UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Diseño e Implementación de un Entorno de Simulación para Pruebas Empresariales en Redes de Datos

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Sotres Cataño Mario

ASESOR(A) DE INFORME

M.I. Tanya Itzel Arteaga Ricci

Ciudad Universitaria, Cd. Mx., 2020

http://casandrasoft.com/diseno-de-redes-de-datos-y-telecomunicaciones/

Introducción

Casi por finalizar mis estudios en la Facultad de Ingeniería, tomé la decisión de comenzar a introducirme al mundo laboral, en el que tuviera la oportunidad de poder aplicar todos los conocimientos que aprendí a lo largo de mi carrera. Quería comenzar a ver los frutos de todo ese esfuerzo y dedicación que tuve a lo largo de varios años.

Considero que ha sido una de las mejores decisiones que he tomado, ya que me permitió poder ver la realidad para la que tanto me estuve preparando y poder comenzar a ejercer mi profesión como Ingeniero en Computación y poner en alto el nombre de la Facultad de Ingeniería

En mi vida profesional me he desempeñado en el campo de las redes de datos principalmente, en donde ingresé como becario a la empresa en la que actualmente me encuentro laborando. Ahí fui adquiriendo las habilidades y conocimientos básicos para ejercer dentro del mundo de las redes. El periodo que estuve como becario fue de 6 meses aproximadamente, para después ascender como Ingeniero Consultor Jr. dentro de la misma empresa. En tal posición he tenido que realizar actividades de consultoría, configuración de equipos, *troubleshooting*, soporte técnico para clientes, coordinación de proyectos, así como tener que seguirme capacitando constantemente con nuevas tecnologías orientadas a las redes de datos. Al mismo tiempo tuve que diseñar, junto con un equipo de trabajo, una topología de red para laboratorio, la cual tiene como objetivo ser utilizada para probar configuraciones e implementación de diseños y poder llevar a cabo proyectos con clientes antes de ser implementadas en la red de producción del mismo, del que hablaré a mayor detalle más adelante.

La empresa en la que laboro fue fundada alrededor del año 2014 por tres socios los cuales, son ex-trabajadores de una de las compañías líderes en el mercado de Telecomunicaciones a nivel mundial que se enfoca en distintas tecnologías como *Routing & Switching* (R & S), telefonía VoIP, *Data Center*, Seguridad, *Wireless*, entre muchas otras más. Los tres socios cuentan con varias de las certificaciones más prestigiosas a nivel de R & S, Seguridad y Proveedores de Servicios, por lo que se cuenta con un nivel bastante alto de conocimiento y expertiz, además de que es *Partner Premier* de la misma compañía de la que migraron. La empresa se dedica especialmente a Consultoría de Redes de Datos hacia empresas de tamaño de todo tipo, ya sean PyMEs o grandes empresas y tiene como característica principal dar servicio y atención al cliente tomando como prioridad su objetivo de negocio.

El giro del negocio se enfoca en ser una empresa que provee y administra soluciones integrales de voz, datos y seguridad enfocados a brindarle a los clientes soluciones y servicios para lograr sus objetivos de negocio, contando con procesos claramente definidos para entregar servicios de calidad de forma consistente para lograr lo que otros no pueden.

Dentro de las actividades que se han hecho con clientes de distintas áreas como instituciones bancarias, proveedores de servicios y corporativos de gran tamaño, se encuentran migraciones de equipos de frontera en centro de datos y dentro del sitio del corporativo, los cuales manejan todo el tráfico del cliente hacia el Internet o redes MPLS, rediseño de la topología que actualmente está funcionando en la red del cliente, pero tiene fallas o no funciona de la mejor manera, solución a problemas de seguridad que afectan de manera parcial o total a la red, servicio de consultoría con proveedores de servicio a nivel internacional así como coordinación de proyectos para realizar a cabo implementaciones.

Uno de los principales objetivos que tiene la empresa, es poder reflejar el nivel de detalle que se tiene en conocimientos cuando se realizan todos los trabajos, así como implementaciones, diseño de topologías y consultorías, lo cual ha llevado a ganarse la confianza de grandes compañías y ser considerados al primer momento para futuros proyectos. Debido al gran desempeño que se ha tenido como *Partner Premier* de la compañía de telecomunicaciones que se mencionó anteriormente, se le ha solicitado a la empresa que dé cursos dentro del área de América Latina y algunas zonas de Estados Unidos y ser parte de eventos importantes para poder darse a conocer y presentar nuevos proyectos en los que se dan distintas soluciones de problemas de seguridad y redes de datos.

Me incorporé a la empresa en julio de 2018 como becario donde estuve un periodo de 6 meses estudiando los conceptos básicos de *Routing & Switching* preparándome para una de las certificaciones principales de *Networking* y apoyando con tareas pequeñas con clientes. Posteriormente ascendí como Ingeniero Consultor Jr. en enero de 2019 hasta la fecha gracias a mi buen desempeño y conocimientos adquiridos y demostrados. En este puesto he realizado actividades de migración de equipos, coordinación de proyectos para implementaciones de nuevos sitios corporativos u oficinas remotas para varios clientes, así como la solución a problemas relacionados con redes de datos.

Al estar en este puesto, se me ha encargado liderar distintos proyectos, así como actividades de migración de equipos, en los que he tenido que estar en contacto con gente del área de tecnologías de la información para poder trabajar en conjunto con los equipos de los clientes, así como el equipo de trabajo con el que colaboro dentro la empresa.

Dado el buen desempeño que he tenido y la confianza que me he ganado por parte de los socios, también se me ha dado la tarea de tener bajo mi cargo a nuevos becarios que ingresan a la empresa, a los que tengo que guíar y dirigir durante su estancia en la empresa para poder incorporarlos a futuros proyectos.

A lo largo de siete meses en los que he laborado como Ingeniero Consultor Jr. he tenido las siguientes responsabilidades:

- Soporte técnico a clientes
- Instalación y configuración de redes de telecomunicaciones
- Capacitación continua

De los proyectos en los cuales estuve participando dentro de la empresa considero tres de ellos como los principales y de los que más he aprendido a lo largo de este tiempo. El primero de ellos fue relacionado con una compañía farmacéutica internacional, en la cual ya había participado mi empresa anteriormente, pero se me pidió que con base en todos sus equipos de telecomunicaciones a nivel nacional, construyera la topología de producción de la misma, así como desglosar los tres sitios que posee a nivel de Capa 2 y Capa 3 del modelo OSI, incluyendo los diversos protocolos de red que se manejan en ambas capas.

El segundo proyecto que considero importante, fue con otra compañía internacional de gran prestigio, que posee una plataforma de movilidad de transporte con la que tuve que participar como coordinador de proyecto debido a que, a lo largo de la República Mexicana,

comenzaron a abrir nuevas sucursales y decidieron estandarizar el equipo de telecomunicaciones que se utilizaría en cada una de las nuevas sedes, por lo que tuve que estar coordinando a los ingenieros de campo para que realizaran las configuraciones pertinentes a los equipos y las demás tareas que solicitaba el cliente.

Por último, el tercer proyecto fue meramente interno en mi empresa, ya que se nos solicitó que diseñáramos e implementáramos una red de laboratorio en el que se pudieran estar realizando pruebas de configuraciones antes de llevarlas a cabo en las redes de producción de los clientes. Considero este último como uno de los más importantes y por lo cual, lo decidí tomar como tema para mi reporte, que expondré a mayor detalle más adelante en el capítulo 1, debido a la complejidad y esfuerzo que demandó, así como el gran aprendizaje que obtuve del mismo.

Al término de los proyectos, adquirí y reforcé ciertas habilidades, como el saber documentar de manera adecuada, aprender a coordinar proyectos de una manera más organizada, liderazgo y llevar a la práctica todos los conceptos y entrenamientos en los que estuve trabajando como becario.

Algo que también tuve que afrontar a lo largo del trabajo junto con mis compañeros con los que participé fue el fracaso, debido a que de vez en cuando nos encontrábamos con algún percance fuera de lo planeado, sin embargo, pude entender que el fracaso no es un motivo para rendirse, sino simplemente es aprendizaje del que vas descubriendo nuevas formas para hacer las cosas, te vas formando un criterio acerca de lo que creías saber o conocer, del gran poder de trabajar en equipo que nos estuvieron inculcando a lo largo de la carrera y de la importancia de levantar la mano cuando necesitas ayuda.

Quiero agradecer a la Facultad de Ingeniería que me ayudó a poder tener muchos de los conocimientos base que me solicitaron en mi trabajo y a la vez, ir haciéndome de las habilidades necesarias para poder alcanzar todos los objetivos que he logrado hasta el momento en el ambiente laboral, ya que, a lo largo de los años en los que estuve como estudiante, tuve que realizar diversas actividades en equipo para poder cumplir con los objetivos de cada materia, los cuales retomé al momento de tener que trabajar con otras personas en las actividades laborales que se me solicitaban pudiendo lograr los objetivos por igual de la mejor manera posible. A su vez, gracias a mi Facultad adquirí habilidades de abstracción que me ayudan para que cuando me encuentro con algún objetivo de dificultad considerable, logro plantearlo de la manera más factible y tener las herramientas necesarias para conseguir el éxito.

https://concepto.de/redes-informaticas/

Objetivo

Dado a que la cantidad de trabajo comenzó a crecer dentro de la empresa, y que cada vez se iban requiriendo entornos para pruebas más sofisticados y robustos, se tornó más

complicado poder tener un laboratorio para cada una de las pruebas que necesitara realizar cada persona encargada en un proyecto.

Debido a que los equipos físicos que se tenían disponibles para laboratorio se debían estar sacando del almacén y colocarlos en algún lugar disponible de trabajo, no habían equipos suficientes para cada persona. Si alguien necesitaba realizar un pequeño laboratorio, tenía que comenzarlo desde cero, es decir, realizar las conexiones físicas y virtuales que requiriera, configuración total o parcial de los equipos a utilizar y actualizado de los mismos. Todo este trabajo llevaba un tiempo considerable que se podía aprovechar de una manera más óptima, por lo que se optó por crear una topología de red de laboratorio para simular una topología empresarial para realizar las diversas configuraciones, diseños e implementaciones en la misma.

Se tenía como objetivo principal, poder tener una topología general y completa, con la que se pudiera trabajar con la mayoría de los proyectos que se comenzaran a tener y poder agilizar los tiempos que antes nos tomaban en poder hacer todos los laboratorios para realizar las pruebas que llegáramos a necesitar. Al tener una topología única para todos los trabajadores, nos permitiría poder estar accediendo de manera remota a los equipos, ya que la topología se conectaría a la red de producción de la empresa y a su vez, nos permitiría poder compartir los mismos equipos para dos o más personas al mismo tiempo, debido a que cada quien podría estar realizando distintas configuraciones sin perjudicar el trabajo de alguien más en el momento, porque estaría todo el equipo en la misma área para trabajar.

Capítulo 1. Proyecto de diseño e implementación de un entorno de simulación para pruebas empresariales en redes de datos

En el siguiente capítulo hablaré del proceso que se siguió para realizar la implementación del laboratorio de pruebas que mencioné anteriormente en la introducción. Comenzaré a explicar acerca de los requerimientos y lineamientos que se tuvieron en consideración al diseñar la

topología de red de laboratorio, así como del proceso de implementación que se llevó a cabo a lo largo del proyecto.

Se considera que al momento de leer el siguiente capítulo, ya se cuentan con los conocimientos básicos de *Routing & Switching* y de redes de datos.

1.1 Análisis de requerimientos

Conforme al aumento de proyectos que se comenzaron a tener en la empresa, se decidió tener una mejor organización a la hora de realizar pruebas de configuraciones en equipos, ya que no se contaba con un espacio oficial de laboratorio en el que se pudiera trabajar. Otro problema que se tenía, era que como todos los equipos se encontraban en el almacén, se perdía tiempo en estar teniendo que sacar todo el equipo que se necesitaba para un solo laboratorio y se tenían que realizar desde cero todas las conexiones físicas y virtuales en los equipos, lo cual tomaba demasiado tiempo en algunas ocasiones, tiempo que se podía utilizar de mejor manera para otras actividades. Al mismo tiempo, se tenía el problema de que si alguien estaba utilizando algún equipo en específico, otra persona no podía utilizarlo al mismo tiempo o tenía complicaciones de poder realizar otras conexiones porque podría repercutir en el trabajo de la persona que estuviera utilizando el equipo antes.

Para poder solucionar todos los inconvenientes que se tenían se optó por crear una topología general que fuera bastante completa y permitiera ahorrar tiempos al momento de realizar pruebas de laboratorio de distintos proyectos. Así mismo, se requería que la red de laboratorio pudiera brindar acceso remoto, por lo que tendría que tener conexión hacia la red de producción, pero sin ocasionar interferencias o afectaciones a la misma y que tuviera la posibilidad de ser escalable a futuro.

Para poder reunir todos los equipos en un espacio común de trabajo, se adquirió un rack para poder instalar todos los equipos físicos (*Switches*, *Routers*, *Firewalls*, Servidores, entre otros) con los que se contaban al momento. También tuvimos que considerar todas las medidas necesarias para poder tener un espacio en el que los equipos pudieran estar prendidos la mayor parte del día, por eso se necesitó asignar un espacio en el que se pudiera mover una persona con bastante facilidad, aire acondicionado para poder tener los equipos funcionando a la temperatura adecuada según las hojas de especificaciones de los equipos, tener actualizados los sistemas operativos de cada uno de los equipos que se tendrían en funcionamiento y material necesario para realizar la instalación y conexiones de todo el equipo.

Se nos solicitó, una vez instalados los equipos, que diseñáramos e implementáramos la topología de laboratorio en la que se pudieran estar realizando pruebas de configuraciones junto con los análisis de soluciones que se pudieran replicar más tarde en las redes de producción de los clientes de cada proyecto que lo llegara a requerir. Para esto, se nos solicitó que la topología a proponer simulara una red de producción, que contara como mínimo con una red de corporativo, dos oficinas remotas y una red *Multiprotocol Label Switching* (MPLS) que las uniera a las tres y que tuvieran conectividad a Internet junto con la posibilidad de poder acceder de manera remota a cada uno de los equipos que fueran considerados para estar en la topología de laboratorio.

1.2 Diseño de la solución

Para cumplir con los requerimientos anteriormente mencionados se propuso la siguiente topología como posible solución que se muestra en la Figura 1.1. Cabe mencionar que los equipos que se ubican dentro del cuadro punteado, son equipos virtualizados que se encuentran instalados dentro de dos servidores Cisco UCS con plataforma VCenter y ESXi 6.0 debido a que se contaba con licencias de éstos y son los que se nos enseñó a usar durante el entrenamiento de becario. El resto de los dispositivos son equipos físicos.

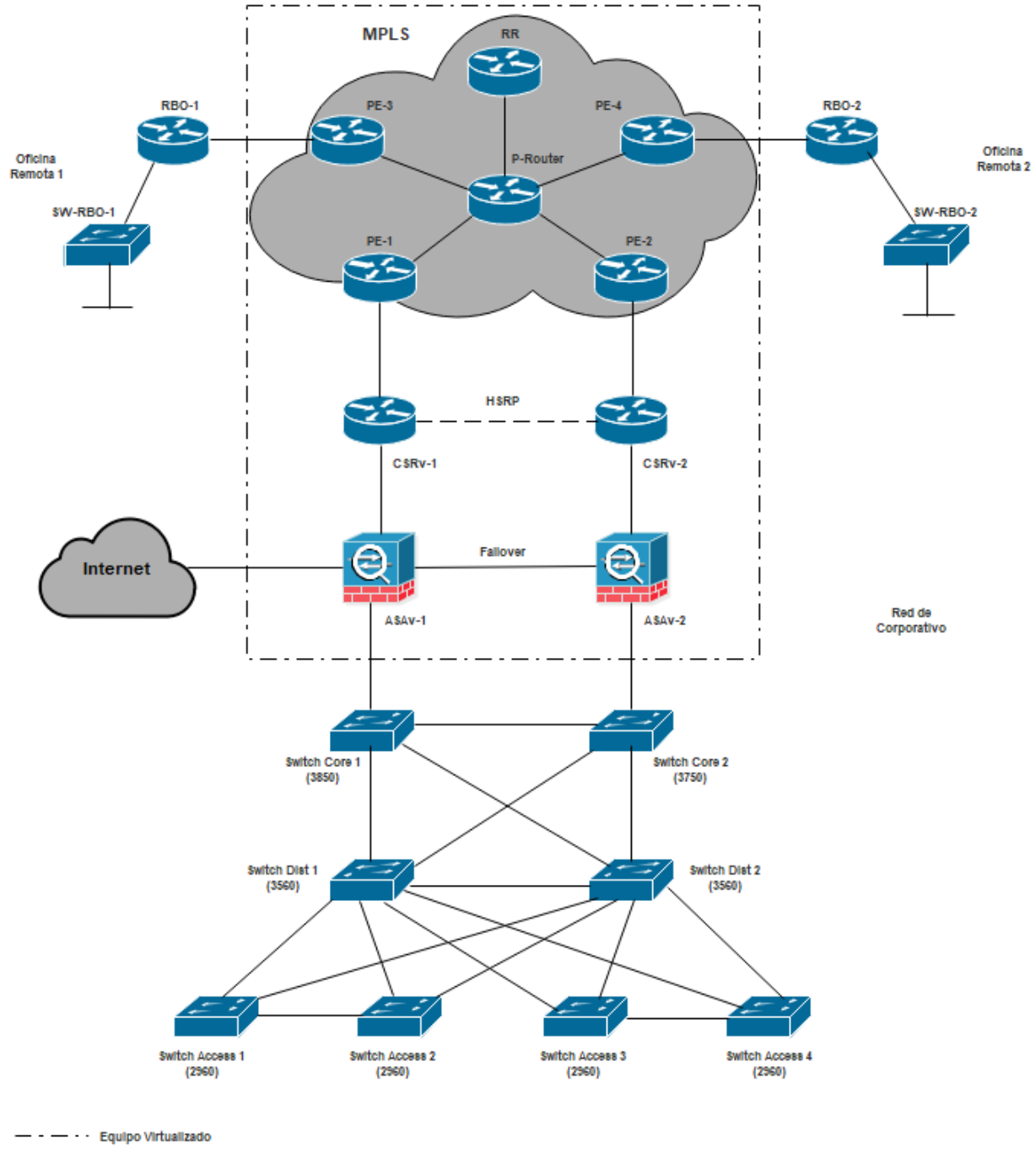


Figura 1.1. Topología de laboratorio propuesta.

Tomando en cuenta los requerimientos, se contempló una red de corporativo con 2 *switches core* y 2 *switches* de distribución para tener redundancia en la red. También se contempló tener 4 *switches* de acceso conectados a ambos *switches* de distribución para tener una topología de tipo malla, permitiendo la comunicación a lo largo de toda la red con distintos caminos de reserva. Los 2 *switches core* estarían conectados a 2 *firewalls* con configuración de *failover*, la cual permite que los dos *firewalls* tengan exactamente la misma configuración y en caso de que el equipo principal falle, el equipo secundario comenzará a trabajar inmediatamente.

En el extremo de la red de corporativo se contempló tener 2 *routers* para tener redundancia y que estuvieran conectados con la red MPLS, que simularía el servicio que brindaría un proveedor de servicios para conectar con oficinas remotas.

Para las oficinas remotas se decidió que sólo tuvieran 1 *router* y 1 *switch* para simular que eran lugares de un tamaño pequeño.

Es importante decir que cuando se llegue a mencionar más adelante alguna capa a nivel de red, se hace referencia al modelo OSI. Para recordarlo rápidamente se muestra a continuación la Figura 1.2 con las capas del modelo mencionado.

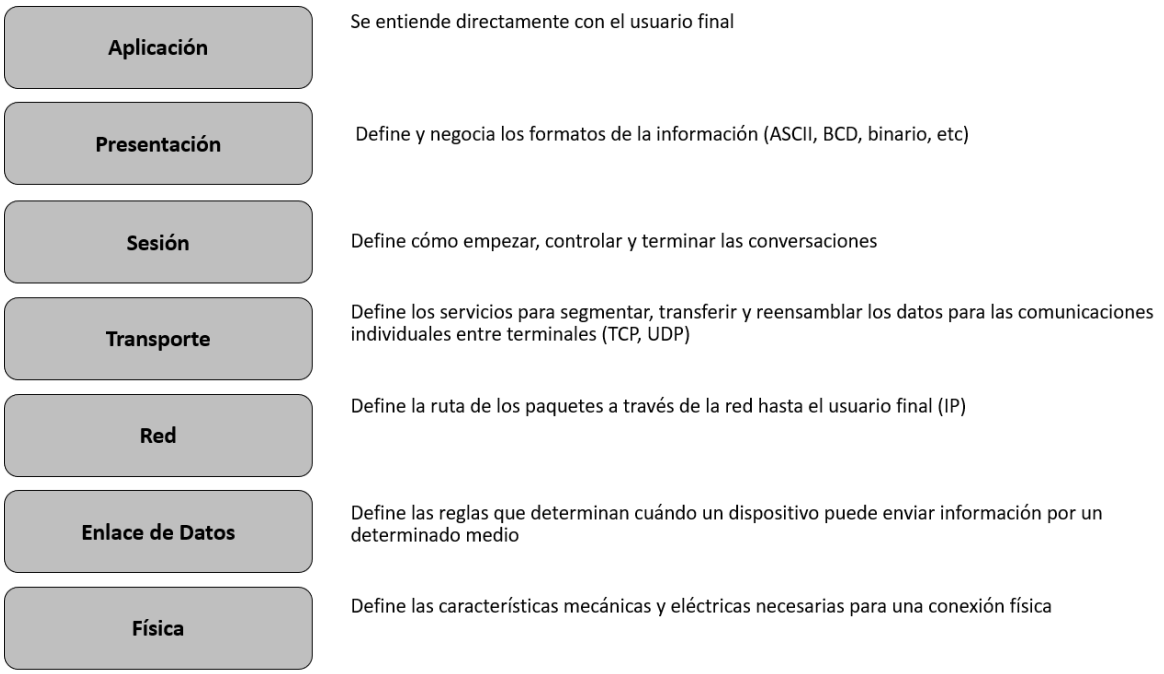


Figura 1.2. Capas del modelo OSI.

1.2.1 Acerca de la topología propuesta

La propuesta de la topología para laboratorio la realicé con ayuda de un experto, que a su vez, era líder del proyecto y nos fue guiando durante el transcurso de éste.

Para cumplir con los requerimientos, realicé un inventario junto con mis compañeros de trabajo para saber los equipos que se tenían disponibles para el laboratorio con sus

respectivas versiones de sistema operativo y modelo para ver qué equipos se utilizarían en la topología y en qué lugar se instalaría cada uno de ellos. Una vez terminado el inventario actualizamos todos los equipos con sistema operativo obsoleto por la versión recomendada por el proveedor y posteriormente se montaron en el rack.

Posteriormente se realizaron las conexiones necesarias entre cada equipo junto con las direcciones IPs internas, que permitirían acceder remotamente a cada equipo para realizar las configuraciones posteriores.

Para el diseño de la topología siempre mantuvimos como prioridad tener redundancia en la red siguiendo las buenas prácticas que ofrece Cisco (ver Anexo B), para que en caso de que uno de los equipos llegase a fallar no sufriéramos de interrupción del servicio.

La red de laboratorio, logra simular una red de producción de una empresa de gran escala, que cuenta con un corporativo y dos sucursales remotas pequeñas. Al mismo tiempo, comunica las tres sucursales por medio de una red MPLS que simula un servicio que arrendaría con algún proveedor de servicios como normalmente sucedería.

Para que la red de laboratorio pudiera tener acceso a Internet, se tuvo que conectar a la red de producción utilizando segmentos de red totalmente distintos para que no impactara en ningún aspecto y al mismo tiempo se hizo uso de la funcionalidad VRF de los *routers*, que se explica más adelante en el capítulo *1* en el apartado 1.*3 Implementación de la topología*, para hacer posible que la topología de laboratorio no aprendiera ningún segmento de red de producción y viceversa.

1.2.2 Diseño de red de corporativo

Para la red de corporativo, decidimos tomar como base las tres capas que se recomienda tener en una topología para tener una distribución de tráfico de datos adecuada a nivel de capa 2 del modelo OSI (Figura 1.2), las cuales son Núcleo (*Core*), Distribución y Acceso.

Con el inventario que realizamos decidimos tomar los equipos con mejor rendimiento como *Core*, que fueron los switches 3850, que se muestra un ejemplo en la Figura 1.3 y 3750, que muestra un ejemplo la Figura 1.4. Estos dos switches fueron elegidos como Core 1 y Core 2 respectivamente. Los dos equipos se consideraron con mejor rendimiento debido a que eran los más recientes que se tenían, las velocidades de transmisión eran mayores (1 Gbps) a comparación de los demás switches que manejan velocidades de 100 Mbps. Al mismo tiempo, estos dos *switches*, tienen posibilidad de aceptar configuraciones a nivel de capa 3. A continuación se muestran las imágenes del modelo de ambos switches.

Figura 1.3. *Switch* Cisco 3850 de 48 puertos.

Fuente: (Cisco, s.f.)Cisco. (n.d.). *Cisco.com*. Retrieved from Cisco.com: https://www.cisco.com/c/es_mx/support/switches/catalyst-3850-48p-e-switch/model.html

Figura 1.4. *Switch* Cisco 3750 de 24 puertos.
Fuente: (Cisco, Cisco.com, s.f.)Cisco. (n.d.). *Cisco.com*. Retrieved from Cisco.com: https://www.cisco.com/c/es_mx/support/switches/catalyst-3750g-24ps-switch/model.html

En la capa de distribución tomamos los equipos con rendimiento medio a nuestro criterio (velocidad de transferencia soportada, características de capa 2 y capa 3, entre otras) que fueron los switches 3560 (Figura 1.5) y por último en la capa de acceso se escogieron los switches 2960 (Figura 1.6).

Figura 1.5. *Switch* Cisco 3560 de 48 puertos.
Fuente: (Cisco, Cisco.com, s.f.)Cisco. (n.d.). *Cisco.com*. Retrieved from Cisco.com: https://www.cisco.com/c/es_mx/support/switches/catalyst-3560-series-switches/tsd-products-support-series-home.html?dtid=osscdc000315

Figura 1.6. *Switch* Cisco 2960 de 24 puertos.
Fuente: (Cisco, Cisco.com, s.f.)Cisco. (n.d.). *Cisco.com*. Retrieved from Cisco.com: https://www.cisco.com/c/es_mx/support/switches/catalyst-2960-48tc-l-switch/model.html?dtid=osscdc000315

Cabe mencionar que los equipos de las dos primeras capas (*Core* y Distribución) cuentan con capacidad de configuraciones a nivel capa 3.

Como se pudo apreciar en la Figura 1.1, las tres capas cuentan con redundancia entre los *switches* para cumplir con nuestra mayor prioridad, la cual es, que la red tenga completo funcionamiento incluso si llega a fallar uno de los *switches Core* o de distribución. Para cumplir de una manera más amplia este requisito, configuramos en los enlaces de las primeras dos capas *Port-Channels* de dos enlaces cada uno para hacer más robusta la redundancia. Estas configuraciones se explicarán a mayor detalle más adelante en el capítulo 1 en el apartado 1.3.1 *Implementación de red de corporativo a nivel de capa 2.*

A nivel de capa 3 propusimos la implementación de dos *Firewalls* (ASAv) y dos *Routers* (CSRv). Estos equipos los virtualizamos debido a la falta de equipo físico para laboratorio,

por lo que decidimos instalarlos en los dos servidores UCS que teníamos, implementando uno de cada tipo en cada servidor. Propusimos los ASAv con conectividad hacia los dos *switch core* que se mencionaron anteriormente, ya que servirían para crear políticas de seguridad a futuro para proteger la red de corporativo y realizar configuraciones que se llegasen a requerir con los clientes, así como *Firewalls* de salida hacia la red MPLS e Internet. Como los dos ASAv contaban con la posibilidad de hacer *Failover* entre ellos, que es una característica que permite simular los dos *Firewall* como uno solo con configuraciones idénticas, situando uno como el primario y el otro como secundario, para que en caso de que el primario llegue a fallar el secundario tome su lugar casi instantáneamente con la misma configuración sin afectar la red, decidimos aprovechar esta característica de los equipos para nuestra red de corporativo. Al mismo tiempo conectamos, para obtener redundancia, los dos ASAv con los dos *routers* CSRv por medio del protocolo de ruteo OSPF[1], igualmente virtualizados, que nos proporcionarían conexión hacia la red MPLS teniendo como rol el de r*outer Customer Edge* (CE) por medio del protocolo de ruteo BGP[2], y por lo tanto, brindarían conexión al mismo tiempo hacia las oficinas remotas. Elegimos OSPF como protocolo para usar por el MPLS, debido a que es un protocolo estándar y era sencillo de implementar para nuestro nivel de conocimiento técnico. En el caso de ruteo externo, BGP es la opción más conocida y más utilizada, por lo que implementamos este protocolo en nuestra topología.
Retomando de nuevo la redundancia en nuestra red, se propuso configurar entre los dos *routers* CSRv HSRP[3], por ser un protocolo de propiedad del fabricante del que usamos los equipos, así como para tener un *router* como primario y otro como secundario para no perder conectividad hacia las redes remotas o la red MPLS.

1.2.3 Diseño de red MPLS

Para el diseño de la red MPLS contemplamos dos protocolos de ruteo, OSPF y BGP. OSPF sería usado para el ruteo interno permitiendo a los *routers* que formasen el MPLS comunicarse entre sí y BGP para comunicar las redes remotas entre sí como se muestra en la Figura 1.7 a continuación:

[1] **Open Shortest Path First (OSPF)** es un protocolo de salida interno que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo.
[2] **Border Gateway Protocol (BGP)** es un protocolo de salida exterior que permite que intercambien información de ruteo entre sí los Sistemas Autónomos.
[3] **Hot Standby Router Protocol (HSRP)**. Protocolo propiedad de Cisco que permite tener routers redundantes tolerante a fallos en una red.

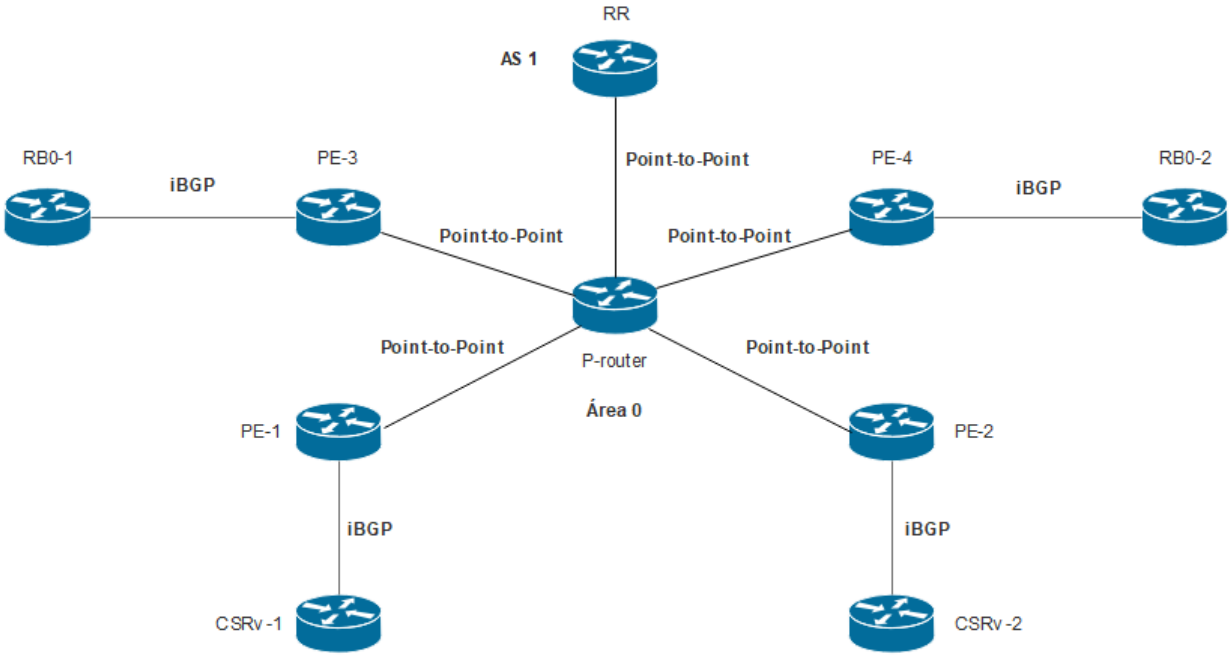


Figura 1.7. Diseño MPLS.

Decidimos utilizar seis *routers* para el MPLS, cuatro de ellos como *Provider Edge Router* (PE) que estarían conectados directamente hacia un *router* que conecta con una red remota o la red de corporativo, para ésta última contemplamos dos *routers* debido a la redundancia que ya explicamos en los capítulos anteriores. A su vez, el quinto *router* funcionaría como *Provider Router* (P-router), el cual funciona como *router* de tránsito en el núcleo de la red y debe de estar conectado a uno o más PE, que en este caso estaría conectado a PE-1, PE-2, PE-3 y PE-4 con tipo de topología *Point-to-Point* utilizando OSPF. Cabe mencionar que el P-router sólo tiene conocimiento de los segmentos de red internos, permitiendo a los PE saber la ruta para llegar al segmento de red que necesitan. Consideramos utilizar el área 0 en OSPF para todos los *routers* por simplicidad y debido a que el número de éstos es considerablemente bajo . Simulando el MPLS también elegimos utilizar un VRF para que nos ayudara a separar el tráfico de los segmentos pertenecientes a nuestra red de cualquier otra que decidiéramos poner, esto para simular un proveedor de servicios que contiene múltiples segmentos de red de varias compañías y necesita hacer privados esos segmentos.

En el caso de BGP utilizamos un *Route Reflector* (RR), el cual funciona como si fuera un *Designated Router* (DR) en OSPF, es decir, va a ser el encargado de indicarle a cada PE cómo llegar a los segmentos de cada red remota por medio de BGP con sistema autónomo (AS) 1 y a su vez, éste estar conectado mediante OSPF al P-router igualmente por área 0 con tipo *Point-to-Point.*

1.2.4 Diseño de oficinas remotas

Para las oficinas remotas decidimos hacer un modelo muy sencillo simulando oficinas remotas pequeñas que consistieran únicamente de un *router* (Cisco *router* 2811, el cual se puede ver en la Figura 1.8) y un *switch* (Cisco Catalyst 2960, que muestra un ejemplo la Figura 1.6) que les otorgara salida a Internet y comunicación hacia la otra red remota junto

con la red de corporativo. Debido a la poca cantidad de equipos requeridos para realizar este diseño, utilizamos solamente equipo físico con el que contábamos en el laboratorio.

Figura 1.8. *Router* Cisco 2811. (Cisco, Cisco.com, s.f.)Cisco. (n.d.). Cisco.com. Retrieved from Cisco.com: https://www.cisco.com/c/en/us/obsolete/routers/cisco-2811-integrated-services-router.html

Para tener conectividad con las demás redes, conectamos ambos *routers* por medio del protocolo de ruteo BGP hacia PE-3 en el caso de la oficina remota 1 (RBO-1) y hacia PE-4 para la oficina remota 2 (RBO-2), esto nos permitiría poder conocer los segmentos de corporativo y la otra oficina remota. Al mismo tiempo, podríamos dar a conocer a los demás sitios los segmentos de red internos que se utilizan en cada oficina remota.

En el caso de los segmentos internos de cada oficina remota, se configuró *router-on-stick* en cada *router* en la interfaz que conecta con el *switch* físico, la cual es una característica que permite configurar varias interfaces virtuales en una sola interfaz física, esto permite que solamente sea necesaria una conexión física para poder hacer el ruteo de distintos segmentos de red en la misma interfaz.

1.3 Implementación de la topología

Teniendo autorizado nuestro diseño para la topología de laboratorio comenzamos a colocar los equipos activos en el rack para posteriormente comenzar con el cableado estructurado necesario para comunicar entre sí los equipos conforme a nuestro diseño. Es importante mencionar que para la administración de los equipos se decidió colocar un *switch* aparte, que tendría conexión hacia todos los equipos físicos y a los servidores en donde se encontrarían los equipos virtualizados y que a la vez está conectado a la red de producción, lo que hace posible que alcancemos a los equipos de laboratorio y éstos tengan salida hacia Internet. Para la administración de los equipos utilizamos el segmento 10.11.0.0/24 y creamos un VRF para que no hubiera problemas con la red de producción al hacer que todo el tráfico de la red de laboratorio no fuera visible por la red de producción y viceversa.

1.3.1 Implementación red de corporativo a nivel capa 2

Como primer paso para la implementación comenzamos construyendo la red de corporativo a nivel de capa 2. Para esto conectamos los *switches core* junto con los *switches* de distribución como se muestra en la figura 1.9 mediante *Port-channels* con dos enlaces cada uno de ellos. Debido a que no se sabía en ese momento qué VLANs serían utilizadas en futuros laboratorios, decidimos dejar los enlaces como troncales (*trunk*) para que dejase pasar todas las VLANs que se encuentren configuradas en los *switches*. Al igual que en los *Port-channels*, los enlaces que conectan a los *switches* de acceso con los de distribución, se les

configuró como enlaces de tipo *trunk*, pero a éstos últimos no se les configuró como *Port-channels* debido a que, como son de nivel de acceso, no hay problema crítico en caso de que uno de los enlaces hacia un *switch* se caiga, porque existe redundancia hacia ambos *switches* de distribución y no necesitan de gran ancho de banda porque no requieren tanto flujo de tráfico como las capas superiores, como es el caso de los *switches core*, que al igual conectan con los dos servidores en los que se encuentran los equipos virtualizados.

A nivel de configuración de VLANs se dejó como VLAN nativa la que viene por defecto en los equipos del proveedor, que en este caso es la VLAN 1 y también decidimos utilizar *Rapid Per-Vlan Spanning-Tree* (RPVSTP) que nos permitió elegir el *switch root* para cada VLAN utilizada en los equipos acorde a futuras necesidades de configuraciones. Al mismo tiempo, el protocolo utilizado nos permitiría tener una velocidad de convergencia mayor a la estándar para que, en caso de que se cayera un enlace o un equipo, se vuelva a establecer automáticamente de manera más rápida el servicio de transferencia de tráfico. Para lo anterior, se configuró al *switch Core 1* para que fuera el *root switch* primario y al *switch Core 2* como el *root switch* secundario, por lo cual todo el tráfico de salida pasaría por el *switch Core 1*.

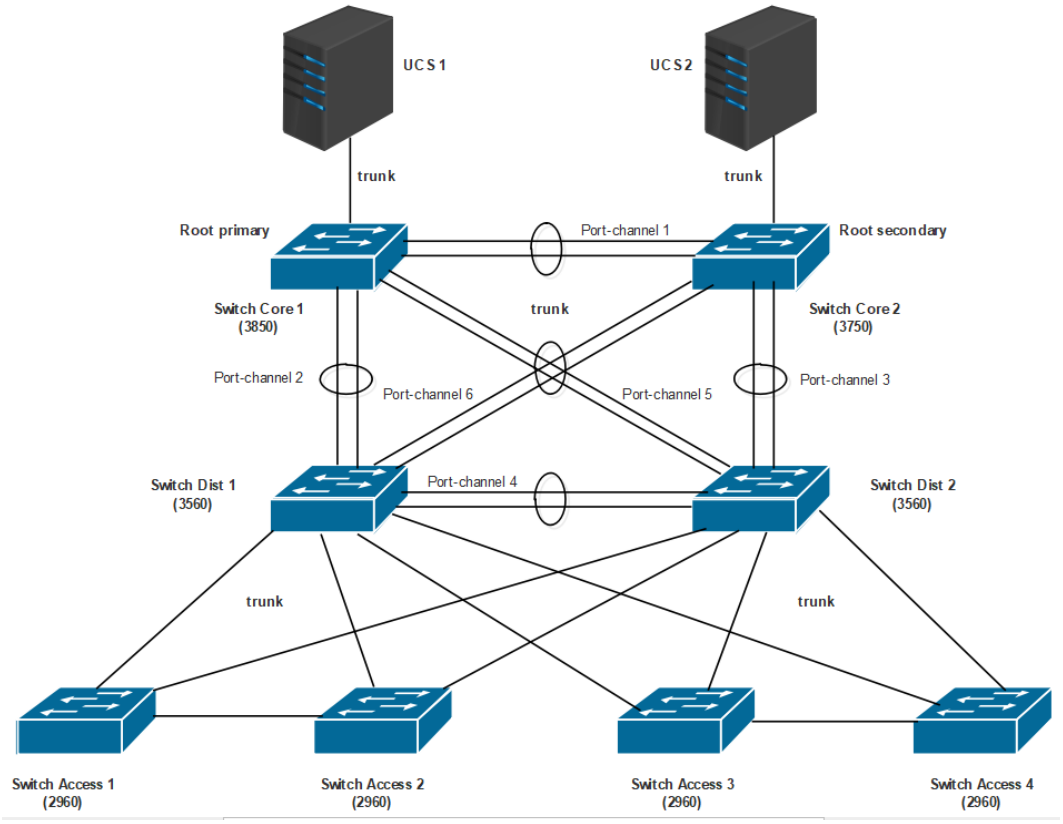


Figura 1.9. Implementación de red de corporativo a nivel de capa 2.

1.3.2 Implementación red de corporativo a nivel capa 3

Para comenzar con la implementación a nivel capa 3 primero tuvimos que configurar ambos servidores con plataforma ESXi y crear en ellos un *switch* virtual que nos permitiese poder

instalar los *firewalls* y *routers* virtuales como si estuvieran conectados físicamente entre sí como se muestra en la Figura 1.10.

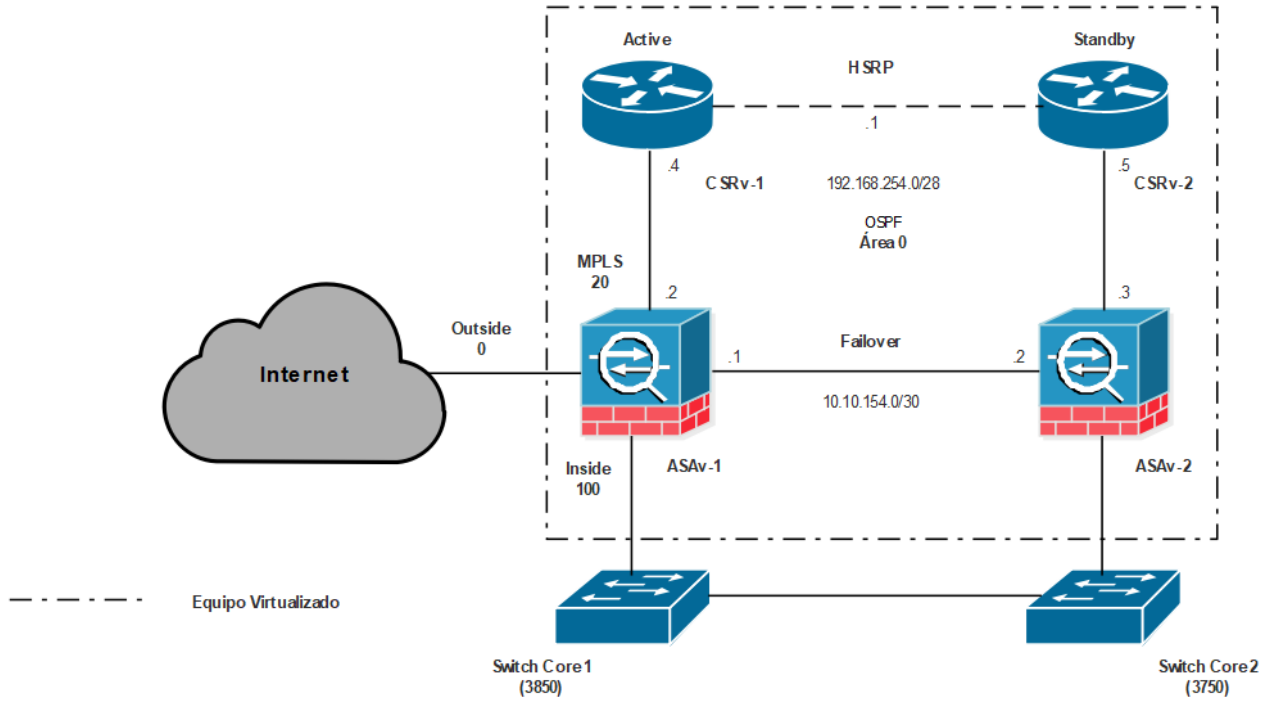


Figura 1.10. Implementación de red de corporativo a nivel de capa 3.

Instalados los *routers* y *firewalls,* realizamos pruebas de comunicación entre ellos para verificar que nuestro *switch* virtual funcionara correctamente. El paso siguiente fue configurar OSPF entre ellos utilizando el área 0 con el segmento de red 192.168.254.0/28. La principal decisión de haber configurado un protocolo de ruteo dinámico entre los equipos, fue para poder propagar las rutas con el MPLS, y por lo tanto, con los sitios remotos. Durante la implementación de OSPF, al mismo tiempo se configuró una interfaz *loopback* en cada equipo orientándolos a que el CSRv-1 estuviera como DR y CSRV-2 como BDR, ésto porque son los equipos que estarían como frontera con el MPLS y por optimización.

Al término de la implementación de enrutamiento dinámico, procedimos a configurar HSRP entre los dos *routers,* dejando como *active* a CSRv-1 y *standby* a CSRv-2 con dirección virtual de 192.168.254.1/28.

Para terminar con la implementación del corporativo a nivel de capa 3, los últimos pasos que realizamos fueron enfocados a los *firewalls* aplicando *failover* como se mencionó en el apartado 1.2.2 y creando tres zonas, las cuales fueron MPLS, *Inside* y *Outside,* como se apreciaron en la figura 1.10 con niveles de seguridad de 20, 100 y 0 respectivamente. Debido a que creamos distintos niveles de seguridad, tuvimos que crear listas de acceso para permitir que la zona de MPLS pudiera comunicarse con nuestra zona interna (*Inside*), es decir, que las oficinas remotas pudieran tener comunicación con la zona de corporativo y viceversa.

Para conectar con Internet, todos los equipos con capacidades de ruteo se configuraron con una ruta por defecto que apuntaba hacia el *firewall* ASAv-1, que después sería conectado

dentro del servidor hacia el *switch* de producción como *gateway* de salida para poder tener acceso a Internet.

1.3.3 Implementación de MPLS

Para la implementación del MPLS, tuvimos que hacernos de conocimientos de mayor nivel, ya que para poder hacer uso de este tipo de tecnología, se tiene que estar familiarizado con ciertos conocimientos de ruteo a mayor detalle. Al mismo tiempo, nuestro líder de proyecto nos dirigió en esta parte debido a la gran experiencia que tiene en el área. Él fue la persona encargada de orientarnos durante la implementación del MPLS tanto en las configuraciones como en el diseño.

Antes de comenzar a instalar los equipos virtuales o realizar configuración alguna, diseñamos el diagrama con direccionamiento lógico que tendría nuestro MPLS, el cual se muestra en la Figura 1.11:

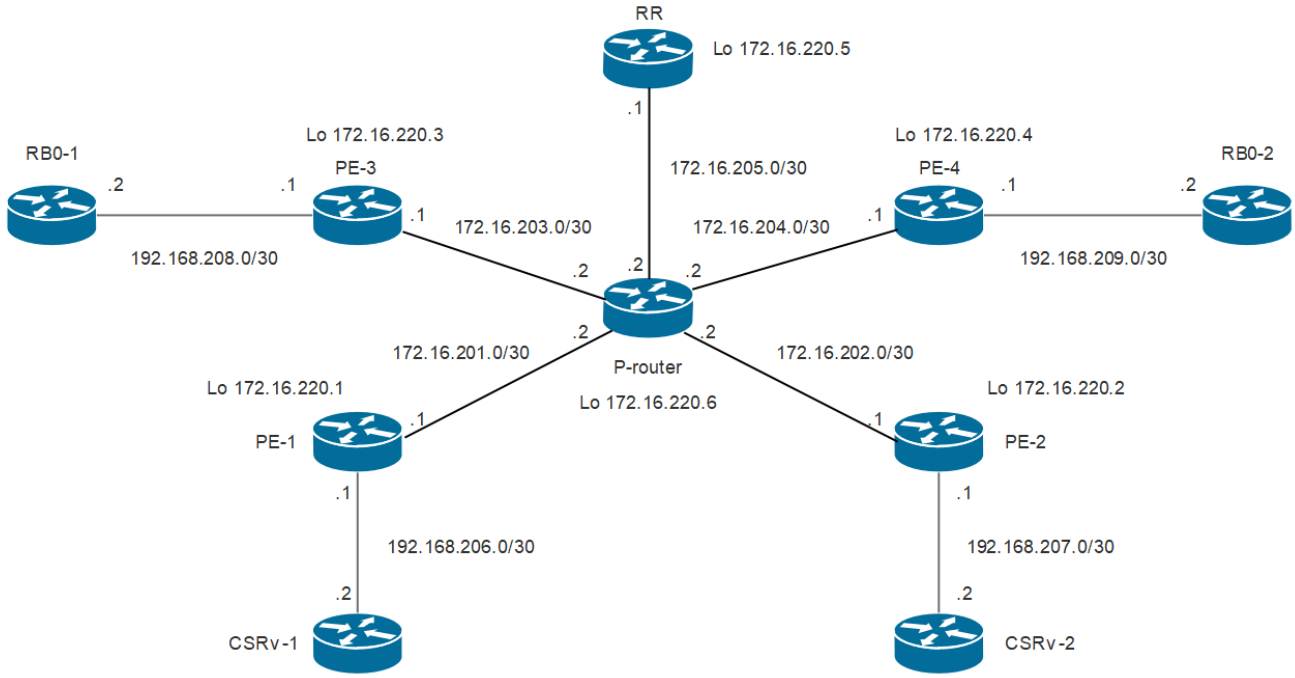


Figura 1.11. Direccionamiento lógico de MPLS.

Como se apreció en la Figura 1.11, se asignaron direcciones *loopback* (Lo) en cada uno de los *routers* pertenecientes al MPLS, esto porque al configurar OSPF más adelante, serían las direcciones que utilizaríamos para formar las adyacencias. Recordando la Figura 1.7, se trata de una topología *Point-to-Point,* por lo que no hay DR ni BDR, todo el tráfico que pase por el MPLS entre cada PE *router* tiene que pasar por el P-router, que es el encargado de dar a conocer los segmentos de cada PE *router*.

Instalados los equipos en el servidor, se realizaron las configuraciones pertinentes para correr OSPF entre P-router, PE-1,2,3 y 4, y RR. Implementado lo anterior, realizamos las pruebas adecuadas para verificar que el funcionamiento fuera el que esperábamos.

Al igual, configuramos VRFs, lo que permite tener distintos segmentos de red sin que se conozcan entre sí, por ejemplo, suponiendo que PE-1 conecta con la compañía X y PE-2 conecta con la compañía Y, ambas compañías pueden tener el segmento privado que se desee y cuando tengan que pasar por el MPLS, que les proporcione algún proveedor de servicios, no sabrían que por el mismo canal pasa la red del otro, ya que no se conocerían porque teniendo un VRF nos permite segmentar/ocultar el tráfico, lo cual es muy utilizado por los proveedores de servicios. En nuestro caso, creamos una VRF incluyendo solamente el segmento de red utilizado por nosotros.

Por último, configuramos BGP para que se conocieran entre sí los sitios remotos y la red de corporativo apuntando cada uno de los *router* frontera de cada sitio a sus respectivos vecinos BGP . Es importante recalcar que el *route reflector (*RR*)* es el encargado de dar a conocer los segmentos BGP de cada sitio, esto quiere decir que cada *router* frontera debe mandar hacia el RR las rutas a conocer para que se propaguen a los otros sitios, imitando el comportamiento de un DR con OSPF, pero utilizando BGP.

1.3.4 Implementación de sitios remotos

Para los dos sitios remotos se consideró una topología del tamaño de una oficina pequeña como se muestra en la Figura 1.12, por lo que sólo se consideró un *router* Cisco 2811 y un *switch* 2960, ambos equipos físicos. El *router* 2811 estaría conectado hacia la red MPLS con las configuraciones con protocolo de ruteo BGP, como se explicó en el apartado 1.3.3, para poder comunicarse entre oficinas remotas y con el corporativo. Como ambos *routers* de las oficinas remotas estarían conectados a los *PE routers*, sólo aprenderían los segmentos que deben de aprender (Oficinas remotas y corporativo).

Como no sabíamos al momento de configurar qué segmentos de red internos se utilizarían en cada sucursal, así como las VLANs que se requerirían, decidimos configurar *router-on-stick* que permite rutear varios segmentos a través de un solo enlace que conecta al *switch* con el *router*. Para esto, se configuró en modo troncal el puerto del *switch* permitiendo pasar las VLANs necesarias o en su defecto, todas, y configurando subinterfaces en el puerto del *router* indicándole qué VLAN pasará por esa subinterfaz y poder rutearla hacia su destino. Esta característica permite poder hacer uso de una sola interfaz física y poder permitir el tráfico entre distintos segmentos de red, para esto se configura en cada subinterfaz una dirección IP perteneciente a cada segmento de red y se utiliza esa misma dirección como el *gateway* para el segmento al que pertenece.

Por último, se le configuró a cada *router* una ruta por defecto apuntando hacia el PE *router* respectivo de cada uno, esto con la finalidad de que todo el tráfico para el que no se le conociera una ruta de salida, como en el caso de querer salir hacia Internet, tendría que pasar por la nube MPLS, la cual llegaría hasta el *firewall* ASAv-1 sin que los *routers* tuvieran conocimiento de todo el proceso interno de la nube MPLS para poder alcanzar el destino.

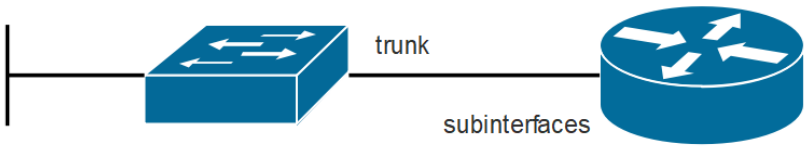


Figura 1.12. Diseño de oficina remota.

http://ascioneluca.ga/galeria-de-fotos

Capítulo 2. Resultados

Para la fase de pruebas tuvimos que ir considerando cada sitio, comenzando con la red de corporativo, que fue la primera que implementamos. En esta etapa nos encontramos con

demasiados problemas con los equipos virtualizados. El primer inconveniente fue que no teníamos un amplio conocimiento en el manejo de la plataforma ESXi, por lo que al momento de tratar de unir los equipos como si estuvieran físicamente conectados a través del *switch* virtual generó problemas, y por lo tanto no se realizaba la conexión correctamente. El segundo problema lo tuvimos con los *routers* virtuales, con ciertos *bugs* que tenían las imágenes del sistema operativo que utilizamos al momento de instalarlos. Éstos no permitían formar la correcta adyacencia con otros equipos al configurar OSPF como se habló en el capítulo 1 en el apartado *1.3.2 Implementación red de corporativo a nivel capa 3.*

Una de las pruebas más importantes, fue la etapa en la que tuvimos que probar que las oficinas remotas se pudieran comunicar entre sí y hacia la red de corporativo a través del MPLS. Al comienzo no logramos hacer que cada *router* frontera conociera los segmentos de otro sitio, por lo que nos pusimos a investigar el correcto funcionamiento que debía tener la red MPLS debido a que nosotros no la configuramos, pero encontramos que el problema era que faltaba un comando dentro de cada PE para que comenzara a propagar los segmentos de red por medio de BGP. Una vez que hicimos lo anterior logramos que los tres sitios pudieran comunicarse entre sí.

Por último, tuvimos que asegurarnos de que todos los dispositivos tuvieran salida hacia Internet, por lo que tuvimos que hacer ciertos ajustes a la red de producción de la empresa para que permitiera el tráfico de nuestro laboratorio, sobretodo del *firewall* ASAv-1, que es hacia donde todos los equipos apuntan para salir hacia Internet.

Constantemente se iba reportando hacia la directiva correspondiente el avance que se iba teniendo, por lo que se establecieron metas semanales que se tenían que ir cumpliendo con cierto grado de prioridad, siempre y cuando no se descuidaran las otras actividades asignadas con los demás proyectos que se llegaran a tener al mismo tiempo.

Al final del laboratorio, la directiva y nuestro líder de proyecto, en este caso el director de Ingeniería de Operaciones, quedaron bastante satisfechos con nuestro trabajo ya que el proyecto se consideró exitoso, aunque se hubiera retrasado un par de meses debido a otras actividades que teníamos y los problemas que mencioné en el apartado anterior, además, se lograron cumplir los objetivos principales, por lo que se pudo comenzar a utilizar prácticamente de inmediato el laboratorio para los clientes con los que se trabajaba al momento.

Poco tiempo después de haber terminado la implementación del laboratorio, pude notar los beneficios que trajo a comparación de la manera de trabajar que se tenía antes. La principal comparación que noté, es que antes todos los equipos que se utilizaban para pruebas como *switches, routers, firewalls, servidores*, etc. tenían que ser sacados del almacén y colocados en cualquier estación de trabajo disponible donde pudieran energizarlos, y una vez que se terminaban de usar tenían que ser regresados. En la actualidad, si uno quiere realizar un laboratorio de pruebas, sólo tiene que conectarse a los equipos vía remota, ya que ya se encuentran instalados y disponibles para su uso, además de contar con conexión hacia Internet y otros dispositivos conectados entre sí por si se requiere su uso también.

https://www.networkworld.es/telecomunicaciones

Conclusiones

A pesar de todos los inconvenientes que tuvimos durante la implementación del laboratorio, que a veces llegaban a detener nuestro avance por varios días, logramos alcanzar los

objetivos que se nos fijaron al inicio. Se logró realizar la implementación del laboratorio con una buena organización, buen trabajo en equipo y sobretodo con un buen desempeño.

También se consiguió aumentar la eficiencia en proyectos posteriores con clientes, ya que permitió crear simulaciones de topologías antes de realizar algún ajuste o implementación en la red de producción de los clientes, así como comenzar a ser proactivos y generar soluciones que fueron ofrecidas durante el primer contacto con varios clientes, por lo que permitió a la empresa tener un mayor crecimiento a partir de la implementación del laboratorio.

Otra de los objetivos que se buscaba al inicio y que se pudo conseguir fue agilizar los tiempos para poder realizar los laboratorios, ya que si una persona necesitaba comenzar algún proyecto que deseaba experimentar en un ambiente controlado primero, ya contaba con los equipos instalados y configurados para sólo llegar y realizar las configuraciones que necesitaba, además de que ya se contaba con un lugar específico y adecuado para trabajar para varias personas y así mismo, tenían acceso a los equipos de manera remota, por lo que sólo tenían que acceder desde su lugar a las direcciones IP de administración de cada equipo y podían comenzar a trabajar con los mismos.

El tener un laboratorio controlado, le ayudó a la empresa a que si surge una nueva tecnología que se necesita o se desea probar, se puede conseguir la imagen virtual para instalar en los servidores UCS y rápidamente comenzar a trabajar con ella y poder ofrecerla a los clientes posteriormente.

Una de las cosas que se adquirieron a su vez, fue que los que participamos en el desarrollo del proyecto, que en su mayoría fuimos de nuevo ingreso, logramos obtener mayor experiencia con los equipos, tanto virtuales como físicos, lo que nos permitió desarrollarnos de una manera más profesional en los proyectos que se nos incluyó tiempo después debido a que los líderes vieron un desempeño considerable en nosotros.

Además, agradezco a la Facultad de Ingeniería por todos los conocimientos que me proporcionó, así como las habilidades que me permitió adquirir para mi desempeño profesional y personal con las que he logrado alcanzar los éxitos que he obtenido en el comienzo de mi vida profesional.

https://www.etcetera.com.mx/opinion/redes-telecomunicaciones-ego-viene-internet/

Bibliografía

Cernick, P., Degner, M., & Kruepke, K. (2000). *Cisco IP Routing Handbook.* Foster City: M&T Books.

Cisco. (10 de Agosto de 2005). *cisco.com*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Cisco. (25 de Mayo de 2006). *cisco.com*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

Cisco. (22 de Enero de 2007). *cisco.com*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/17612-bgp.html

Cisco. (s.f.). *cisco.com*. Obtenido de https://www.cisco.com/c/en/us/products/security/virtual-adaptive-security-appliance-firewall/index.html

Cisco. (s.f.). *cisco.com*. Obtenido de https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/ha_active_standby.html

Collado, E. (4 de Mayo de 2009). *eduangi.org*. Obtenido de https://www.eduangi.org/node424.html

Davila, L. P. (21 de Marzo de 2018). *VRF (Virtual Routing and Forwarding).* Obtenido de https://community.cisco.com/t5/documentos-routing-y-switching/vrf-virtual-routing-and-forwarding/ta-p/3406835

Odom, W. (2016). *Official Cert Guide CCENT/CCNA 100-105.* Indianápolis: Cisco Press.

Odom, W. (2017). *CCNA Routing and Switching 200-105 Official Cert Guide.* Indianápolis: Cisco Press.

https://www.optical.pe/servicios-gestionados/gestion-de-enlaces/

Glosario

AS *Automated System* es el conjunto de *routers* que se encuentran bajo una sola administración técnica.

ASAv *Cisco Adaptive Security Virtual Appliance* es una solución de seguridad de red virtualizada que proporciona cumplimiento de políticas e inspección de amenazas en entornos heterogéneos y de múltiples sitios.

ASCII *American Standard Code for Information Interchange* es un código de caracteres escritos que se basa en el alfabeto latino, idéntico al empleado por el inglés moderno

BCD *Binary Code Decimal* es un estándar para representar números decimales en el sistema binario, en donde cada dígito decimal es codificado con una secuencia de 4 bits.

BDR *Backup Designated Router* con la segunda prioridad más alta en topología *multipoint* OSPF que conserva un respaldo de todas las rutas conocidas por el DR.

BGP *Border Gateway Protocol* es un protocolo de ruteo exterior que permite intercambiar información a los Sistemas Autónomos entre sí.

CE *Customer Edge* es el *router* de frontera que conecta con el *router* de frontera del proveedor de servicios.

CSRv *Cisco Cloud Services Router 1000V Series* ofrece funciones de ruteo, seguridad y gestión de red como servicios de la nube.

Data Center Tecnología enfocada a las locaciones físicas de las organizaciones para almacenar su información y aplicaciones críticas.

DR *Designated Router* con la prioridad más alta en topología multipoint OSPF que contiene las rutas conocidas que comparte con los *routers* en la misma área.

Failover Característica que permite tener redundancia entre *firewalls* ASA al tener un *firewall* activo y otro pasivo. En caso de caer el *firewall* activo, el pasivo tomará su lugar con la misma configuración junto con la dirección IP.

Firewall Dispositivo de seguridad de red que monitorea tráfico de entrada y salida, y decide si permite o bloquea tráfico específico basándose en reglas específicas.

Gateway Puerta de enlace de salida encargada de enrutar el tráfico hacia distintos segmentos de red que no se encuentran dentro del área local.

HSRP *Hot Standby Router Protocol* ofrece redundancia entre *routers* para las redes IP al asegurar que el tráfico de usuarios se recupere de forma inmediata de los errores de primer salto compartiendo una dirección IP y MAC virtuales entre *routers*.

IOS Sistema operativo que es usado por la mayoría de los *routers* y *switches* de Cisco
LAN Red de área local.

MPLS *Multiprotocol Label Switching* es una tecnología WAN usada para crear un servicio basado en IP para clientes, utilizando la red interna del proveedor de servicios reenviando el tráfico con una etiqueta MPLS en lugar de la dirección IP de destino.

Networking Área enfocada a las redes de datos

OSI *Open Systems Interconnection* es un modelo de referencia para los protocolos de comunicación de las redes informáticas.

OSPF *Open Shortest Path First* es un protocolo estándar de ruteo interno que usa bases de datos *link-state* y el algoritmo *Shortest Path First (*SPF*)* para encontrar la mejor ruta hacia las redes conocidas.

Partner Premier Certificación de Cisco que le es otorgada a sus socios de negocio al lograr especializaciones específicas.

PE *Provider Edge Router* conecta con el *router* de frontera del cliente al que le proporciona servicio.

Point-to-Point Conexión uno a uno entre *routers*

Port-Channel Grupo de enlaces ethernet que se comportan como uno solo.

P-router *Provider Router.* En MPLS, se conoce como *P router* al equipo que funciona como *router* de tránsito en el núcleo de la red. Generalmente está conectado a uno o más PE.

PyMES Empresas de tamaño pequeño y mediano.

Root switch En *Spanning-tree* es el *switch* que gana la elección al tener la prioridad más baja, por el que pasará todo el tráfico de las VLAN de los demás *switches*.

Router-on-stick se refiere a la característica de los *routers* Cisco que utilizan enlaces troncales en una sola interfaz ethernet, que a su vez permite rutear las distintas VLANs por que pasan por el mismo enlace.

Routing Área del Networking enfocada en procesos y protocolos de enrutamiento

RPVSTP *Rapid Per-Vlan Spanning-Tree* es un protocolo propietario de Cisco que permite la rápida convergencia y tener un *root switch* para cada VLAN configurada en el *switch*.

RR *Route Reflector* es aquel *router* que está configurado para reenviar actualizaciones a los vecinos a través del mismo sistema autónomo.

Spanning Tree Protocol Protocolo definido por la IEEE con el estándar 802.1D. Permite a los *switches* crear redundancia en la red bloqueando algunos puertos para evitar *loops* infinitos en la misma.

Switching Área del Networking encargada enfocada en el procesamiento, filtrado y reenvío de paquetes.

TCP *Transmission Control Protocol* es un estándar que define cómo se debe establecer y mantener una conexión entre aplicaciones e intercambio de información a través de la red.

Troubleshooting Palabra utilizada para referirse a la solución de problemas

Trunk Enlace que permite el tráfico de dos o más VLANs a través del mismo canal.

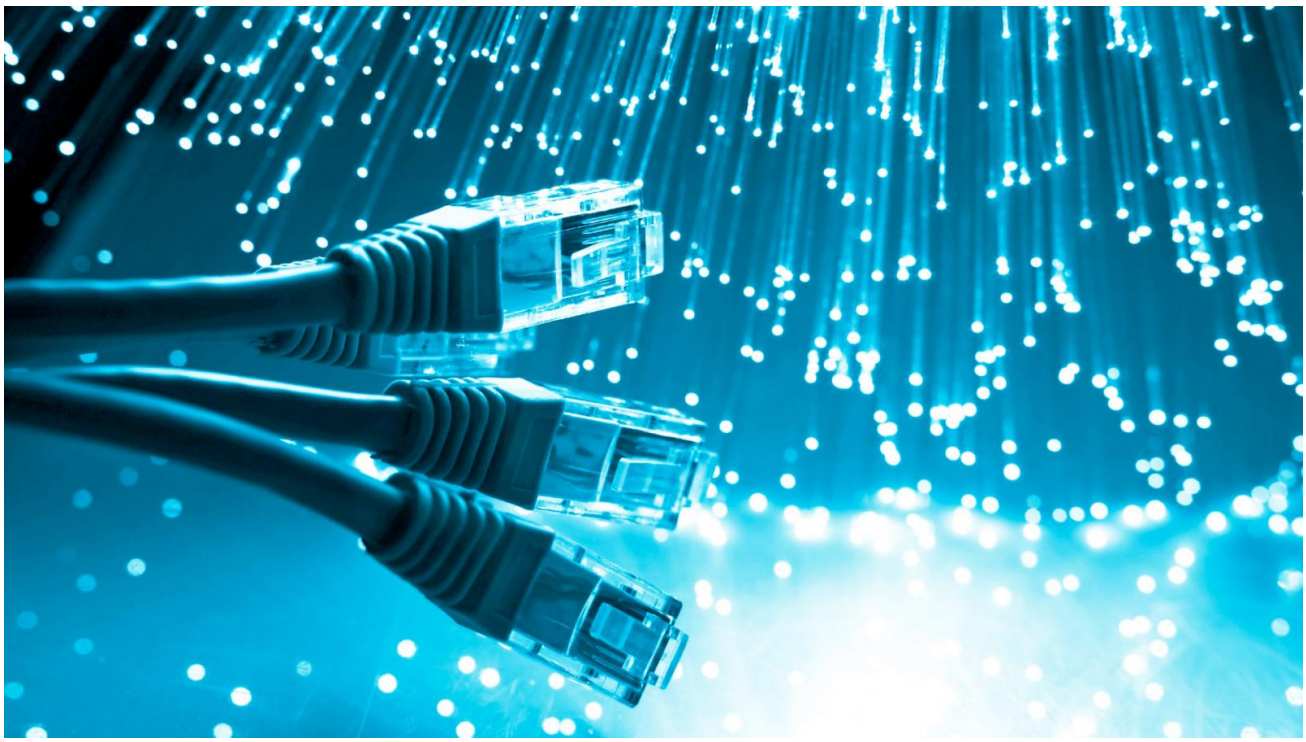
UCS *Cisco Unified Computing System* es un servidor de data center compuesto de hardware, soporte de virtualización, switching y software de administración fabricado por Cisco Systems

UDP *User Datagram Protocol* es un protocolo alternativo a TCP, usado principalmente para establecer conexiones de baja latencia y sin gran importancia y tolerante a pérdidas entre las conexiones realizadas por las aplicaciones.

VLAN *Virtual LAN* es un grupo de dispositivos conectados a uno o más *switches* que están agrupados al mismo dominio *broadcast*

VRF *Virtual Routing and Forwarding* es una funcionalidad que permite a un router tener distintas tablas de enrutamiento totalmente independientes.

Wireless Tecnología enfocada en combinar las redes inalámbricas con las redes alámbricas.



https://www.tic.ir/en/news/17030/Broadband-Commission-for-Sustainable-Development-advances-efforts-to-connect-the-world-s-nearly-four-billion-other-half

Anexo A. Simbología usada en la topología

Router

Equipo que sirve para interconectar distintas redes LAN entre sí o hacia el Internet.

Switch

Equipo para conectar varios dispositivos finales entre sí dentro de una LAN.

ASA

Es una una plataforma que proporciona servicios de seguridad y VPN de próxima generación para entornos de pequeñas, medianas y grandes empresas.

Internet

Conjunto integrado por las diferentes redes de cada país del mundo.

MPLS

Es una tecnología WAN usada para crear un servicio basado en IP para clientes, utilizando la red interna del proveedor de servicios reenviando el tráfico con una etiqueta MPLS en lugar de la dirección IP de destino.

Servidor

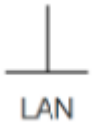
Equipo físico utilizado para almacenar máquinas virtuales que comparten recursos físicos del servidor.

Conexión Ethernet

Conexión física con cable de cobre.

Conexión Virtual

Conexión virtual realizada entre máquinas virtuales que se encuentran funcionando dentro de un servidor.



Conexión demostrativa hacia red LAN.

https://www.neweggbusiness.com/smartbuyer/over-easy/small-office-network-setup/

Anexo B. Buenas prácticas de Cisco para fortalecer los dispositivos Cisco IOS

El siguiente anexo tiene como intención dar un breve resumen de algunas de las buenas prácticas a nivel general que recomienda Cisco para hacer más robusta la configuración de los dispositivos que manejan el sistema operativo IOS. Para mayor información a detalle

acerca de las configuraciones y buenas prácticas que recomienda Cisco se aconseja visitar el siguiente enlace:

https://www.cisco.com/c/es_mx/support/docs/ip/access-lists/13608-21.html

Cisco explica las buenas prácticas que recomienda para fortalecer los dispositivos que corren sistema operativo IOS en los siguientes puntos:

- Operaciones de Seguridad
- Plano de Administración
- Plano de Control
- Plano de Datos

Operaciones de Seguridad

Dentro de este punto, Cisco habla acerca de prácticas como monitoreo de actualizaciones de versiones de sistema operativo, autenticación, protocolos de seguridad, entre otros:

- **Monitoreo de Boletines y Respuestas de Seguridad de Cisco:** Se aconseja revisar constantemente por actualizaciones de los sistemas operativos que manejan los distintos equipos, ya que cada actualización puede solucionar algún problema o vulnerabilidad que ha sido encontrada.

- **Aprovechamiento de Autenticación, Autorización y Contabilización:** Es bastante recomendado utilizar el protocolo AAA para el acceso a los dispositivos y limitar las acciones que pueden realizar las personas que tengan acceso a los mismos.

- **Centralización de Monitoreo y Colección de Registros:** Habla acerca de tener una estrategia para atender incidentes con ayuda de los registros que se tengan dentro de cada equipo, como podría ser el uso de un servidor Syslog para tener registro de todos y cada uno de los equipos dentro de la red.

- **Uso de Protocolos de Seguridad siempre que sea posible:** Se aconseja utilizar protocolos de seguridad tanto para acceder a los equipos utilizando SSH que cifra la información, así como el uso de los protocolos SCP para la transferencia de archivos.

- **Netflow para Visibilidad del Tráfico:** Cisco sugiere el uso del protocolo Netflow para tener una visibilidad completa y en tiempo real del tráfico que pasa a través de uno o más equipos para poder ver el comportamiento de la red y ver si hay alguna anomalía en la misma.

- **Administración de la Configuración:** Se recomienda que antes de realizar cualquier cambio en un equipo que pueda afectar a la red de producción, se haga un plan de trabajo, así como agendar los tiempos que se consideren necesarios para poder realizar cambios en los equipos. De igual manera, hacer un respaldo de configuración por si se tiene que regresar el equipo a los valores que tenía antes de realizado el cambio.

Plano de Administración

En este punto, Cisco detalla las configuraciones y sugerencias que hace para tener una buena, así como una segura administración en todos los equipos. Cisco hace mención de protocolos como SSH, TACACS+, RADIUS, Syslog, SCP, entre otros más.

Cisco detalla las configuraciones que recomienda para fortalecer los accesos remotos a los equipos con el uso de contraseñas, usuarios, listas de control de acceso, uso de puertos específicos relacionados con temas de seguridad. De igual forma, también menciona qué protocolos es bueno tener configurados para poder tener un registro en el que se pueda ver el tiempo exacto en el que ocurrieron cambios, fallas, etc. Se mencionan protocolos como NTP, SNMP, versiones recomendadas de protocolos, etc.

Plano de Control

En el Plano de Control, Cisco detalla las configuraciones que se recomienda llevar a cabo para poder tener un control adecuado y seguro del tráfico de red. Hace énfasis en el protocolo de ruteo BGP, del cual muestra las configuraciones para llevar a cabo autenticaciones entre BGP peers con el uso de MD5, filtrado de prefijos aprendidos como anunciados, listas de control de acceso para proteger comunicaciones entre conexiones establecidas de BGP.

También se dan a conocer configuraciones para limitar la comunicación hacia los equipos con el uso de ICMP, esto para evitar ataques de denegación de servicio.

Plano de Datos

Cisco aconseja limitar el tráfico de datos por donde no se requiera, esto para evitar un alto procesamiento de CPU en los equipos al estar atendiendo mensajes que no son de importancia para los mismos. Para limitar el tráfico, Cisco hace mención del uso de listas de control de acceso, mapeo de rutas, filtrados de tráfico modificando valores de TTL, controles de acceso y el uso de VLANs privadas.