	Si
Criterio de clasificacion	DSCP/ToS, IP/MAC Source/Dest, Source/Dest TCP/UDP Port#, 802.1p, Port, VLAN	DSCP/ToS, IP/MAC Source/Dest, Source/Dest TCP/UDP Port#, 802.1p, Port, VLAN	DSCP/ToS, IP/MAC Source/Dest, Source/Dest TCP/UDP Port#, 802.1p, Port, VLAN
L2/L3	Si	Si	Si
Capacidad de Policing	single- y two-rate, Traffic Colo Marker	Single y Dual Rate	single- y two-rate, Traffic Colo Marker
Capacidad de evitar congestion	WRED o Tail Drop	No se utiliza el equipo es no bloqueante	WRED o Tail Drop
PRIORIZACION			
Tipos de priorizacion	SP, WFQ, SP+WFQ, Deficit WFQ	Strict-prioity y weighed round robin (SP y WRR)	WRR y Strict Priority
LAYER 3 - IPv4			
Routing Protocols	RIPv1/v2, OSPF, BGP, ISIS	RIPv1/v2, OSPFv2, IS-IS, BGP	RIPv1/v2, OSPF, BGP, ISIS
Max. Routes en IPv4 Fowarding Table	512K	512K por System	256K
Max. IPv4 Routes Soportadas	1 Million	1 Million	500 K
Maximum Numero deBGP Routes en the RIB	1 Million	1 Million	150K
Layer 3 Redundancy (e.g. VRRP, HSRP, ESRP,...)	VRRP, VRRP-e	VRRP y ESRP	HSRP, VRRP
Policy Based Routing	Si	Si	Si
MPLS	No	Si, necesita licencia	No
Características de IPv6			
IPv6 soportado en Hardware	Si	Si	Si
Routing Protocolos	RIP NG, OSPFv3, ISIS, BGPv6	RIP NG, OSPFv3, IS-IS y BGPv6	RIP NG, OSPFv3, BGPv6
Máximo Numero de IPv6 Routes en Fowarding Table	64,000	8.000 en Hardware y 65.000 en Software.	128,000
Multicast Routing PIM, DVMRP?			
Multicast Routing PIM, DVMRP?	Si	PIM	Si
Modes of PIM	Sparse, Dense, SSM	Sparse, Dense y SSM	Sparse, Dense
PIM Snooping	No	Si	Si
MLD v1/v2	Si	Si	Si
LAYER 4 -7 FEATURES			
Funcionalidades	Classification, (Re-Marking, Policing by ACL-Policies	Classification, (Re-Marking, Policing by ACL-Policies	Classification, (Re-Marking, Policing by ACL-Policies

DISPONIBILIDAD			
Fuentes de poder redundantes	Si	Si	Si
Motor de switching redundante	Si	Si	Si
Mecanismos de failover	Hitless Management Failover	Hitless Management Failover	Hitless Management Failover
Motor de Switching Hot Swappable	Si	Si	Si
Port Module Hot Swappable	Si	Si	Si
Switch Fabric Hot Swappable	Si	Si	Si
ADMINISTRABILIDAD			
CLI	Si	Si	Si
WEB enterface	Si	Si	Si
Out of band. (ser., eth.)	Serial, Ethernet 10/100/1000	Serial, Ethernet 10/100 base-T	Serial
ASCII Config.	Si	Si	Si
Herramientas de administración (ej. HP NNM)	IronView Netwok Manager (enM), integrable con HP NNM	Ridgelene 3.0, integrable con HP NNM	CiscoWoks
sFlow (RFC 3176)	NetFlow, sFlow RFC 3179	Sflow version 5	Netflow
SNMP	V1, V2c, V3	V1 y V2c, V3	V1, V2c, V3
SNMP-V3	Si	Si	No
RMON/ RMON V2	RFC1757 Groups 1, 2, 3, 9	RFC1757 Groups 1, 2, 3, 9	RFC1757 Groups 1, 2, 3, 9
Licencia adicional por RMON?	No	No	Si
NTP	SNTP	SNTP version 4	Si
DNS resolver	Si	Si	Si
Syslog Logging	Si	Si	Si
Temporature Sensor	Si	Si	Si
Config-Backup via tftp / ftp / secure copy	TFTP / SCP	TFTP / SCP-2 / SFTP	TFTP / SCP
SEGURIDAD			
Privileged Access Level	SU, PC, RO	Admln y User	SU, PC, RO
Radius / TACACS+	RADIUS / TACACS / TACACS+	Radius / TACACS+	RADIUS / TACACS / TACACS+
Access Control Lists	Si	Si	Si
IPv4 ACLs Soportadas	Si	Si	Si
IPv6 ACLs Soportadas	Si	Si	Si
Access Profiles	Si	Si	Si
Network Login (802.1x) via Client SW	Si	Si	Si
SSH2 Client + Server	Si	Si	Si
Secure Copy	Si	Si	Si
TROUBLESHOOTING			
Debugging	CLI via Console, Telnet o SSH	CLI via Console, Telnet o SSH	CLI via Console, Telnet o SSH
Diagnostics	show y debug cmd, statistics	show y debug cmd, statistics	show y debug cmd, statistics
Traffic Mirroing	Si	Si	Si
CPU Load por Process?	Si	Si	Si
Memoy Utilization por Process?	Si	Si	Si

IP Tools (e.g. Ping, extended Ping, extended trace)	extended Ping & Trace	extended Ping & Trace	extended Ping & Trace

➔ **Equipos de Distribución**

Marca	BROCADE	EXTREME NETWORKS	CISCO
Modelo	**624S-HPOE**	**Summit X460-24P**	**3560G-24PS**
PARAMETROS FISICOS			
Descripción Física	20 x 10/100/1000BaseT RJ-45 + 4 x GE SFP, 2 x 10GE XFP (Opcional)	24 puertos 10/100/1000 Base-T y 4 combo puertos 100/1000 Base-X , 4 puertos 100/1000 Base-X dedicados, 2 puertos 10G SFP+ (Modulo opcional)	24 x 10/100/1000BaseT, 4 x SFP, 2 puertos 10G SFP+
H/W/D	1.73" x 17.5" x 19.6"	1.73" x 17.4" x 17."	1.73" x 17.4" x 16.1"
Unidades de Rack (RUs)	1	1	1
OPCIONES DE ENERGIA			
AC y DC Opciones	Si	Si	Si
Redundante y Removible	Si	Si, internal	External Redundancy
Consumo Total de energía	624: 509 W	481 W, 1650 BTU/hr por PSU 962 W, 3284 BTU/hr (dual PSU)	3560G-24PS: 540 W
PoE Opción	Si	Si	Si
Redundancia para PoE	n/a	Si	External Redundancy
EQUIPAMIENTO			
10/100/1000BaseT Puertos por Switch	20	24	24, 48
Class 3 PoE puertos por Switch	20	24	24, 48
SFP Puertos por Switch	4	8	4
10GbE Port Density por Switch	2	2	2
Stacking Puertos	Si	Si	No
Max Número de switches in Stack	8	8	4
PORFORMANCE			
Backplane Capacity/ Switching porfomance	152 Gbps	176 Gbps	32 Gbps
L2 Throughput (Mpps)	624: 114 Mpps	130.9 Mpps	38.7 Mpps
SDRAM	128 MB	1 GB DRAM	128 MB
PHYSICAL LAYER			
Physical Port Redudancy	UDLD	ELRP	UDLD, TDR, FlexLinks
Auto MDI/MDIX	Si	Si	Si
LAYER 2 SWITCHING			
max. Numero de MAC Addresses por Switch	32K	32K	12K
Jumbo Frames	Si	Si	Si
LLDP	Si	Si	No, CDP

VLANS			
Numero deVLANs	4096	4.094	1024
VLAN Criteria	Port-based, Protocol-based	Port-based, Protocol-based yMAC-based	Port-Based
VLAN Tagging	802.1q, Dual Mode, SAV/Q-in-Q	802.1q, Q-in-Q	802.1q, Q-in-Q
VLAN Propagation	GVRP	No	VTP
Private VLANs	Si	Si	Si
Voice VLAN Feature	Si	No	Si
LINK AGGREGATION			
802.3ad	Si	Si	Si
Numero dePuertos por Trunk Group	13 fo GE, 1 fo 10GE	Up to 8	Up to 8
STP			
STP por VLAN	Si	Si, pero con PVST+	Si
STP fast Fowarding	Fast Port, Fast Uplink	Edge safe guard, Type Link, restricted-role	Portfast, Uplink Fast
Rapid-Spanning Tree (802.1w)	Si	Si	Si
MSTP (802.1s)	Si	Si	Si
METRO FEATURES			
MRP / Ring topology	Si	No	No
QinQ / SAV	Si	Q-in-Q	Q-in-Q
VSRP	Si	ESRP	HSRP
Topology Groups	Si	Si	No
MULTICAST			
IGMP	v1, v2, v3	Si	v1, v2, v3
IGMP snooping	Si	Si	Si
IGMPv3 Snooping	Si	Si	Si
Multicast VLAN Registration (MVR)	No	Si	Si
PIM Snooping	Si	Si	No
Multicast Routing PIM, DVMRP?	PIM, DVMRPv2	PIM	PIM, DVMRP
Supoorted PIM Modes	SM, DM, SSM	SM.DM, SSM	Sparse yDense
RATE LIMITING			
ACL- Based Rate Limiting	Si	Si	Si
Stom Control	Unknown Unicast, Broadcast, Multicast	Unknown Unicast, Broadcast, Multicast	Broadcast, Multicast, Unknown Unicast
LAYER 3 FEATURES- IPv4 yIPv6			
Routing Protocols	RIPv1/v2, OSPF, BGP	RIPv1/v2, OSPF, IS-IS, BGP	RIPv1./v2, OSPF, EIGRP, BGP
Max. Routes in IPv4 Fowarding Table	16K	12K	11K
Layer 3 Redundancy	VRRP, VRRPe	VRRP, ESRP	HSRP
Policy Based Routing (PBR)	Si	Si	Si
IPv6 Support?	Mgmt Only	Si	Si
Routing Protocols	RIPng, OSPFv3, IS-IS, BGPv6	RIPng, OSPFv3, IS-IS, BGPv6	RIPng, OSPFv3
QOS			
Hardware Queues por Port	8	8	4
802.1p Honoing & Marking	Si	Si	Si

DSCP/ TOS/ IP Prec Honoing & Marking	Si	Si	Si
Criterio de Clasificación	DSCP/ToS, IP/MAC Source/Dest, Source/Dest TCP/UDP Port#, 802.1p, Port, Ethertype	DSCP/ToS, IP/MAC Source/Dest, Source/Dest TCP/UDP Port#, 802.1p, Port, Ethertype	S/D MAC & IP, TCP/UDP Port
Types of Prioitization	Strict (Prioity) o WRR Queuing o Combo	Stric Prioity yWeighted round robin (SP yWRR)	Strict Prioity & SRR
Rate Limiting / Shaping (BW allocation)	Si	Si	Si
Traffic Shaping	No	Si	Si, SRR & WTD
ADMINISTRABILIDAD			
CLI	Si	Si	Si
WEB Interface	Si	Si	Si
Element Management Tools, Integration in Standard Tools	IronView Netwok Manager (INM)	Ridgeline 3.0	CiscoView
sFlow (RFC 3176)	Si	Si, version 5	No
Traffic Mirroing (Port, VLAN)	Por Port , Por-VLAN	Por Port y vlan	Por-Port, Por-VLAN, RSPAN
SNMP-V3	Si	Si	Si
SEGURIDAD			
Radius / TACACS+	RADIUS / TACACS / TACACS+	RADIUS / TACACS+	Radius / TACACS+
MAC Port Security	Si	Si	Si
Access Control Lists	Si	Si	Si
Ingress & Egress ACL Support?	Ingress Only	Si	Si
Max Numero de ACLs por switch	1024 entries	4,192 ingress y512 egress ACL rules	2000 entries
Netwok Login (802.1x) via Client SW	Si	Si	Si
Dynamic ARP Inspection	Si	Si, similar feature but with different name	Si
DHCP Snooping	Si	Si	Si
DHCP Opcion 82	No	Si	Si
IP Source Guard	No	Si, caracteristicas similar pero con diferente nombre	Si
STP- BPDU Guard	Si	Si, caracteristicas similar pero con diferente nombre	Si
STP- RootGuard	Si	Si, caracteristicas similar pero con diferente nombre	Si
SSH Client + Server	Si, SSH2	Si, SSH2	Si, SSHv2
Secure Copy	Si	Si	No
SSL	Si	Si	Si

Anexo B: Plantilla de configuración

 # Nombre del equipo y ubicación
#==========================
#
configure snmp sysName "SWMODELO-ID"
configure snmp sysLocation "Arequipa;UCSM;UBICACION"
configure snmp syscontact UCSM-Admin

#Configuración de IP administrativa Administracion en banda
#==========================
#La IP Administrativa se configura en la vlan del local comercial (Usuarios_SF o Usuarios_BF o Usuarios_HT)
#
#donde x es el id del switch
configure vlan Mgmt_switches ipaaddress 10.90.0.x/24

#Configuración de IP administrativa Administracion fuera de banda
#==========================
#La IP Administrativa se configura en la vlan del local comercial (Usuarios_SF o Usuarios_BF o Usuarios_HT)
#
#donde x es el id del switch
configure vlan Mgmt ipaddress 10.90.0.x/24

 # Configuración de cuentas locales
#==========================
#
#creacion de cuentas locales con permiso de administrador nivel 15
create account admin netmaster <pass>
#creacion de cuentas locales con permiso de operador nivel 1
create account user netoper <pass>
#borrar cuentas
delete account <nombreusuario>
delete account <nombreusuario>

 # Configuración DNS
#==========================
 # Verificar: "show dns"
#
configure dns-client default-domain ucsm.net.pe

configure dns-client add name-server 192.168.2.8
configure dns-client add name-server 192.168.2.9

 # Sincronización de reloj (SNTP)
#==========================
 # Para verificar: show switch o show sntp
#
config timezone -300 noautods
configure sntp-client update-interval 3600
configure sntp-client primary 10.90.0.6 vr "VR-Default"
enable sntp-client

 # Monitoreo via SNMP
#==========================
#
enable snmp access snmp-v1v2c
enable snmp access snmpv3
enable snmpv3 default-group
enable snmpv3 default-user
configure snmpv3 add community sw_ucsm name sw_ucsm user v1v2c_rw

configure snmpv3 add notify defaultNotify tag defaultNotify
y
configure snmpv3 add community private name private user v1v2c_rw
y
configure snmpv3 add community public name public user v1v2c_ro
y

 # Habilitar el registro de comandos de conf para el SYSLOG
#==========================
#
enable cli-config-logging
enable cpu-monitoring interval 20
configure log target memory-buffer number-of-messages 5000

 # Configuración SYSLOG
#==========================
#
configure syslog add 172.22.7.10:514 vr VR-Default local0
enable log target syslog 172.22.7.10:514 vr VR-Default local0
configure log target syslog 172.22.7.10:514 vr VR-Default local0 filter DefaultFilter severity Debug-Data
configure log target syslog 172.22.7.10:514 vr VR-Default local0 match Any

configure log target syslog 172.22.7.10:514 vr VR-Default local0 format timestamp seconds date Mmm-dd event-name none priority tag-name

 # Configuración ELRP
#====================
#para la verificacion de bucles, los resultados con show log, show elrp
#para verificar: show elrp
#
enable elrp-client
configure elrp-client periodic <nombrevlan> ports all interval 60 log-and-trap disable port permanet

 # Configuración de Autenticación via Radius (Cliente IP Switch: 172.22.X.Y)
#=============================
 # para verificar: show radius / show conf aaa
#
configure radius mgmt-access primary server <IP> 1812 client-ip <IP> vr VR-Default
configure radius mgmt-access primary shared-secret encrypted "<password>"
configure radius mgmt-access secondary server <IP> 1812 client-ip <IP> vr VR-Default
configure radius mgmt-access secondary shared-secret encrypted "<password>"
configure radius-accounting mgmt-access primary server <IP> 1813 client-ip <IP> vr VR-Default
configure radius-accounting mgmt-access primary shared-secret encrypted "<password>"
configure radius-accounting mgmt-access secondary server <IP> 1813 client-ip <IP> vr VR-Default
configure radius-accounting mgmt-access secondary shared-secret encrypted "<password>"
enable radius mgmt-access
enable radius-accounting mgmt-access

 # Administración vía web, ssl y ssh2
#=======================
 # Requisito: Instalar el módulo SSH y habilitar SSL, reiniciar los procesos snmpMaster, thttpd.
#
download image <ip> vr vr-default <nombreimagensshsegunversiondeexos> primary/secondary
y
enable web https

enable ssh2

 # Configuración Spanning tree
#=======================
#
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan <nombrevlan>
#indica los puertos que se van asignar
configure stpd s0 ports link-type edge 1 - 24 edge-safeguard enable
#para la configuracion de rapid stp
configure stpd s0 mode dot1w
enable stpd
enable stpd s0

#Control de Acceso de SNMP y Telnet
#=======================
 # Validar que el servicio TFTP esta activo en el servidor 172.22.7.77
 # Se procede a realizar un TFTP al servidor 172.22.7.77

tftp get 172.22.7.77 vr "VR-Default" acl_telnet.pol

configure snmp access-profile acl_telnet
configure telnet access-profile acl_telnet

Anexo C: Glosario

8

- **802.1d**: Estándar de IEEE para puentes MAC y para impedir la formación de bucles en infraestructuras redundantes.
- **802.1q**: Permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking), utilizado en la implementación de VLANs.
- **802.1p**: Proporciona un mecanismo para asignar calidad de servicio.

A

- **ACL**: Lista de control de acceso.
- **Adaptabilidad**: la facilidad con que un diseño de red puede adaptar fallas, cambiar patrones de tráfico, requerimientos de negocio o técnicos u otros cambios.
- **ADSL**: línea de abonado digital asimétrica, es una de las tecnologías de DSL. provee mayor ancho de banda de bajada que de subida.
- **Agente**: En administración de redes, es el proceso que reside en el dispositivo administrado.
- **Asequibilidad**: Meta del diseño de red que especifica la importancia de los costos en la implementación y diseño de una solución.
- **Área**: Conjunto de redes lógicas segmentadas y sus dispositivos conectados.
- **ATM**: Modo de transferencia asíncrona. Estándar internacional de transmisión.

B

- **Backbone**: La red que conecta que conecta otras redes y se convierte en la ruta primaria entre las dos redes.
- **BGP**: Protocolo de acceso de borde. Es el protocolo de enrutamiento entre dominios en una red.
- **BW**: Ancho de banda.
- **Broadcast**: Mensaje que es enviado a todos los nodos de una red.

C

- **Clasificación**: Específica qué campos de paquetes coinciden con valores específicos. Todos aquellos paquetes que coincidan con las especificaciones definidas por el usuario, se clasifican juntos.
- **Cable coaxial**: Cable de transmisión blindado.
- **Congestión**: La condición en el que el tráfico de red llega o está por llegar a la capacidad máxima.
- **Convergencia**: Velocidad y habilidad en el cual un grupo de dispositivos de red ejecutan un protocolo específico y cuánto tiempo les tomara adaptar un cambio.

D

- **Data store**: Área de la red donde reside la data de la capa de aplicación. Puede ser un servidor, conjunto de servidores, mainframe, tape backup.
- **DHCP**: Protocolo de configuración de host dinámico.
- **DiffServ**: Arquitectura para proporcionar calidad de servicio basándose en la clasificación de tráfico y el marcado de paquetes. ; Propuesta de la IETF que provee diferenciación de los servicios creando clases de servicio con distintas prioridades utilizando el campo Type of Service (TOS) del encabezado IPv4 o el campo Priority del encabezado IPv6.
- **DSCP**: Punto de código de servicios diferenciados.

- **DUT**: Device under testing. Dispositvo bajo pruebas.

E

- **Eficiencia**: La medida de cuanta carga es requerida para producir cierta cantidad de throughput en una red.
- **EIGRP**: Protocolo de enrutamiento creado por Cisco el cual es propietario.
- **Ethernet**: Tecnología LAN inventada por Xerox Corporation. Es similar a IEEE 802.3.

F

- **Fast Ethernet**: velocidad máxima 100 Mbps.
- **Fibra Óptica**: Medio físico capaz no es susceptible a interferencia electromagnética.
- **Firewall**: Router, Switch, software, appliance o servidor designado como buffer entre redes conectadas.
- **FTP**: Protocolo de transferencia de archivos. Es un protocolo de capa 7. RFC959

G

- **Gigabit Ethernet**: Tecnología LAN de velocidad 1000 Mbps especificada en el estándar IEEE 802.3z

H

- **Hub**: En Ethernet e IEEE 802.3 un repetidor multipuerto Ethernet.

I

- **ICMP**: Protocolo de control de mensaje. RFC 792.

- **IEEE**: Instituto de ingenieros eléctricos y electrónicos. Organización profesional la cual sus actividades incluyen el desarrollo de estándares de comunicaciones y de red.
- **IETF**: Grupo de Trabajo en Ingeniería de Internet.
- **IP**: Protocolo de Internet.
- **ISP**: Proveedor de servicios de internet.

J

- **Jitter**: Variación en el retardo de paquetes de un mismo flujo de información.

L

- **LAN**: Red de área local.

M

- **MAC**: Control de acceso al medio.
- **MAN**: Red de área metropolitana.
- **MIB**: Información base de administración.
- **MM**: Management module. Módulo de administración de un equipo.
- **MTU**: Unidad máxima de transmisión.

N

- **NAT**: Protocolo de traducción de direcciones de red. Provee mecanismos para la traducción de direcciones privadas a direcciones enrutables o públicas.

O

- **OSPF**: Open Shortest Path First. Protocolo de enrutamiento de red.

P

- **Policing**: Mecanismo utilizado para modelar el tráfico saliente por descarte de paquetes.
- **pps**: Paquetes por segundo. Una medida de cuan rápido un switch o router pueden reenviar data.
- **Puerto**: Interface de un dispositivo de red como switch, router, appliance.

Q

- **QoS**: Calidad de servicio.

R

- **RADIUS**: Remote authentication dial-in user service. Protocolo y base de datos para la autenticación, autorización y contabilización de usuarios.
- **RFC**: Solicitud de comentarios. Serie de documentos escritos por la IETF como principal medio de información acerca de los protocolos de internet y TCP/IP.
- **RMON**: Administración Remota. Agente MIB desarrollado por la IETF que define las funciones para la administración remota.

S

- **SLA**: Acuerdo de nivel de servicio o Service Level Agreement, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

- **SNMP**: Protocolo simple de administración de red. Protocolo para la administración de red para redes TCP/IP. Provee el monitoreo y control de dispositivos, administrar configuraciones, estadísticas, performance y seguridad.
- **STP**: Protocolo de bridge que utiliza el algoritmo Spanning Tree.
- **Switch**: Dispositivo de red que filtra, reenvía, e inunda frames basada en la dirección MAC de destino de cada frame. Opera en la capa 2.

T

- **TACACS**: Terminal access controller access control system. Protocolo de autenticación que provee autenticación de acceso remoto.
- **TCP**: Protocolo de control de transmisión.
- **Topología**: Disposición lógica de nodos de red mediante una estructura de red.
- **ToS**: Tipo de servicio.
- **Troughtput**: Velocidad y tasa de información que puede manejar un dispositivo de red.

U

- **UDP**: Protocolo de datagrama de usuario.
- **UTP**: Unshielded Twisted Pair. Cable par trenzado no blindado.

V

- **VLAN**: Red de área local virtual, es un método de crear redes lógicamente independientes dentro de una misma red física.
- **VoIP**: Voz sobre redes IP.

W

- **WAN**: Red de área Amplia.
- **Wire speed**: La capacidad máxima teórica de throughput de un sistema de red