Laboratorio de redes de datos para la experimentación con enrutamiento BGP en redes con enlaces redundantes.

Juan Felipe Hernandez Urrego

Universitaria Agustiniana

Facultad de ingeniería

Ingeniería en telecomunicaciones

Bogotá D.C.

2024

Laboratorio de redes de datos para la experimentación con enrutamiento BGP en redes con enlaces redundantes

Juan Felipe Hernandez Urrego

Director:
Ramiro Osorio Diaz

Trabajo de grado para optar al título de Ingeniero en Telecomunicaciones

Universitaria agustiniana

Facultad de ingeniería

Ingeniería en telecomunicaciones

Bogotá D.C.

2024

Agradecimientos

Agradezco a todo el personal docente de la Universidad Uniagustiniana, que enfatizo sobre mis estudios, éticas y enseñanza como profesional, en especial a los profesores Martha Isabel Villareal López y Ramiro Osorio Diaz.

Y de una manera muy especial al profesor Mauricio Alonso Villalba, el cual tuvo un énfasis de manera personal, de poder idealizarnos que aun sin ser profesionales nos dio la visión y motivación que podíamos desarrollar cualquier tipo de labor profesional, solo es cuestión de disciplina, capacidades y "perrenque ". Así mismo con la profesora Martha Isabel Villareal López, quien me brindo su apoyo en momentos difíciles personales y siempre hizo sentir el grupo de estudiantes como una familia.

A mi querida madre Marinela Urrego Castañeda, mi querida abuela Luz Marina Castañeda, tíos y de manera especial a mi querido padre Geovany Fernando Hernandez que me brindo la oportunidad de cursar mis estudios y el apoyo incondicional.

Así mismo a mis compañeros Mateo Andrés Ramírez, Daniela Guevara y en especial a María Alejandra Covilla quienes me apoyaron en todo momento y circunstancia sobre todo el proceso de la carrera.

Resumen

El laboratorio que se planteó como objetivo genera de redes de datos para la experimentación con enrutamiento BGP en redes con enlaces redundantes, se centra en la propuesta de diseño, práctica y simulación de protocolos de enrutamiento BGP. La importancia de este proyecto se centra en aprender sobre un entorno controlado el funcionamiento de las redes redundantes a nivel empresarial o laboral. También permitirá a estudiantes y profesionales adquirir conocimientos sobre la gestión de equipos de comunicaciones, redes interconectadas y la importancia de los protocolos de enrutamiento para la disponibilidad del servicio empresarial, debido a que el uso de practica con equipos físicos dispone de un costo monetarios, debido al precio de los equipos para poder realizar este tipo de laboratorios. Este proyecto aborda desafíos como el uso inadecuado del protocolo de enrutamiento, mal diseño de topología logia, mal diseño de segmentación de red, la mala interoperabilidad y manejo de la configuración de equipos, así mismo para generar la capacidad de desarrollar cualquier tipo de desafío y que la personal sea capaz de dar una pronta solución.

Palabras clave: BGP, HSRP, enrutamiento, router, switch, topología.

Abstract

The laboratory that was set as the objective of generating data networks for experimentation with BGP routing in networks with redundant links, focuses on the proposal for the design, practice and simulation of BGP routing protocols. The importance of this project focuses on learning in a controlled environment the operation of redundant networks at a business or work level. It will also allow students and professionals to acquire knowledge about the management of communications equipment, interconnected networks and the importance of routing protocols for the availability of the business service, because the use of practice with physical equipment has a monetary cost, due to at the price of the equipment to be able to carry out this type of laboratories. This project addresses challenges such as the inappropriate use of the routing protocol, poor lodge topology design, poor network segmentation design, poor interoperability and management of equipment configuration, as well as to generate the ability to develop any type of challenge and that the staff is capable of providing a prompt solution.

Keywords: BGP, HSRP, routing, router, switch, topology.

Tabla de contenido

1 Introducción

En la actualidad sobre el desarrollo de las redes de telecomunicaciones, la necesidad de las conexiones seguras y constantes se ha convertido el requisito fundamental para la estabilidad y continuidad de las empresas, especial mente en entornos bancarios y transaccionales. La implementación de soluciones de conectividad redundante a nivel físico y lógico ha surgido como una respuesta para esta demanda, destacando y dando solución así con protocolos de enrutamiento dinámico como puede ser BGP, OSPF, MPLS, HSRP dando así garantía y confiabilidad sobre la disponibilidad de las redes de telecomunicaciones.

Sin embargo, la configuración y la implementación de estos protocolos son los siguientes desafíos como, uso no adecuado de protocolo de enrutamiento, mal diseño de la interoperabilidad de la construcción de la malla BGP y otros, por lo cual puede impactar la estabilidad y eficiencia de la red. La complejidad de la gestión y configuración de protocolos puede conducir a errores que afecte el funcionamiento óptimo de las redes empresariales en un entorno interconectado y dependiente de la conectividad continua.

En este contexto este proyecto de grado se enfoca en proponer un diseño, practica y la simulación sobre el protocolo de enrutamiento BGP a redes con enlaces redundantes. Este laboratorio virtual proporcionara un entorno controlado para experimentar y aprender sin riegos permitiendo a los estudiantes y profesionales en un entorno simulado a nivel transaccional o bancario.

La importancia de este proyecto radica en su contribución y conocimiento sobre la gestión de redes de telecomunicaciones interconectadas para tener claridad sobre el funcionamiento o diseño transaccional en un entorno de experimentación segura.

Este laboratorio busca obtener el conocimiento y la importancia de los protocolos de enrutamiento sobre las redes empresarias y proveedores de servicio con el propósito de lograr los objetivos que se enfocan en la importancia y necesidad de las redes intercomunicación para la disponibilidad del servicio empresarial.

2 Planteamiento Del Problema

El desarrollo de redes de conectividad ha producido la manifestación de necesidades de conexiones seguras y constantes. La ausencia de servicios de conectividad puede provocar la caída total de negocios, como el transaccional. Es por lo que se ha desarrollado soluciones de conectividad redundante a nivel físico y lógico.

A nivel lógico, la implementación de protocolos de enrutamiento dinámico como BGP (Border Gateway Protocol) ha surgido como una solución clave para la conectividad redundante. Sin embargo, la configuración a nivel de implementación sobre BGP plantea desafíos como el uso inadecuado del protocolo, el diseño deficiente de la interoperabilidad en la construcción de la malla BGP, mal diseño a nivel de conectividad o topología lógica. Es fundamental abordar de manera efectiva estos desafíos para garantizar el funcionamiento optimo sobre las rede empresariales en un entorno interconectado y dependiente de la conectividad continua.

3 Pregunta De Investigación

¿Cuáles son las consideraciones claves que se deben tener al momento de diseñar y configurar un entorno de laboratorios de simulaciones para enrutamiento BGP con el objetivo de garantizar una disponibilidad?

4 Justificación

La creación de un laboratorio para el enrutamiento BGP en redes con enlaces redundantes se justifica por su importancia en la gestión de redes, la escasez de recursos educativos y la necesidad de práctica. El enrutamiento BGP desempeña un papel fundamental en las redes empresariales y en los proveedores de servicios de Internet con enlaces redundantes, asegurando la disponibilidad continua de la red. Al proporcionar un entorno controlado para experimentar y aprender sin riesgos, este laboratorio ofrece beneficios tanto a estudiantes como a profesionales.

5 Objetivos

5.1 Objetivo principal

Implementar un laboratorio de redes de datos para la experimentación con enrutamiento BGP en redes con enlaces redundantes.

5.2 Objetivos específicos

- Realizar un estudio exhaustivo sobre el desarrollo del protocolo BGP y su aplicación en redes con enlaces redundantes.
- Diseñar un laboratorio de simulación que incluya enrutadores virtuales, enlaces redundantes y nodos de prueba, permitiendo la práctica y experimentación con enrutamiento BGP en redes con enlaces redundantes.
- Desarrollar una guía de estudio completa que sirva como recurso didáctico para el desarrollo de prácticas de laboratorio relacionadas con el enrutamiento BGP en redes con enlaces redundantes.

6 Marcos de referencia

6.1 Estado del arte

Salcedo et al., (2012) hablan sobre los protocolos OSPF-TE y BGP en función de autodescubrimiento para VPN de capa uno sobre GMPLS, comparando los resultados de cada uno sobre su simulación de cada protocolo se evidencio potencia del framework GMPLS para la implementación de redes privadas virtuales garantizando la calidad del servicio y enrutamiento de las redes.

Mediante los resultados se crean las tablas de información de los puertos de cada uno de los PE, para tener el reconocimiento de las VPN, esta distribución informa de manera automática sobre OSPF-TE o BGP, el cual por medio estos protocolos son los seccionados debido a la determinación más adecuada para el autodescubrimiento. (pp.132-133,142-143).

Así mismo, Muguerza, (2014) estudia la migración del acceso a internet de una empresa a un sistema autónomo, realizando su estudio por medio de dos proveedores de internet con un escenario multihoming (muticonexión entre un host o red informática de una red), para realizar la conexión peering BGP con los proveedores.

En su finalidad se realizan pruebas de funcionamiento a nivel de equipos y la implementación de redundancia sobre los enlaces, simulando caídas de la línea y de equipos para saber el comportamiento y disponibilidad de esta cuando suceda un escenario de estos. (pp.1-4,86).

Sin embargo, Cuesta, (2015) realiza el análisis con respeto al Jitter y Delay sobre las redes soportadas en MPLS, BGP y OSPF a nivel del comportamiento de la calidad un video midiendo el comportamiento con cada uno de estos protocolos y enrutamiento por medio del software Wireshark para realizar la medición dB en sus variables.

A demás, realizaron la implementación del proyecto, incluyendo configuraciones de servidores y Router para el seguimiento sobre el rendimiento de la calidad del video, para tener en cuenta donde se puede observar el mejor enrutamiento y disponibilidad hacia el video. (pp.12-16,87-88).

Por otro lado, Choquehuanca, (2016) busca detalladamente el diseño y la implementación de una red privada virtual redundante para una compañía de DELOS!, el cual por medio de los protocolos BGP y GLBP, buscan la mejor disponibilidad debido a su enrutamiento por medio de Vecinos y la superación de limitaciones de los protocolos de Router redundantes existentes adicionando el balanceo de la carga.

Finalmente, gracias al enrutamiento con sus protocolos mejora la disponibilidad del servicio, la seguridad y la transmisión de datos aun así teniendo en cuenta el ancho de banda para la calidad del servicio debido a que el ancho de banda puede llegar a limitar en algún momento la disponibilidad de la red. (pp.15-18,117).

De igual modo, Aguas, (2019) discute la coexistencia de IPv4 con IPv6 sobre el protocolo BGP, asegurando que a medida que pasa el tiempo se está realizando la implementación de la IPv6 a las redes, pero aun así dando por favorito la IPv4 sobre muchas organizaciones a la espera de una buena respuesta o mejoría sobre IPv6, aun así, teniendo alternativas como la NAT, pero confirmando que según las variables a largo plazo IPv6 será necesario para la continuidad, estabilidad y evolución del estudio.

En otras palabras, IPv6 es la mejor solución a futuro debido a que ofrece mayor seguridad, nuevas funciones internas, mejor movilidad sobre los nodos, una implementación eficaz para asegurar el crecimiento de la red y una vida más prolongada a comparación de la IPv4. (pp.12-13,27-28).

A demás, Martínez, (2021) se enfoca sobre el diseño de una Red perimetral de gran escalada, basada sobre el protocolo BGP, el objetivo principal es eliminar la dependencia de los proveedores de telecomunicación y proporcionar una mejor disponibilidad, flexibilidad y continuidad de los servicios.

Dado a esto, se utilizó un sistema autónomo de prefijos IP propios, para une mejor guía sobre el enrutamiento, junto con el protocolo BGP para establecer las sesiones de los proveedor y dar la disponibilidad solicitada teniendo en cuenta que para mejor disponibilidad se debe tener varios proveedores para tener múltiples sesiones de enrutamiento, pero brindando enlaces redundantes y equipos optimizados para reducir gastos conectado por medio de una arquitectura que brinde disponibilidad, residencia y seguridad en los servicios de internet. (pp.2,10-11,114).

A diferencia de, Ignacio et al., (2021) presenta un estudio describiendo la experiencia sobre la implementación de trafico de internet sobre la ciudad de Salta, Argentina, donde se realiza pruebas de transferencia y capacidad sobre la red para invitar a los proveedores locales e instituciones ser parte del intercambio de tráfico sobre la redundancia de la red, realizando una conectividad simultanea entre todo por medio de simulaciones de redes con protocolos relacionales como BGP, OSPF, Entre otros.

Por lo tanto, se realizó las simulaciones por medio del Software GNS3, enfocada a una topología Mixta dando así resultados sobre el intercambio de trafico de redes más rápida y eficiente buscando promover la formación de los recursos humanos, conocimientos técnicos sobre los proveedores y una mejor experiencia para el usuario final. (pp.38-41).

6.2 Marco conceptual

6.2.1 BGP

Según Oracle, (2015) BGP es "(Border Gateway Protocol, puerta de enlace de borde) Un protocolo que intercambia información de enrutamiento entre sistemas autónomos". (p.9).

6.2.2 OSPF

Según Tapasco, (2008) OSPF es " ("Open Shortest Path First"). Es un protocolo de Encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA – Link State Algorithm) para calcular la ruta más corta posible ". (p.9).

6.2.3 VPN

Según Oracle, (2015) VPN es "(virtual prívate network, red privada virtual) Una sola red lógica y segura que emplea túneles en una red pública como Internet". (p.40).

6.2.4 Dirección de datos

Según Oracle, (2015) dirección De Datos es:

> Dirección IP que puede utilizarse como dirección de origen o destino de datos. Las direcciones de datos forman parte de un grupo IPMP y se pueden usar para enviar y recibir tráfico en cualquier interfaz del grupo. Además, el conjunto de direcciones de datos de un grupo IPMP se puede utilizar continuamente siempre que funcione una interfaz en el grupo. (p.13).

6.2.5 Enrutamiento

Según Tapasco, (2008) Enrutamiento es " Es el mecanismo por el cual los paquetes de información viajan desde su origen hasta su destino, siguiendo un camino o ruta a través de la red ". (p.6).

6.2.6 Enrutamiento dinámico

Según Oracle, (2015) Enrutamiento Dinámico es:

> Un tipo de enrutamiento en el que el sistema actualiza automáticamente la tabla de enrutamiento mediante protocolos de enrutamiento, como RIP para redes IPv4 y RIPng para redes IPv6. Es mejor utilizar el enrutamiento dinámico en redes de gran tamaño con muchos hosts. (p.17).

6.2.7 Enrutamiento estático

Según Oracle, (2015) Enrutamiento estático es "Un proceso en el que el administrador de red del sistema puede agregar rutas manualmente a la ruta de enrutamiento". (p.18).

6.2.8 MPLS

Según Tapasco, (2008) MPLS es "(Multiprotocol Label Switching). Tecnología que permite conectividad de todas las sedes de un cliente entre sí y que proporciona mayor eficiencia en las comunicaciones (menos retardo)". (p.8).

6.2.9 VLAN

Según Oracle, (2015) VLAN es "(virtual local área network, red de área local virtual) Una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo". (p.39).

6.2.10 NAT

Según Oracle, (2015) NAT es "(network address translation, traducción de direcciones de red) Traducción de una dirección IP que se utiliza en una red a otra dirección IP conocida en otra red. Se utiliza para limitar la cantidad de direcciones IP globales que se necesitan". (p.26).

6.2.11 DNS

Según Oracle, (2015) DNS es:

> (domain name system, sistema de nombre de dominio) Un servicio que proporciona las directivas y los mecanismos de nomenclatura para la asignación de dominio y los nombres del equipo para direcciones fuera de la empresa, como las de Internet. DNS es el servicio de información de la red utilizado por Internet. (p.15).

6.2.12 Router

Según Incual, (2015) Router es:

> Dispositivo (llamado en inglés) que ayuda a que los paquetes de datos enviados por la red encuentren su destino. En una estructura en red puede tenerse un puerto para la LAN y otro para el encaminador, o bien múltiples puertos para conectar múltiples encaminadores. (p.7).

6.2.13 Switch

Según Cisco, (2012) Switch es:

> Los switches se utilizan para conectar varios dispositivos a través de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad. (p.2).

6.2.14 DHCP

Según Oracle, (2015) DHCP es:

(Dynamic Host Configuration Protocol, protocolo de configuración dinámica de host) Un protocolo que permite la configuración automática de red de los hosts de una red TCP/IP mediante un mecanismo de cliente-servidor. Este protocolo permite que los hosts de una red TCP/IP soliciten y sean asignados direcciones IP, y, además, que detecten información sobre la red a la cual están conectados. (p.13).

6.2.15 ARP

Según Oracle, (2015) ARP es:

(Address Resolution Protocol, protocolo de resolución de direccione) Un protocolo que proporciona asignación dinámica entre las direcciones IP y las direcciones Ethernet. ARP sólo se utiliza con redes IPv4. Las redes IPv6 utilizan el protocolo ND (Neighbor Discovery) para convertir direcciones de protocolo. (p.8).

6.2.16 Jitter

Según Incual, (2015) Jitter es "Cambio indeseado y abrupto de la propiedad de una señal". (p.5).

6.2.17 HSRP

Según CCNA, (2015) HSRP es:

El protocolo HSRP proporciona una alta disponibilidad de red, ya que proporciona redundancia de routing de primer salto para los hosts IPv4 en las redes configuradas con una dirección IPv4 de Gateway predeterminado. HSRP se utiliza en un grupo de routers para seleccionar un dispositivo activo y un dispositivo de reserva. En un grupo de interfaces de dispositivo, el dispositivo activo es aquel que se utiliza para enrutar paquetes, y el dispositivo de reserva es el que toma el control cuando falla el dispositivo activo o cuando se cumplen condiciones previamente establecidas. (p.1).

6.2.18 VRRP

Según (Oracle, 2015) VRRP es "(Virtual Router Redundancy Protocol, protocolo de redundancia de enrutador virtual) Un protocolo que proporciona una alta disponibilidad de direcciones IP, como las que se utilizan para los enrutadores y equilibradores de carga". (p.40).

6.2.19 IPv4

Según Oracle, (2015) IPv4 es "(Internet Protocol, versión 4, protocolo de Internet, versión 4) Una versión del protocolo de Internet que admite un espacio de dirección de 32 bits. IPv4 en ocasiones se denomina simplemente IP". (p.24).

6.2.20 IPv6

Según Oracle, (2015) IPv6 es "(Internet Protocol, versión 6, protocolo de Internet, versión 6) Una versión de protocolo de Internet que admite espacio de direcciones de 128 bits". (p.24).

6.2.21 Dirección MAC

Según Oracle, (2015) Dirección MAC es "(Media Access Control address, dirección de control de acceso a medios) Una dirección exclusiva que se asigna a una interfaz de red. La dirección MAC se utiliza para la comunicación en el segmento de red física". (p.14).

6.2.22 TCP/IP

Según Oracle, (2015) TCP/IP es:

> Una pila de protocolo TCP/IP que permite que los protocolos IPv4 e IPv6 operen en la misma infraestructura de red sin el uso de un mecanismo de colocación en túneles. La red de Oracle Solaris es una pila doble. Esta técnica de pila doble es compatible en hosts y enrutadores. (p.28).

6.2.23 Solicitud de vecino

Según Oracle, (2015) Solicitud de vecino es "Solicitud enviada por un nodo para determinar la dirección de capa de enlace de un vecino. Asimismo, una solicitud de vecino verifica que se pueda contactar con un vecino mediante una dirección de capa de enlace almacenada en caché". (p.37).

6.2.24 Descubrimiento de vecinos

Según Oracle, (2015) Descubrimiento de vecinos es "Mecanismo de IP que permite a los hosts encontrar otros hosts que residen en un enlace conectado". (p.13).

6.2.25 Anuncio de vecinos

Según Oracle, (2015) Anuncio de vecinos es "Respuesta a mensaje de solicitud de vecino o proceso de un nodo que envía anuncios de vecino no solicitados para anunciar un cambio de dirección de capa de enlace". (p.8).

6.2.26 ISP

Según Tapasco, (2008) ISP es " (Proveedor de Servicios de Internet). Es una empresa dedicada en conectar a Internet a los usuarios o a las distintas redes que tengan y dar el mantenimiento necesario para que el acceso funcione correctamente". (p.7).

6.2.27 LAN

Según Rodríguez, (2007) LAN es:

> (Local Área Network): Red de área local que consiste en dos o más nodos, generalmente en un área relativamente pequeña (local). Las estaciones de trabajo de una LAN se conectan con el propósito principal de compartir información y recursos locales. Típicamente, una red casera es una LAN, así como la red de una oficina pequeña o la red de una planta manufacturera. (p.8).

6.2.28 WAN

Según Rodríguez, (2007) WAN es "Red que interconecta dos o más LAN utilizando alguna forma de línea de telecomunicaciones, como las líneas telefónicas o dedicadas de alta velocidad". (p.13).

6.2.29 Paquete

Según Tapasco, (2008) Paquete es "Agrupamiento lógico de Información que incluye un encabezado que contiene información de Control y usualmente datos del usuario.". (p.9).

6.2.30 Gateway

Según Tapasco, (2008) Gateway es "(Puerta de Enlace). Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación, tiene como propósito traducir información del protocolo utilizado en una red al protocolo usado en la red destino". (p.6).

6.2.31 Nodo

Según Tapasco, (2008) Nodo es "Punto final de una conexión en la red o unión común a dos o más líneas en una Red". (p.8).

6.2.32 Mascara de dirección

Según Rodríguez, (2007) Mascara de dirección es "Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se la llama simplemente máscara". (p.9).

6.2.33 Topología

Según Rodríguez, (2007) Topología es "Organización física de la red. De bus, de anillo y de estrella son las topologías más comunes de las redes". (p.12).

6.3 Marco teórico

Sun et al., (2009) presentan un método propuesto mediante un monitoreo en BGP-Update para anomalías en el enrutamiento de Internet. El objetivo principal es validar la tensión de ancho de banda y la congestión de los enlaces, utilizando la estructura de enrutamiento de Internet a nivel de IP desde el dominio de AS para localizar rápidamente anomalías de enrutamiento. También establecen un nuevo marco para la filtración de mensajes de enrutamiento y clasificación de los mensajes de actualizaciones, con el fin de reducir el desperdicio de ancho de banda y espacio de almacenamiento.

Se logra mediante la utilización del protocolo BGP para monitorear las actualizaciones de enrutamiento. Se implementó el software de Traceroute para detectar y obtener información de los enrutamientos. Se utilizó un enfoque de muestreo para reproducir y analizar el historial de actividades de enrutamiento, permitiendo así diagnosticar las anomalías de enrutamiento. (pp.172-173,176).

Por otro lado, Oprescu et al., (2011) presentan un trabajo llamado dVirt, una infraestructura virtualizada distribuida que permite a los operadores de red comprender mejor los mecanismos de enrutamiento BGP y anticipar los comportamientos de la red. Utiliza la virtualización con un software de enrutamiento Quagga para simular redes y cómo pueden ayudar a los operadores de red a comprender y solucionar los problemas relacionados con el enrutamiento BGP.

Se explica que mediante el software crearon infraestructuras virtualizadas distribuidas que emulan la conectividad en capa 2 y simulan de manera precisa el enrutamiento IP y la dinámica del protocolo BGP. En resumen, combinaron la virtualización y el software para crear una herramienta de simulación de red para comprender el comportamiento del enrutamiento BGP. (pp.151-152,154).

En cambio, Musawi, et al., (2016) está basado en analizar el protocolo Border Gateway, que se utiliza para intercambiar información de enrutamiento entre sistemas autónomos de comunicaciones (AS). Los mensajes de BGP incluyen el proceso de abrir, actualizar, notificar y mantener viva la información más importante para utilizar y anunciar nuevas rutas, retirar rutas anunciadas o actualizarlas previamente.

Las políticas de BGP se definen en cómo se toma la decisión del enrutamiento y los AS se interconectan mediante diferentes relaciones, como cliente-proveedor, igual a igual o de vecino a vecino. (pp.377-378).

Sin embargo, Gómez et al., (2017) Buscaban presentar una propuesta ETMP-BGP que utiliza Software-Defined Networking (SDN) para mejorar el enrutamiento interdominio en BGP. Su objetivo era demostrar cómo ETMP-BGP puede mitigar las congestiones a nivel de AS y superar los esquemas de BGP existentes mediante simulaciones.

Para lograrlo, implementaron el enfoque ETMP-BGP que utiliza SDN para mejorar el enrutamiento interdominio en BGP. Utilizando la retroalimentación de las destinaciones para detectar y ajustar las rutas congestionadas a nivel de AS, realizaron simulaciones para evaluar el rendimiento de ETMP-BGP y compararlo con el esquema existente de BGP para así mejorar el enrutamiento en comparación con los enfoques tradicionales. (pp.420-421,425).

A diferencia de Hammood y Musawi. (2021) proponen el uso de algoritmos de selección de características para identificar las anomalías de BGP y mejorar la fiabilidad de Internet. Además, se extraen 55 características de BGP, y se encuentran 9 características clave para identificar fugas de la tabla de enrutamiento y fallos de enlace, sugiriendo mejoras en la seguridad de BGP.

Se logró mediante la extracción de 55 características de BGP y la utilización de algoritmos de selección de características para identificar las anomalías. Encontraron 9 características clave para identificar fugas de la tabla de enrutamiento y fallos de enlace. Los anuncios totales de los prefijos y el número de anuncios de IPv4 son clave para diferenciar fugas de la tabla de enrutamiento. Por otro lado, las características relacionadas con el cambio de origen y AS-PATH, como el anuncio al camino más largo y la distancia de edición, son clave para identificar los fallos de enlace. (pp.1-4).

6.4 Marco legal

La ley 1978 (2019) De la República de Colombia busca como objetivo principal alienar los agentes y autoridades del sector de las tecnologías de la información y las comunicaciones (TIC), para simplificar y modernizar el marco institucional del sector enfocado en la brecha digital y potencializare la vinculación del sector privado en el desarrollo de los proyectos para mejorar la eficiencia en el pago de contraprestaciones y cargas económicas en el sector.

Sobre el articulo 3 el cual habla sobre Prioridad al acceso y uso de la tecnología de la información y telecomunicaciones donde todos loa gentes deberán colaborar y se ven obligados a la priorización de las tecnologías para la producción de bienes y servicio sin discriminatorias hacia la conectividad, sociedad, educación, contenidos y competitividad.

A nivel de promoción de inversión todos los ISP o servicios de telecomunicaciones pueden acceder y hacer uso del espectro y contribuirán al fondo único de tecnologías de la información y las comunicaciones, con la asignación necesaria y adecuada para cada uno de este.

Sobre los accesos a las TIC y despliegue de infraestructura se enfoca en el goce efectivo de los derechos constitucionales a la comunicación, situaciones emergentes, educación, salud, seguridad personal y el acceso libre a la información, entre otras. La nación debe asegurar la prestación oportuna y de calidad sobre los servicios de comunicaciones así mismo con el despliegue de la infraestructura en redes de telecomunicaciones a nivel de servicio de televiso radiodifundida, radiodifusión sonora y entidades territoriales.

El articulo 4 informa sobre la inversión sobre construcción, operación y mantenimiento de infraestructura de tecnología de la información y comunicaciones y así mismo velar por la protección del medio ambiente y salud pública.

A nivel de ISP se habla sobre el articulo 10 el cual habilita de manera general la instalación, ampliación, modificación, operación y explotación de redes para las prestaciones de servicios de telecomunicaciones sea suministradas al público o no el cual este presenta no incluye el derecho al uso del espectro radioeléctrico.

El ministerio de las TIC debe de llevar el registro informático relevante sobre las redes, habilitación, autorización y permisos conforme al reglamente, el cual los ISP deben de inscribirse y quedar bajo el registro de proveedor de redes y servicios de telecomunicaciones con un representante legal. (Arts. 1-7,10-13)

7 Metodología de investigación

El presente proyecto se desarrollará desde un enfoque experimental cuantitativo de la investigación, que se podrá evidenciar en fases como:

- Análisis sobre el enrutamiento BGP aplicado en enlaces redundantes.
- Definición de los requisitos técnicos y recursos necesarios para el desarrollo del laboratorio.
- Selección de las herramientas necesarias para la creación de enlaces, equipos y nodos de prueba.
- Desarrollo de la topología de red, incluyendo la configuración BGP en el laboratorio.
- Simulación de situaciones del mundo real en redes redundantes.
- Registro de datos sobre el rendimiento, la disponibilidad y la configuración de BGP.
- Análisis de los datos recopilados en cada simulación de laboratorio.
- Identificación de problemas y posibles soluciones en la configuración de BGP.
- Recopilación de retroalimentación sobre el desarrollo del laboratorio.
- Presentación de los resultados finales en el informe.

8 Administración del proyecto

8.1 Cronograma

Tabla 1.
Cronograma

		Mes 1				Mes 2				Mes 3				Mes 4			
FASES	Acitividades	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4
FASE 1	Investigación exhaustiva sobre protocolo BGP y su aplicación en redes redundantes																
	Selección de proyectos de investigación																
	Desarrollo objetivo 1 acorde a la selección de proyectos de investigación BGP																
	Validación y aprobación del objetivo con tutor																
FASE 2	Búsqueda de software para la simulación de redes redundantes																
	Diseño de topología lógica de la red																
	Diseño de direccionamiento de los componentes de la topología																
	Instalación de software para la simulación de redes redundantes																
FASE 3	Implementación de topología y direccionamiento sobre el software de simulación																
	Configuración de dispositivos de interconexión en software de simulación																
	Pruebas de funcionamiento sobre la simulación de red																
	Guía para la creación del video sobre la simulación de la red																
FASE 4	Creación del video sobre la simulación de red																
	Diseño guía de estudio para el desarrollo de las practicas																
	Creación de guía de estudio para el desarrollo de las practicas																

Nota: Cronograma realizando para el desarrollo del proyecto. Elaboración propia.

8.2 Presupuesto

En la tabla 1 se realiza una estimación como presupuesto para la realización del proyecto y la que se relaciones los principales conceptos de gasto.

Tabla 2.
Presupuesto trabajo de grado

Descripción	Cantidad por semana	Valor unitario	Valor total
Transporte	10	$2.950	$354.000
Computador	N/a	$3.500.000	$3.500.000
Internet	N/a	$100.000	$100.000
Comida	5	$10.000	$600.000
Licencia Office	N/a	$180.000	$182.000
Total	15	$3.792.950	$4.734.000

Nota: Presupuesto de trabajo de grado para el desarrollo del proyecto. Elaboración propia.

9 Desarrollo del proyecto

9.1 Objetivo 1

En el estudio exhaustivo que se realizó para la solución del primer objetivo (Realizar un estudio exhaustivo sobre el desarrollo del protocolo BGP y su aplicación en redes con enlaces redundantes.), donde se realizó la búsqueda por medio de Google Académico, IEEE Explore y CiteSeer el cual tuvo en cuenta los estudios más relacionados a nivel de protocolo BGP y redundancia como objetivo final del cliente.

Jiménez (2021), habla sobre el diseño e implementación de una arquitectura redundante con fin el fin de implementar un balanceo de carga mediante el protocolo BGP y OSPF para obtener una ruta alterna para la transmisión de los servicios de telecomunicaciones hacia los equipos finales en el DC (Datacenter), su primer desarrollo fue por medio de un equipo Core, el cual realizaba la trasmisión de la información hacia los equipos finales el cual causaba problemas de saturación al dirigir toda la información sobre un equipo de red Core.

Mediante el proceso de solución para el problema de saturación se realiza nuevamente un diseño sobre la topología empleado una VPN y VPLS en la red de transporte para así habitar la interconectividad por una ruta principal y secundar entre otros equipos redundantes mediante el mismo protocolos de BPG y OSPF habilitando el balanceo de la carga entre si mismo, para validar la funcionalidad se realiza una tracert sobre un equipo final cliente para validar la toda la ruta que toma él envió de tráfico. (pp.1,9,53).

En cambio, Bustos. (2016), realizo una implementación de una red MPLS utilizando le método de VRF LITE y monitoreo sobre Observium, con el inicio del desarrollo por medio de un ISP, el cual presta los datos y acceso a internet a la empresa Urbano Expressa nivel nacional, con una red multiprocol label swirching MPLS.

Se desarrolla el proceso de investigación sobre el direccionamiento, enrutamiento topológico ancho de banda, servicios y los equipos que presta como tal el ISP para así proponer un diseño más optima sobre la nueva tecnología de la MPLS.

Al momento de implementación se realizó la estación de un router en paralelo para así no afectar el funcionamiento de la red que se encontraba en operación, con tecnología nueva MPLS con configuración VRF lite, BGP, route-map, prefix-list y redundancia a nivel de UM (Ultima milla), por último, a la final de cada configuración y entrega de enlace, se coloca sobre el Monitor

Observium, permitiendo monitorear el funcionamiento, consumo de ancho de banca y la disponibilidad del enlace. (pp.9,142-143).

En relación de Jiménez (2021); Bustos (2016), su objetividad es el mejoramiento de la disponibilidad de trafico de red y monitoreo sobre este para así mismo brindarles un servicio eficiente a los clientes con relación de las configuraciones como BGP, OSFP, MPLS entre otros.

Por lo tanto, García y Narváez, (2018), buscan el mejoramiento de los enlaces de red sobre un área amplia de empresa con una solución CISCO, analizando los componentes que hace parte de la solución y el funcionamiento correcto.

Esta solución permite utilizar los enlaces redundantes de forma activa-activa simultáneamente para el tráfico de los servicio y administración de red, teniendo en cuenta el rendimiento de esta basa en un monitoreo sobre cada enlace con umbrales definidos sobre rangos necesarios para la disponibilidad el cual, el enlace que no del funcionamiento correcto se desvía el tráfico de este por otro que tenga mejor disponibilidad, adicionalmente se incremente la seguridad en él envió de paquetes entre localidades cifrando todo el tráfico para así disminuir los riesgos con la perdida de integridad, confidencialidad y disponibilidad de la información. (pp.8-10,148-150).

Por otro lado, Quesquén (2019), presentar un diseño de red óptico-inalámbrica para el envío de voz y de datos, a beneficio de que este tipo de red está en constante crecimiento, versatilidad y nivel de funcionamiento ya que opera sobre el medio ambiente sin necesidad de cables o equipos complejos facilitando si configuración.

Las diferentes empresas de lima están en constante crecimiento el cual tiene la necesidad de conectar sus sucursales con su sede principal, generando problema de interconectividad, el cual tienen la necesidad de contar con un sistema que envié información a alta velocidad (Imágenes, documentos, planos, voz, Etc.), sin que genere interferencia electromagnética debido a que se utiliza la comunicación en radio frecuencia y debido a esto presenta una alta sensibilidad a la presencia de la interferencia electromagnética.

Se tuvo pronosticado sobre la investigación los medios de trasmisión de datos como el par trenzado, cable coaxial y fibra ópticas a referente de medios guiados y por medios no guiados como luz laser, multiplexación DWDM que funciona sobre bajo los mismos conceptos de la fibra óptica. (pp.11-12,74).

En conclusión, sobre García y Narváez, (2018); Quesquén (2019), buscan el mejoramiento tanto en medios de transición guiados y no guiados para una alta disponibilidad sobre empresas para

conectar sucursales sobre la principal con relación de monitoreo sobre umbrales de pronóstico y cumplimiento de los enlaces, para así determinar el funcionamiento de estos y descartar aquellos que no cumplan sobre el rango establecido.

Así mismo Castañeda (2018), sobre la empresa Americatel se cuenta con una redundancia de transporte con un punto crítico sobre el router rOlG-MGMT, el cual está ubicado sobre el nodo principal y generando así un alertamiento debido a que si se llega a generar algún incidente sobre este se perderá gestión sobre el nodo.

Por medio del servicio de administración de Router el cual permite la gestión de las redes por medio de sus Vlans como: Red metro, gestores de radio, equipos de energía, entre otras; por ende, se ha tenido incidentes sobre cortes de energía o falla sobre la tarjeta de red el cual provoca la indisponibilidad a los equipos perdiendo el control y monitoreo haciendo necesario la manipulación de estos de forma manual para recuperar la gestión.

La solución de este se enfoca con el uso del router de contingencia, que actualmente está en uso y perteneciente a la red de gestión, con la idea de hacer uso del protocolo HSRP para general el balanceo del tráfico al momento de la caída del Router Principal con el mecanismo de IP SLA, teniendo el desarrollo por un diagnóstico, configuración, monitoreo, y evaluación del esquema de redundancia. (pp.4-5,53-54).

De la misma manera Castillo (2022), trata de la red telemática de UNMSM encargada de proyectar, dirigir y preservar la operatividad de la red de datos y servicios de telecomunicaciones el cual no tiene la infraestructura capaz de soportar fallos de enlaces de datos.

Esta red cuenta con limitaciones y no está preparada para nuevos servicios o ampliación de esta, se propone diseñar una red de alta disponibilidad y redundancia que permita a la universidad Nacional Mayor de San Marcos reducir el gasto del OPEX y disminuir futuras fallas de enlaces.

Con la propuesta del diseño se logra maximizar el tiempo útil de las redes de datos, dando mejor disponibilidad, a nivel de datos, voz, videoconferencia, hosting, alojamiento de servidores, acceso a internet y redes externas con la seguridad de recuperarse sobre cualquier incidente producido a nivel de red de datos. (pp.1,42,45).

En resumen, Castañeda (2018); Castillo (2022), hablan sobre la recuperación de los equipos a nivel de incidentes, balanceo de tráfico, expansión de la red de datos, entre otros para así dar mejor eficiencia y calidad hacia la empresa o usuarios final, teniendo gestión sobre toda su infraestructura, abarcando cada novedad generada en la red con una solución óptima y sin daño.

9.2 Objetivo 2

El objetivo 2 se basa en Diseñar un laboratorio de simulación que incluya enrutadores virtuales, enlaces redundantes y nodos de prueba, permitiendo la práctica y experimentación con enrutamiento BGP en redes con enlaces redundantes.

Para el desarrollo de este objetivo se propone el diseño preliminar de cómo podría ser la primera topología lógica para la creación, teniendo en cuenta que es solo una idea para facilitar el desarrollo final.

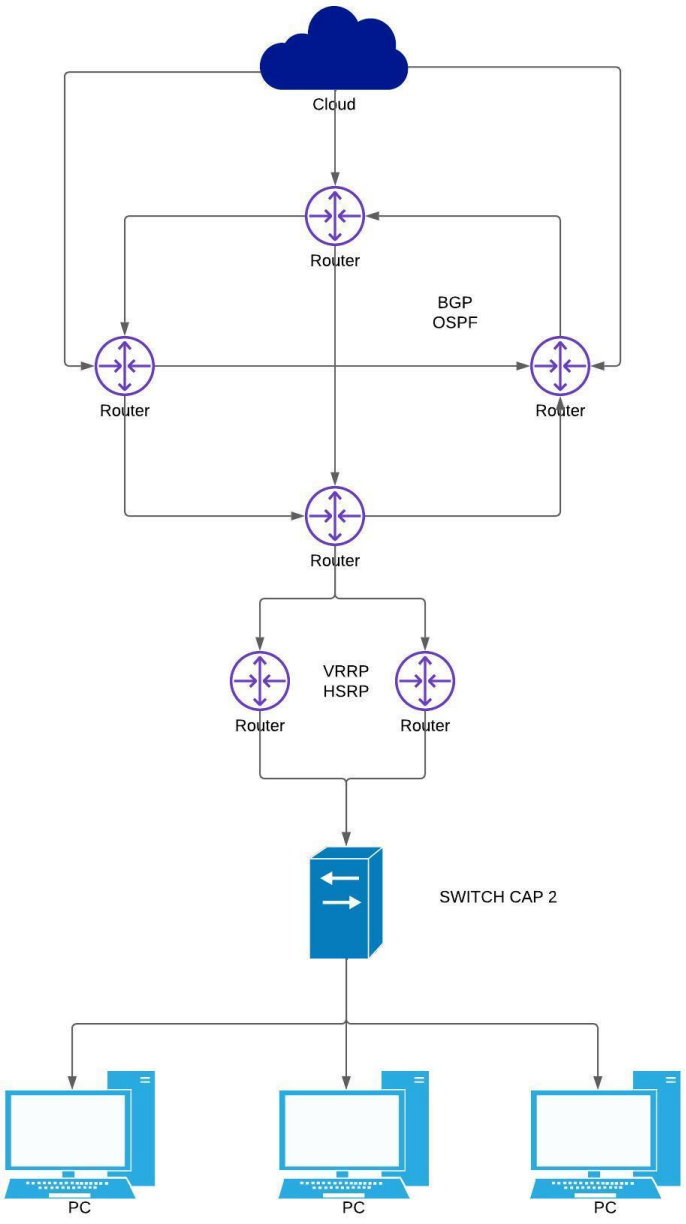


Figura 1. Primer diseño de topología lógica. Elaboración propia.

Anexo al proceso que se lleva con la topología lógica, también se ha venido definiendo y desarrollando donde se va a realizar como tal la simulación, ya que se tiene programas seleccionados como GNS3, NetSim, VIRL, EVE-NG y Cisco Packet Tracer, debido a que la Universidad Uniagustiniana es academia CISCO y dentro de sus cursos se usa utiliza el simulador Cisco Packet Tracer se realiza el enfoque sobre este y también el uso de los recursos de maquina no son tan alto.

La topología logia establecida para el desarrollo de la simulación propuesta se basa en las redes de comunicación de Redeban Multicolor ya que este es una parte de un modelo el cual se establece para la comunicación de los datafonos fijos que hay sobre los comercios como Éxito, Olímpica-Sao, Falabella, entre otros. Quienes ofrecen el servicio de pago por medio de datafono, QR, canjeo de bonos, consignación y retiros de dinero, entre otros servicios. Gracias al uso de varios ISP estas redes dan una alta disponibilidad y eficiencia para el desarrollo oportuno del servicio. (Es un caso real-empresarial).

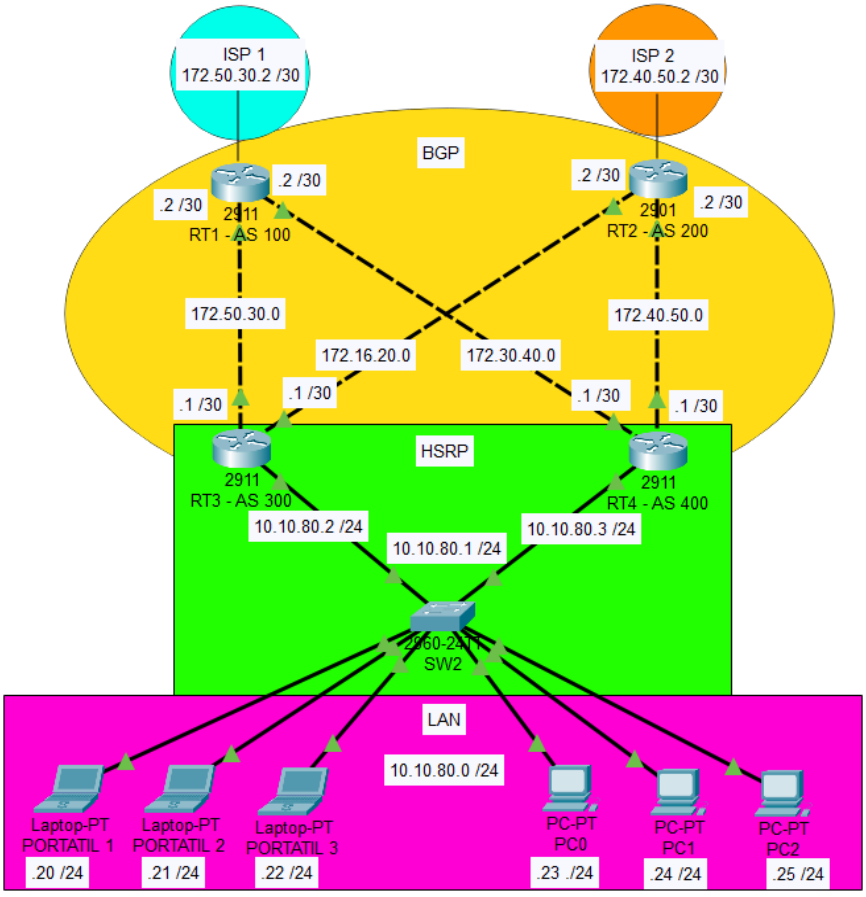


Figura 2. Diseño final de topología lógica. Elaboración propia.

9.2.1 Descripción de la topología lógica

Sobre la topología propuesta se van a utilizar los siguientes dispositivos de interconexión como:

Routers Cisco 2911, Con las siguientes características importantes, puertos Ethernet integrados de alta velocidad como ranuras para módulos de expansión para servicio, el cual incluye capacidades de distribución de energía y seguridad mejorada. Una der las características principales es brindar conectividad segura, para los servicios de voz, video y aplicaciones. Además, soporta protocolos de enrutamiento estático y dinámicos como son OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) y BGP (Border Gateway Protocol). Este protocolo es el que se va a implementar en la simulación. Otros de las características importantes es HSRP (Hot Standby Router Protocol) el cual se utiliza para la redundancia del tráfico nivel de la disponibilidad de los proveedores de servicio. Para la simulación se utilizar un total de 4 Routers.

(véase en anexo 5).

Switch Cisco 2960, ofrece una conectividad Gigabit y Fast Ethernet, así como características novedosas, Power over Ethernet Plus (PoE+), seguridad avanzada, gestión eficiente y tecnologías de ahorro de energía. Además, ofrece opciones limitadas de garantía del hardware y soporte técnico para satisfacer las necesidades de conectividad y operación segura de redes. Para la simulación solo se utilizó 1 Switch.

(véase en anexo 6).

En la simulación también se utilizaron equipos básicos como portátiles (3) y PC's (3) que se encuentran en el simulador.

Para la conectividad de los equipos, a nivel de Routers se utilizó un cableado crossover el cual sirve para conectar equipos que se encuentre en la misma capa o que son equipos iguales para la generación del protocolo BGP, para la conectividad de Router-Switch se utiliza un tipo de cableado directo el cual opera sobre equipos que NO se encuentren sobre la misma capa o que no sean equipos iguales, así mismo para la conectividad de los equipos básicos a nivel LAN.

Tabla 3.
Direccionamiento de los componentes de la topología lógica propuesta.

RT1 - AS 100			
Interface	Ip	Mascara	Función
Gig 0/0	172.30.40.2	255.255.255.252	RT4 - PPAL
Gig 0/1	172.50.30.2	255.255.255.252	RT3 - BK
RT2 - AS 200			
Interface	Ip	Mascara	función
Gig 0/0	172.16.20.2	255.255.255.252	RT3 - PPAL
Gig 0/1	172.40.50.2	255.255.255.252	RT4 - BK
RT3- AS 300			
Interface	Ip	Mascara	Función
Gig 0/0	172.16.20.1	255.255.255.252	BGP PPAL
Gig 0/1	172.50.30.1	255.255.255.252	BGP BK
Gig 0/2	10.10.80.2	255.255.255.0	HSRP - PPAL
RT4- AS 400			
Interface	Ip	Mascara	Función
Gig 0/0	172.30.40.1	255.255.255.252	BGP PPAL
Gig 0/1	172.40.50.1	255.255.255.252	BGP BK
Gig 0/2	10.10.80.3	255.255.255.0	HSRP - BK
RT VIRTUAL			
Interface	Ip	Mascara	Función
Gig 0/2	10.10.80.2	255.255.255.0	RT3 - PPAL
Gig 0/2	10.10.80.3	255.255.255.0	RT4 - BK
RT VIRTUAL	10.10.80.1	255.255.255.0	HSRP - Gateway
SW LAN			
Interface	Ip	Mascara	Función
Fa 0/0	10.10.80.20	255.255.255.0	PORTÁTIL 1
Fa 0/1	10.10.80.21	255.255.255.0	PORTÁTIL 2
Fa 0/2	10.10.80.22	255.255.255.0	PORTÁTIL 3
Fa 0/3	10.10.80.23	255.255.255.0	PC0
Fa 0/4	10.10.80.24	255.255.255.0	PC1
Fa 0/5	10.10.80.25	255.255.255.0	PC2

Nota: Tabla sobre las interfaces para la conectividad de los equipos de intercomunicación.

Se realizo un video para corroborar la implementación y de la simulación sobre la topología lógica planteada anteriormente.

9.2.2 Enlace del video

https://drive.google.com/file/d/1NIncYO78SDlMgk9F5rt12sLmGc8YTPEs/view?usp=drive_link

9.3 Objetivo 3

El logro del objetivo 3 se enfoca sobre el desarrollar una guía de estudio completa que sirva como recurso didáctico para el desarrollo de prácticas de laboratorio relacionadas con el enrutamiento BGP en redes con enlaces redundantes, el cual se basa sobre el (véase en anexo 2. Guía de estudio: Configuración de BGP y HSRP).

El desarrollo de esta guía fue en base a la estructura de las guías de actividades que se realizan con Cisco Packet Tracert en el entorno estudiantil de la Universidad Uniagustiniana, con una didáctica de aprendizaje basado en problemas enfocado en la enseñanza y aprendizaje en simular redes de entornos empresariales redundantes.

9.3.1 Topología Lógica

indica la estructura lógica de la red para realizar la conectividad.

9.3.2 Tabla de conectividad

indica el dispositivo, interfaz y el tipo de cableado que se debe de utilizar para su conectividad.

9.3.3 Tabla de direccionamiento Ip

indica el direccionamiento Ip que se va a utilizar sobre los equipos de conectividad y LAN.

9.3.4 Objetivos

establece la base de la guía, donde se centra el desarrollo y cumplimento que se va a desarrollar.

9.3.5 Aspectos básicos/situación

proporciona la información general sobre el tema o problema para enfocar y entender el desarrollo de la guía.

9.3.6 Recursos necesarios

Son los equipos, software y equipos finales simulados para el desarrollo de la guía.

9.3.7 Análisis de resultado

Evalúa el conocimiento y la funcionalidad de la guía cumpliendo todos los aspectos propuestos por los objetivos.

9.3.8 Encuesta de satisfacción

Evalúa la satisfacción que tiene el desarrollo de la guía.

Así mismo sobre el desarrollo de la guía se estructuro en partes y pasos, de manera que cada objetivo se convirtiera una parte a desarrollar y cada paso el proceso a seguir para poder cumplir con la configuración establecida. Cada paso cuenta con su respectivo contexto sobre el desarrollo,

ejemplos de configuración, imágenes de apoyo, notas adicionales y encuetas para confirmar la funcionalidad del desarrollado.

Esta estructura por partes y pasos facilita que el estudiantes o profesional pueda seguir de forma clara y organizada el proceso de configuración y aprendizaje, abordando cada objetivo de manera gradual y con el apoyo de los diferentes recursos incluidos en cada paso. Al dividir el desarrollo de la guía en esta forma, se busca asegurar que el estudiante o profesional pueda comprender íntegramente el tema de enrutamiento BGP en redes con enlaces redundantes.

Tras el desarrollo de la implementación de la guía de estudio a nivel estudiantil se obtuvo resultados de satisfacción muy positivos en el proceso de enseñanza y aprendizaje, ya que se pudo observar que los alumnos lograran comprender de manera clara y detallada los conceptos claves sobre el funcionamiento del protocolo BGP y su configuración en el escenario con enlaces redundantes. Esto se reflejó en la calidad de las configuraciones implementadas por los estudiantes en las practica de guía de estudio.

Gracias al enfoque del paso a paso de la guía, acompañado de los recursos de apoyo como ejemplos, imágenes y notas, permitió que los alumnos pudieran seguir el proceso de forma ordenada y sin mayor dificultad permitiéndoles cumplir todos los objetivos de la práctica de forma satisfactoria.

9.3.9 Resultados encuesta de satisfacción

La encuesta de satisfacción se llevó a cabo mediante el formulario de Google y se centró en la clase de interconexión de redes e integración dirigida por el profesor Ramiro Osorio Diaz. Seis participantes realizaron la actividad de evaluación. Los resultados revelaron un 90% de satisfacción, destacando que la guía proporcionada se percibió como una herramienta de aprendizaje altamente efectiva por parte de los alumnos.

Figura 3. Resultado tabla de conectividad. Elaboración propia.

Figura 4. Resultado tabla de direccionamiento Ip. Elaboración propia.

Figura 5. Resultado asignación de interfaz. Elaboración propia.

Figura 6. Resultado configuración básica. Elaboración propia.

Figura 7. Resultado configuración BGP. Elaboración propia.

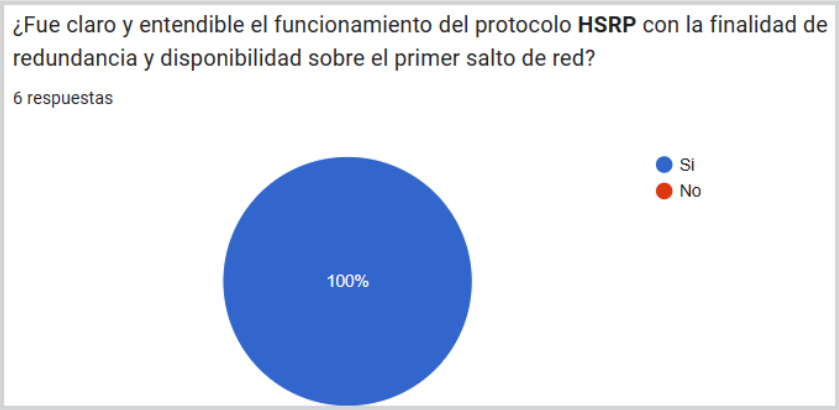


Figura 8. Resultado configuración HSRP. Elaboración propia.

Figura 9. Resultado análisis de resultado. Elaboración propia.

Figura 10. Resultado de satisfacción. Elaboración propia.

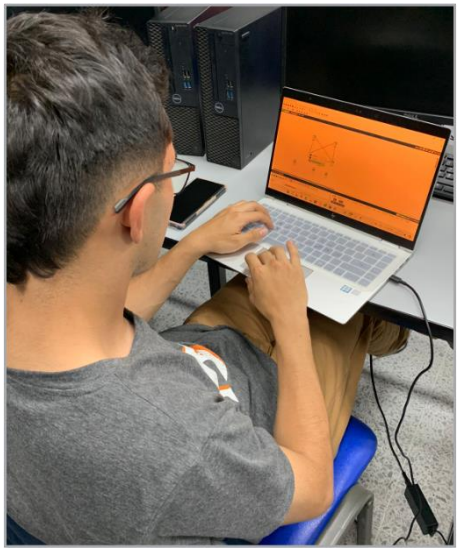


Figura 11. Estudiante realizando Guía de estudio – topología lógica. Elaboración propia.

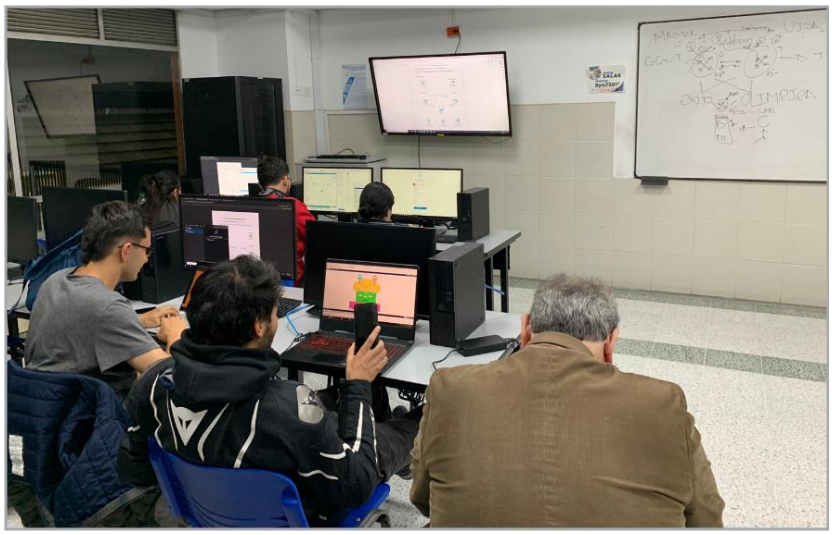


Figura 12. Explicación de topología lógica y funcionalidad de datafonos. Elaboración propia.

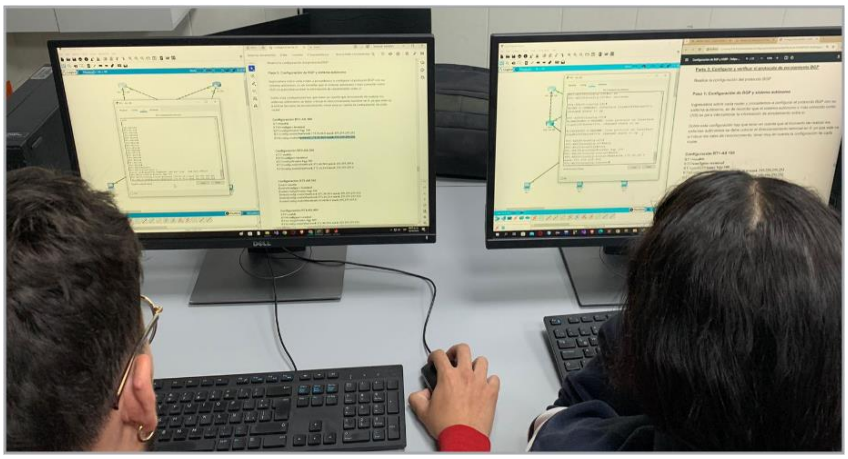


Figura 13. Configuración de Equipos de intercomunicación. Elaboración propia.

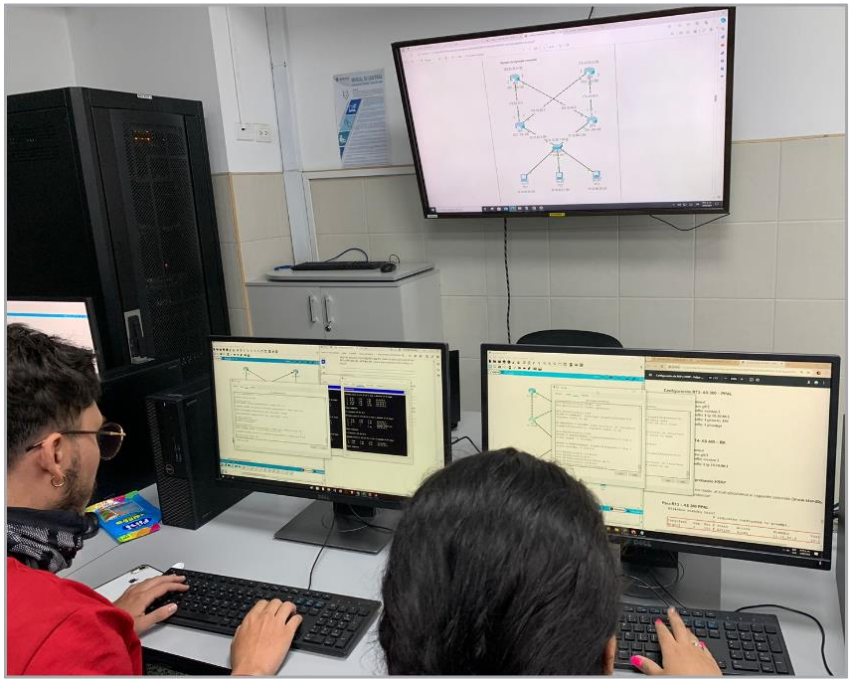


Figura 14. Pruebas sobre equipos de intercomunicación – protocolo BGP. Elaboración propia.

10 Conclusiones.

Basado en el desarrollo del laboratorio de simulación sobre enlaces redundantes con BGP se deja en evidencia que en primer lugar el diseño de la topología lógica y su segmentación es la base para poder tener un desarrollo óptico sobre la redundancia. Es necesario tener encuentra también el tipo de equipos que se van a utilizar a nivel de routers, switches así mismo como sus versiones, la disponibilidad que brinda el equipo y la capacidad de soportar protocolo de enrutamiento robustos como lo es el BGP por el alto índice de tráfico que se puede tener y la disponibilidad que depende de este.

Al momento de realizar la configuración es fundamental buscar la disponibilidad total para la red del cliente, asegurando que para ellos debe de ser transparente cualquier novedad o falla a nivel de enrutamiento aun así hay que tener encuentra que si fallan los dos ISP que se tiene para la red loca, ahí si se observa una afectación total en el servicio hasta que uno de estos se restablezca, así se pudo evidenciando sobre el desarrollo del laboratorio.

también debemos tener en cuenta que la mayoría de las empresas que utilizan este tipo de diseños o enlaces redundantes su principal fuente de ingreso o facturación del servicio se hace a través de internet, relacionando mi experiencia laboral sobre Redeban ya que la mayoría de los servicios se basa en a la disponibilidad total de los datafonos para realizar pagos mediante tarjetas, QR, transferencia, entre-cuentes, entre otros servicios.

Gracias desarrollo del laboratorio de simulación, los clientes pueden entender y comprender la importancia de contratar varios proveedores de internet (ISP) para garantizar la disponibilidad. también se destaca el protocolo HSRP, que determina el primer salto de red y el enrutamiento del tráfico dependiendo la configuración de este, escogiendo la disponibilidad del proveedor de servicio dependiendo la prioridad y la disponibilidad del canal.

En cuanto el desarrollo de la guía práctica relacionado con el simulador Cisco Packet Tracert, debido a que la Universidad Uniagustiniana es academia CISCO, se enfatiza en la importancia de profesionales y estudiantes puedan conocer, experimentar y desarrollar la base de topología redundantes que se puede encontrar a nivel empresarial y laboral. Esto permite profundizar en sus estudios o adquirir conocimientos básicos fundamentes sobre el funcionamiento de routers, switch, protocolos de enrutamiento en relación de la carrera de ingeniería en telecomunicaciones.

11 Referencias

Aguas L., (2019). Coexistencia de IPv4 con IPv6 a través del protocolo BGP. *Revista Nexos Científicos*, *3*(1). 12-29. Recuperado de: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index

Al-Musawi B., Branch P., Armitage G., (2017). BGP Anomaly Detection Techniques: A Survey. *IEEE Communications Surveys & Tutorials. Firstquarter, 19*(1). 377-396. - DOI: 10.1109/COMST.2016.2622240

Bustos C., (2016). *Diseño e implementación de la red de datos de urbano express sobre una red MPLS utilizando el método de VRF LITE y monitoreo mediante observium.* (Tesis de grado, Universidad de las Americas). Recuperado de: https://repositorioslatinoamericanos.uchile.cl/handle/2250/2789673

Castañeda G., (2018). *Implementación de un esquema de redundancia en la red de gestión de Americatel, mediante el uso de protocolo HSRP y SLA, en la sede principal Olguín.* (Tesis de grado, Universidad Tecnológica del Perú). Recuperado de: https://repositorio.utp.edu.pe/handle/20.500.12867/1002

Castillo J., (2022). *Diseño de una red de alta disponibilidad y redundancia con la finalidad de garantizar la conectividad de la UNMSM.* (Tesis de grado, Universidad Nacional Mayor de San Marcos). Recuperado de: https://cybertesis.unmsm.edu.pe/handle/20.500.12672/18927

Choquehuanca P., (2016). *Diseño e implementación de una red privada virtual redundante usando BGP y GLBP para la compañía DELOSI.* (Tesis de grado, Universidad Nacional Tecnológica de Lima Sur). Recuperado de: https://repositorio.untels.edu.pe/xmlui/handle/123456789/1089

Cisco. (2012) *Lo que usted necesita saber sobre routers y switches: Conceptos generales.* Cisco Systems Inc. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

Congreso De Colombia (2019, 25 de julio). *Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones* [Ley 1978]. Recuperado de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1978_2019.html

García J., Narváez G., (2018). *Mejoramiento en el uso de los enlaces WAN para clientes corporativos en una empresa de telecomunicaciones usando la solución de CISCO Intelligent WAN.* (Tesis de grado, Escuela Superior Politécnica Del Litoral). Recuperador de: https://www.dspace.espol.edu.ec/bitstream/123456789/45970/1/D-106548%20Garc%c3%ada-Narv%c3%a1ez.pdf

García J., Wang R., Chen M., Chou C., (2017, 5-8 de mayo). ETMP-BGP: Effective Tunnel-based Multi-Path BGP Routing Using Software-Defined Networking. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Canada. Recuperado de: https://ieeexplore.ieee.org/document/8122641

Hadi N., Al-Musawi B., (2021). Using BGP Features Towards Identifying Type of BGP Anomaly. 2021 International Congress of Advanced Technology and Engineering (ICOTEN). Yemen. Recuperador de: https://ieeexplore.ieee.org/document/9493491

HSRP Como funciona: Conceptos FHRP-CCNA 2. (2015). CCNA. Recuperado de: https://ccnadesdecero.es/hsrp/

Ignacio A., Sánchez E., Arias D., (2021 15-16 de abril). Simulación De Enrutamiento BGP Con GNS3. Universidad Nacional de Salta. XXIII Workshop de Investigadores en Ciencias de la Computación. Argentina. Recuperado de: https://sedici.unlp.edu.ar/bitstream/handle/10915/120027/P%C3%B3ster.pdf-PDFA.pdf?sequence=2&isAllowed=y

Incual.(2015). Cualificación Profesional: Administración Y Diseño De Redes Departamentales. Recuperador de: https://incual.educacion.gob.es/documents/20195/1873855/IFC081_3_RV+-+A_GL_Documento+publicado/141e387f-a0ac-4d57-9074-62357078354c

Jimenez S., (2021). *Diseño e implementación de una arquitectura de red redundante empleando balanceo de carga mediante los protocolos bgp y ospf para optimizar la red regional de Lima.* (Tesis de grado, Universidad Nacional Tecnológica de Lima Sur). Recuperado de: https://repositorio.untels.edu.pe/xmlui/handle/123456789/918

Martin C., (2015*). Análisis De Desempeño Con Respecto Al Jitter Y Delay, En Redes Soportadas En Mpls, Bgp Y Ospf Transmitiendo Video Sobre Ip.* (trabajo de grado, Universidad Santo Tomás) Recuperado de: https://repository.usta.edu.co/handle/11634/309

Martinez C., (2021). *Diseño de una red perimetral de internet de gran escala basada en el protocolo BGP, sistemas autónomos y prefijos IP propios.* (trabajo de grado, Universidad Peruana de Ciencias Aplicadas (UPC). Recuperado de: https://upc.aws.openrepository.com/handle/10757/656268

Muguerza C., (2014). *Configuración y gestión del equipamiento de red para el nuevo acceso a Internet de una empresa con encaminamiento BGP.* (trabajo de grado, Universidad Pública de Navarra) Recuperado de: https://academica-e.unavarra.es/xmlui/handle/2454/11824

Oprescu I., Meulle M., Owezarskit P., (2011). dVirt: a Virtualized Infrastructure for Experimenting BGP Routing. IEEE. 36th Conference on Local Computer Networks. Alemania. Recuperado de: https://ieeexplore.ieee.org/document/6115174/authors#authors

Oracle. (2015). Glosario de términos de redes. Recuperado de: https://docs.oracle.com/cd/E56339_01/html/E53820/gnchw.html

Quesquen L., (2019). *Diseño y Configuración De Un Sistema De Comunicaciones Basado En Transmisión Óptica En El Espacio Libre - Fso Y Redundancia Con Enlace Wireless Punto A Punto De 5.8 Ghz Para Sedes Empresariales En La Ciudad De Lima.* (trabajo de suficiencia, Universidad Nacional Tecnológica de Lima Sur).

Rodrigo Rodríguez. (2007). Cátedra: Redes de Computadoras: Glosario de Términos básicos. Recuperado de: https://rodrigorodriguez.files.wordpress.com/2009/02/glosario_redes.pdf

Salcedo O., López D., Hernández C., (2012). Evaluación de los protocolos OSPF-TE y BGP en funciones de autodescubrimiento para L1VPN sobre GMPLS. *Tecnura, 16*(33). 131-144. Recuperado de: https://repository.udistrital.edu.co/handle/11349/20629

Sun Y., Xu Y., Wu D., (2009). THE IMPLEMENTATION OF BGP-UPDATE BASED MONITORING METHOD FOR ROUTING ANOMALIES. IEEE International Conference on Network Infrastructure and Digital Content. China. Recuperado de: https://ieeexplore.ieee.org/document/5360800

Tapasco Garcia, M.O. (2008). *Proyecto propuesto como requisito parcial para obtener el pregrado en Ingeniería de Sistemas y Computación* (Tesis de maestría, Universidad Tecnológica De Pereira). Recuperado de: https://core.ac.uk/download/pdf/71395663.pdf.

12 Anexos

12.1 **Anexo 1.** Enlace para el desarrollo de la practica en Cisco Packet Tracert.

https://drive.google.com/file/d/1U506f6l4pEU8lF4tZm7POf_2T4RdBnDY/view?usp=drive_link

12.2 **Anexo 2.** Guía de estudio: Configuración de BGP y HSRP.

Practica de laboratorio: Configuración de BGP y HSRP

Topología Lógica

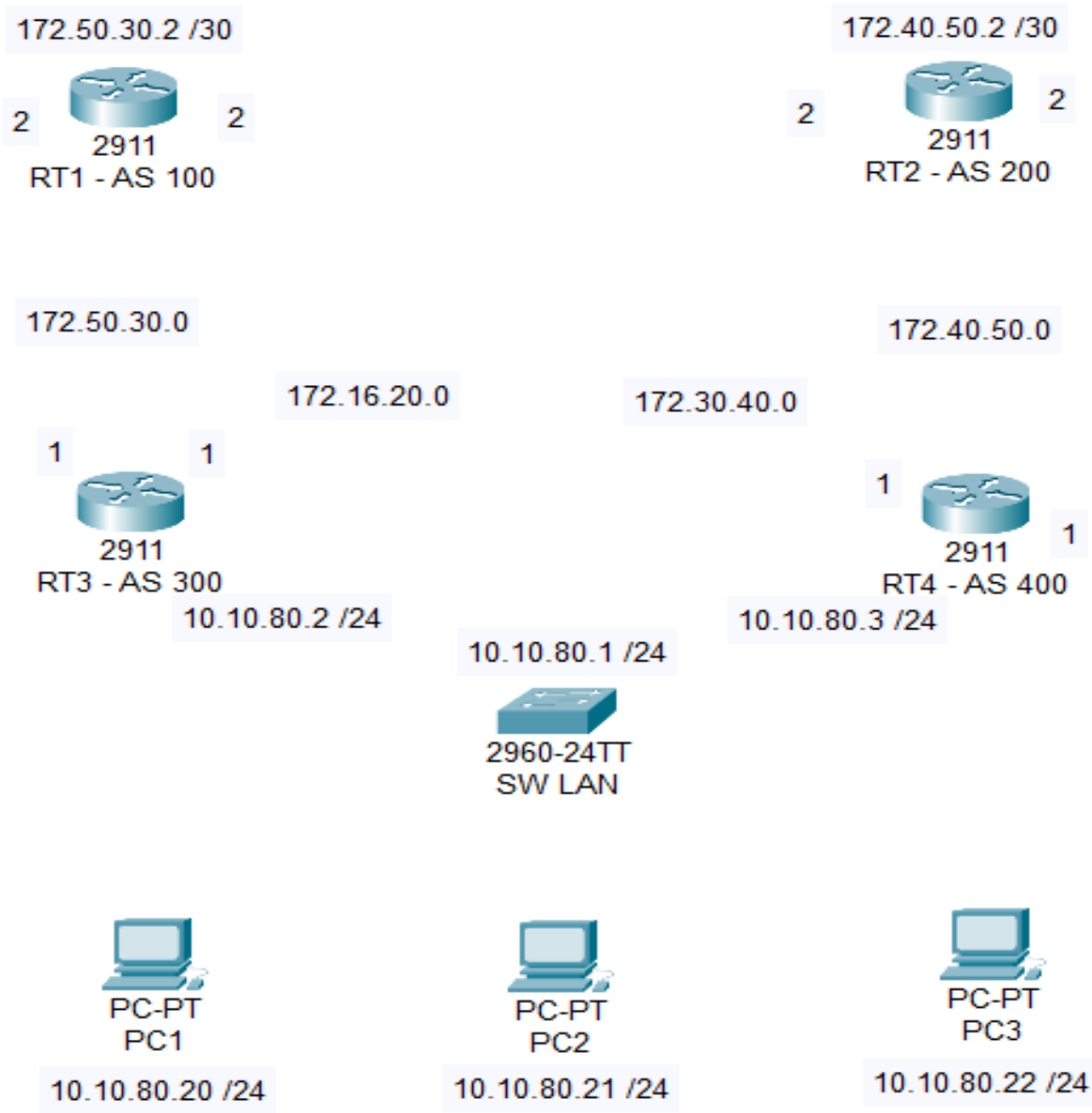


Tabla de conectividad - cableado		
Dispositivo	Interfaz	Tipo de cable
RT3 - RT2	Gig 0/0 | Gig 0/0	CROSS-OVER
RT1 - RT4	Gig 0/0 | Gig 0/0	CROSS-OVER
RT3 - RT1	Gig 0/1 | Gig 0/1	CROSS-OVER
RT4 - RT2	Gig 0/1 | Gig 0/1	CROSS-OVER
RT3 - SW LAN	Gig 0/2 | Fa 0/24	STRAIGHT-THROUGH
RT4 - SW LAN	Gig 0/2 | Fa 0/23	STRAIGHT-THROUGH
PC1 - SW LAN	Fa 0/0 | Fa 0/1	STRAIGHT-THROUGH
PC2 - SW LAN	Fa 0/0 | Fa 0/2	STRAIGHT-THROUGH
PC3 - SW LAN	Fa 0/0 | Fa 0/3	STRAIGHT-THROUGH

Tabla de direccionamiento				
Dispositivo	Interfaz	Dirección Ip	Máscara de subred	Gateway
RT1 - AS 100	Gig 0/0	172.30.40.2	255.255.255.252	N/A
	Gig 0/1	172.50.30.2	255.255.255.252	N/A
RT2 - AS 200	Gig 0/0	172.16.20.2	255.255.255.252	N/A
	Gig 0/1	172.40.50.2	255.255.255.252	N/A
RT3 - AS 300	Gig 0/0	172.16.20.1	255.255.255.252	N/A
	Gig 0/1	172.50.30.1	255.255.255.252	N/A
	Gig 0/2	10.10.80.2	255.255.255.0	N/A
RT4 - AS 400	Gig 0/0	172.30.40.1	255.255.255.252	N/A
	Gig 0/1	172.40.50.1	255.255.255.252	N/A
	Gig 0/2	10.10.80.3	255.255.255.0	N/A
PC1	NIC	10.10.80.20	255.255.255.0	10.10.80.1
PC2	NIC	10.10.80.21	255.255.255.0	10.10.80.1
PC3	NIC	10.10.80.22	255.255.255.0	10.10.80.1

Objetivo general de la guía

Esta guía tiene como propósito capacitar a los participantes en la configuración y verificación de redes, centrándose en la implementación efectiva de protocolos fundamentales como BGP para la conectividad entre proveedores de servicios de internet y HSRP para garantizar la redundancia de primer salto en entornos locales. Se busca proporcionar a los estudiantes las habilidades necesarias para asegurar una conectividad confiable y de alta disponibilidad tanto a nivel global como en redes locales, mediante la combinación de teoría y práctica utilizando herramientas como Cisco Packet Tracer y equipos de red específicos.

Objetivos para el desarrollo de la guía

Parte 1: Armar la red y verificar la conectividad

Parte 2: Configuración básica de switch y routers.

Parte 3: Configurar y verificar el protocolo de enrutamiento BGP

Parte 4: Configurar y verificar la redundancia de primer salto mediante HSRP

Aspectos básicos/situación

El protocolo BGP (Border Gateway Protocol) es fundamental para la conectividad entre proveedores de servicios de internet (ISP), ya que permite el intercambio de información de enrutamiento entre sistemas autónomos. Esto garantiza que los proveedores de internet puedan seleccionar le mejor ruta para el tráfico de datos, optimizando así la disponibilidad y el rendimiento para sus clientes.

Además, a nivel de redes locales (LAN), para asegurar la mejor disponibilidad y redundancia, se implementa el protocolo HSRP (Hot Standby Router Protocol) en los router finales. El HSRP permite crear una puerta de enlace virtual, de modo que si un router falla el otro puede tomar de forma inmediata y transparente el control del tráfico asegurando la conectividad del servicio.

Esta combinación de BGP a nivel de proveedor de servicios de internet y HSRP a nivel de redes locales es fundamental para garantizar una conectividad confiable y de alta disponibilidad tanto a nivel global como en entornos locales.

Nota: asegúrese de que todos los routers y switch no tengan ninguna configuración.

Recursos necesarios:

- Equipo pc con software de simulación Cisco Packet Tracert
- 4 rotuers (Cisco 2911).
- 1 switch (Cisco 2960-24)
- 3 computadores

Parte 1: Armar la red y verificar la conectividad

En la parte 1, establecerá la topología de red, la conectividad de los equipos con el cableado de red indicado, configuración de las direcciones de IP sobre cada interfaz y equipos.

Paso 1: Realizar el cableado como indica la tabla de conectividad

Conecte los equipos como indica la tabla de conectividad, recuerde que los tipos de cables se encuentran sobre connections, tenga en cuenta los diferentes tipos de cables que le solicitan para conectar cada dispositivo.

Paso 2: Configuración Sobre los PC'S

Para la configuración de los dispositivos, debemos de darte doble clic para que nos habilite la interfaz gráfica y poder realizar la configuración.

- Vamos a la parte de Desktop
- Ingresamos a IP Configuración
- Ingresamos los datos dados por la tabla de direccionamiento sobre cada equipo.

PC1

IPv4 Address: 10.10.80.20

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.80.1

PC2

IPv4 Address: 10.10.80.21

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.80.1

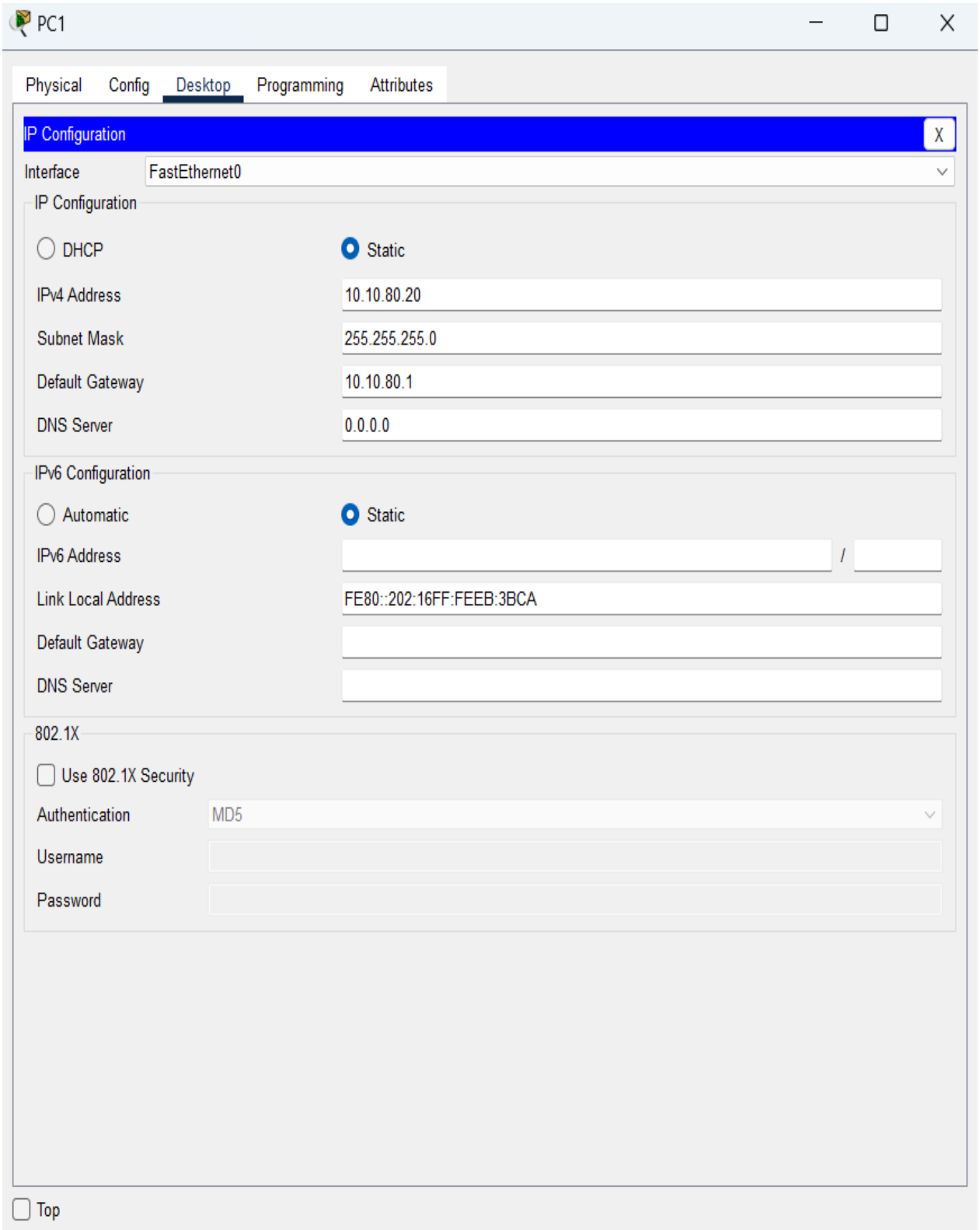
PC3

IPv4 Address: 10.10.80.22

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.80.1

Ejemplo sobre PC1



Paso 3: Configuración de direccionamiento sobre los routers

En esta parte vamos a configurar las IP's sobre cada interfaz de los router, deshabilitar la búsqueda de DNS, dejar la descripción correspondiente sobre cada interfaz y subir las interfaces para tener conectividad.

Recuerde que estas configuraciones se deben de replicar sobre todos los routers teniendo en cuenta su direccionamiento ip y mascara de subred como indica la tabla de enrutamiento.

Nota: Recuerde que **RT3 – AS 300 y RT4 – AS 400** lleva una configuración demás sobre la interfaz Gig 0/2 ya que este es para el realizar el protocolo **HSRP.**

Paso 4: Ingresar a la interfaz de configuración del router

- Damos doble clic sobre el router
- Vamos a la parte que dice CLI

Paso 5: Deshabilitar la búsqueda de DNS

Ingresamos sobre todos los router y switch donde ejecutamos el siguiente comando (no ip domain-lookup) para deshabilitar la búsqueda DNS, ya que este si llegamos a ejecutar algún comando mal nos pausara un tiempo mientras trata de realizar la búsqueda de DNS.

Router>**enable**
Router#**configure terminal**
Router(config)#**no ip domain-lookup**

Paso 6: Configuración de las interfaces sobre el router.

Se realiza la configuración de cada router sobre cada interfaz con su respectivo direccionamiento.

Nota: Recuerde guardar al realizar cualquier configuración con el comando write memory (**wr**) en la parte de enable sobre la configuración de los routers.

Configuración RT1 – AS 100 G0/0

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/0**
Router(config-if)#**ip address 172.30.40.2 255.255.255.252**
Router(config-if)#**description BGP-RT1-G0/0**
Router(config-if)#**no shutdown**

Configuración RT1 – AS 100 G0/1

Router>**enable**
Router#configure **terminal**
Router(config)#**interface g0/1**
Router(config-if)#**ip address 172.50.30.2 255.255.255.252**
Router(config-if)#**description BGP-RT1-G0/1**
Router(config-if)#**no shutdown**

Configuración RT2 – AS 200 G0/0

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/0**
Router(config-if)#**ip address 172.16.20.2 255.255.255.252**
Router(config-if)#**description BGP-RT2-G0/0**
Router(config-if)#**no shutdown**

Configuración RT2 – AS 200 G0/1

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/1**
Router(config-if)#**ip address 172.40.50.2 255.255.255.252**
Router(config-if)#**description BGP-RT2-G0/1**
Router(config-if)#**no shutdown**

Configuración RT3 – AS 300 G0/0

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/0**
Router(config-if)#**ip address 172.16.20.1 255.255.255.252**
Router(config-if)#**description BGP-RT3-G0/0**
Router(config-if)#**no shutdown**

Configuración RT3 – AS 300 G0/1

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/1**
Router(config-if)#**ip address 172.50.30.1 255.255.255.252**
Router(config-if)#**description BGP-RT3-G0/1**
Router(config-if)#**no shutdown**

Configuración RT3 – AS 300 G0/2

Router>**enable**
Router#**configure terminal**

Router(config)#**interface g0/2**
Router(config-if)#**ip address 10.10.80.2 255.255.255.0**
Router(config-if)#**description HSRP_PPAL-RT3-G0/2**
Router(config-if)#**no shutdown**

Configuración RT4 – AS 300 G0/0

Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/0**
Router(config-if)#**ip address 172.30.40.1 255.255.255.252**
Router(config-if)#**description BGP-RT4-G0/0**
Router(config-if)#**no shutdown**

Configuración RT4 – AS 400 G0/1

Router>**enable**
Router#configure **terminal**
Router(config)#**interface g0/1**
Router(config-if)#**ip address 172.40.50.1 255.255.255.252**
Router(config-if)#**description BGP-RT4-G0/1**
Router(config-if)#**no shutdown**

Configuración RT4 – AS 400 G0/2

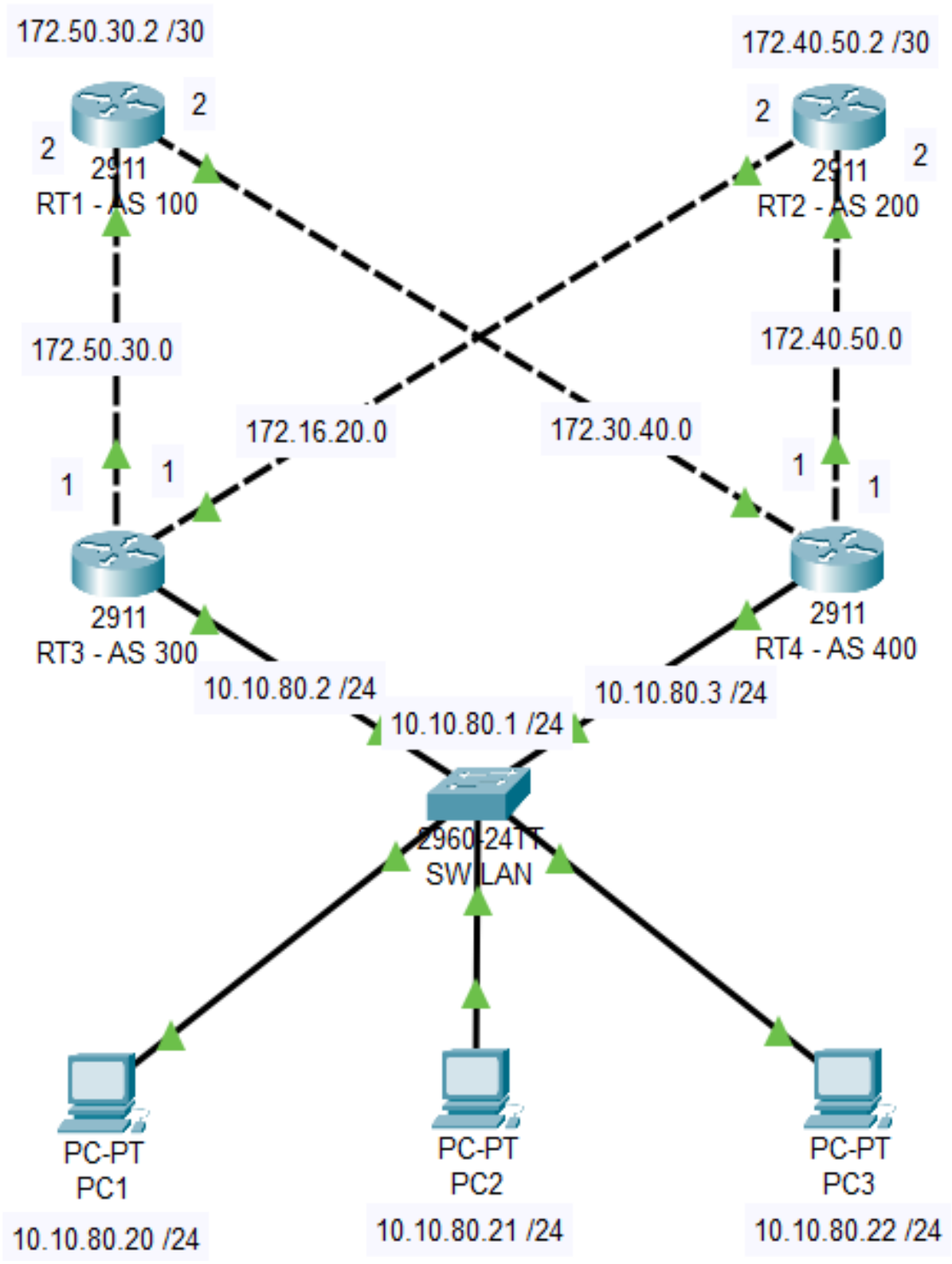
Router>**enable**
Router#**configure terminal**
Router(config)#**interface g0/2**
Router(config-if)#**ip address 10.10.80.3 255.255.255.0**
Router(config-if)#**description HSRP_BK-RT4-G0/2**
Router(config-if)#**no shutdown**

Paso 7: Validación de topología, conectividad y direccionamiento

Validar que a nivel de topología se evidencie todas las interfaces con conectividad, sobre los router, validar que todas las interfaces estén con su configuración correspondiente sobre el cuadro de direccionamiento.

Para validar el direccionamiento sobre los router, ejecutamos el siguiente comando (**show running-config**) sobre enable, es de recordar que hay otros comandos para también validar el direccionamiento.

Ejemplo de topología conectada



Ejemplo sobre RT1-AS 100

Router>**enable**
Router#**show running-config**

```
interface GigabitEthernet0/0
 description BGP-RT1-G0/0
 ip address 172.30.40.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description BGP-RT1-G0/1
 ip address 172.50.30.2 255.255.255.252
 duplex auto
 speed auto
```

Ejemplo sobre RT3 – AS 300

Router>**enable**
Router#**show running-config**

```
interface GigabitEthernet0/0
 description BGP-RT3-G0/0
 ip address 172.16.20.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description BGP-RT3-G0/1
 ip address 172.50.30.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 description HSRP_PPAL-RT3-G0/2
 ip address 10.10.80.2 255.255.255.0
 duplex auto
 speed auto
```

Paso 8: Comprobar direccionamiento de equipos

Realice sobre **RT 2- AS 200 y RT 4 – AS 400** las validaciones de ejemplo que se hizo sobre **RT1 – AS 100y RT3 - AS 300** y confirmando su configuración con su respectivo direccionamiento así mismo validando **PC2 y PC3** sobre el ejemplo de **PC1** con su respectivo direccionamiento.

Paso 9: Comprobar conectividad

Realice ping entre equipos PC1 a PC2. ¿fue éxito el ping? _____.

Realice ping entre PC1 a RT3 – AS 300, tenga en cuenta que el ping se debe de realizar sobre el direccionamiento de la interfaz. ¿fue éxito el ping? _____.

Realice ping entre RT1 – AS 100 a RT4 - AS 400, tenga en cuenta que el ping se debe realizar sobre el direccionamiento de la interfaz. ¿fue éxito el ping? _____.

Realice ping entre RT2 – AS 200 a RT4 – AS 400, ¿fue éxito el ping? _____.

Realice ping entre RT3-AS 300 a RT4-AS400, ¿fue exitoso el ping? _____.

Parte 2: Configuración básica de switch y routers.

En esta parte se va a configurar básica sobre los equipos, para si tener gestion y seguridad al momento de realizar configuraciones

Paso 1: Configuración de nombre

Ingresamos nuevamente sobre la interfaz de configuración sobre routers y swirch, procedemos a realizar la configuración del nombre sobre cada equipo.

Configuración SW LAN

Switch>**enable**
Switch# **configure terminal**
Switch(config)#**hostname SW_LAN**
SW_LAN(config)#

Configuración RT1 – AS 100

Router>**enable**
Router#**configure terminal**
Router(config)#**hostname RT1**
RT1(config)#

Paso 2: Configuración de hora y fecha

Ya que nos encontramos sobre la interfaz de configuración, procedemos a configurar la fecha y hora sobre los equipos, el comando para este es (clock set [hh:mm:ss] [month] [day] [year]).

Configuración SW-LAN

Switch>**enable**
SW_LAN#**clock set 14:54:00 09 April 2024**

Configuración RT1- AS 100

RT1>**enable**
RT1#**clock set 14:54:00 09 April 2024**

Paso 3: Configurar Contraseñas EXEC y de inicio de sesión

Ahora procedemos a configurar y a encriptar la contraseña de ingreso y de EXEC para poder ingresar a la configuración de enable y Configure terminal, esto se realiza para tener la seguridad y gestión adecuada sobre los equipos.

Contraseña de ingreso: **cisco**

Contraseña de EXEC: **class**

Configuracion SW-LAN

SW_LAN>**enable**
SW_LAN#**conf terminal**
SW_LAN(config)#**enable secret class**
SW_LAN(config)#**line console 0**
SW_LAN(config-line)#**password cisco**
SW_LAN(config-line)#**login**
SW_LAN(config-line)#**exit**
SW_LAN(config)#**service password-encryption**

Configuracion RT1- AS 100

RT1>**enable**
RT1#**configure terminal**
RT1(config)#**enable secret class**
RT1(config)#**line console 0**
RT1(config-line)#**password cisco**
RT1(config-line)#**login**
RT1(config-line)#**exit**
RT1(config)#**service password-encryption**

Paso 4: Configurar Banner de Bienvenida

Por último, vamos a configurar un banner de bienvenida, el cual, al momento de ingresar sobre cualquier equipo, este será nuestra primera vista de bienvenida u información.

Configuracion SW-LAN

SW_LAN>**enable**
SW_LAN#**configure terminal**
SW_LAN(config)#**banner motd $El acceso no autorizado, esta prohibido$**

Configuracion RT1- AS 100

RT1#**enable**
RT1#**configure terminal**
RT1(config)#**banner motd $El acceso no autorizado, esta prohibido$**

Paso 5: Replicar configuración sobre routers

Ya que tenemos configurado el switch y el RT1 – AS 100, vamos a replicar todas estas configuraciones sobre los routers restantes.

Paso 6: Probar y confirmar Configuración básica de switch y routers.

Cierre todas las pestañas de configuración de los equipos e ingrese nuevamente

¿Se evidencian el banner de bienvenida que configuro sobre los dispositivos? _____.

¿Puede ingresar sobre los equipos con las contraseñas configuradas? _____.

Si ejecuta el comando show clock detail sobre la interfaz de enable ¿Qué puede evidenciar? _____.

Nota: Recuerde guardar los cambios después de realizar todas las configuraciones indicas, no modifique las contraseñas o si las va a modificar téngalas en cuenta de recordarlas.

Parte 3: Configurar y verificar el protocolo de enrutamiento BGP

Realice la configuración del protocolo BGP

Paso 1: Configuración de BGP y sistema autónomo

Ingresamos sobre cada router y procedemos a configurar el protocolo BGP con su sistema autónomo, es de recordar que el sistema autónomo o más conocido como (AS) es para intercambiar la información de enrutamiento entre sí.

Sobre esta configuración hay que tener en cuenta que al momento de realizar los sistemas autónomos se debe colocar el direccionamiento terminal en 0, ya que este va a indicar las rutas de reconocimiento, tener muy en cuenta la configuración de cada router.

Configuración RT1-AS 100

RT1#**enable**
RT1#**configure terminal**
RT1(config)#**router bgp 100**
RT1(config-router)#**network 172.50.30.0 mask 255.255.255.252**
RT1(config-router)#**network 172.30.40.0 mask 255.255.255.252**

Configuración RT2-AS 200

RT2>**enabl**e
RT2#**configure terminal**
RT2(config)#**router bgp 200**
RT2(config-router)#**network 172.40.50.0 mask 255.255.255.0**
RT2(config-router)#**network 172.16.20.0 mask 255.255.255.0**

Configuración RT3-AS 300

Router>**enable**
Router#**configure terminal**
Router(config)#**router bgp 300**
Router(config-router)#**network 172.50.30.0 mask 255.255.255.252**
Router(config-router)#**network 172.16.20.0 mask 255.255.255.252**
Router(config-router)#**network 10.10.80.0 mask 255.255.255.0**

Configuración RT4-AS 400

RT4>**enable**
RT4#**configure terminal**
RT4(config)#**router bgp 400**
RT4(config-router)#**network 172.40.50.0 mask 255.255.255.252**
RT4(config-router)#**network 172.30.40.0 mask 255.255.255.252**
RT4(config-router)#**network 10.10.80.3 mask 255.255.255.0**

Paso 2: configuración de vecinos

Para poder seguir con la configuración de BGP, es de recordar que sobre este protocolo en cada router hay que especificarle las direcciones IP de cada vecino y el número de su sistema autónomo.

Tenga muy en cuenta cada configuración del router, este proceso ya que vamos a configurar son las direcciones IP de los vecinos para generar adyacencia.

Configuración RT1-AS 100

RT1#**enable**
RT1#**conf terminal**
RT1(config)#**router bgp 100**
RT1(config-router)#**neighbor 172.50.30.1 remote-as 300**
RT1(config-router)#**neighbor 172.30.40.1 remote-as 400**

Configuración RT2-AS 200

RT2>**enable**
RT2#**configure terminal**
RT2(config)#**router bgp 200**
RT2(config-router)#**neighbor 172.16.20.1 remote-as 300**
RT2(config-router)#**neighbor 172.40.50.1 remote-as 400**

Configuración RT3-AS 300

RT3#**enable**
RT3#**conf terminal**
RT3 (config)#**router bgp 300**
RT3 (config-router)#**neighbor 172.50.30.2 remote-as 100**
RT3 (config-router)#**neighbor 172.16.20.2 remote-as 200**
RT3 (config-router)#**end**

Configuración RT4-AS 400

RT4>**enable**
RT4#**configure terminal**
RT4(config)#**router bgp 400**
RT4(config-router)#**neighbor 172.40.50.2 remote-as 200**
RT4(config-router)#**neighbor 172.30.40.2 remote-as 100**

Paso 3: Verificación del protocolo BGP

Al finalizar la configuración indicada sobre los pasos anteriores, vamos a verificar que haya quedado la configuración sobre cada router,

Para confirmar esto vamos a realizar 2 comando para la certificar la configuración sobre cada router.

Comando: show ip bgp

Este comando nos mostrará las IP sobre los redes y vecinos de nuestro BGP.

Ejemplo RT3 – AS 300

RT3>**enable**
RT3#**show ip bgp**

```
BGP table version is 12, local router ID is 172.50.30.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.80.0/24    0.0.0.0                  0     0 32768 i
*                   172.16.20.2              0     0     0 200 400 i
*                   172.50.30.2              0     0     0 100 400 i
*> 172.16.20.0/30   0.0.0.0                  0     0 32768 i
*> 172.30.40.0/30   172.50.30.2              0     0     0 100 i
*                   172.16.20.2              0     0     0 200 400 i
*> 172.40.50.0/30   172.16.20.2              0     0     0 200 400 i
*                   172.50.30.2              0     0     0 100 400 i
*> 172.50.30.0/30   0.0.0.0                  0     0 32768 i
*                   172.50.30.2              0     0     0 100 i
*                   172.16.20.2              0     0     0 200 400 100 i
```

Comando: show running-config

Este comando nos mostrará las IP sobre los redes y vecinos de nuestro BGP.

Ejemplo RT3 – AS 300

RT3>**enable**
RT3#**show running-config**

```
router bgp 300
 bgp log-neighbor-changes
 no synchronization
 neighbor 172.50.30.2 remote-as 100
 neighbor 172.16.20.2 remote-as 200
 network 172.50.30.0 mask 255.255.255.252
 network 172.16.20.0 mask 255.255.255.252
 network 10.10.80.0 mask 255.255.255.0
```

Reiter estos mismos comandos sobre cada router y confirme:

¿Se genero el mensaje informativo de BGP-5-ADJCHANGE cuando configuro los vecinos? _____.

¿Qué diferencia tiene las network de RT3-AS 300 a diferencia de RT1-AS100? _____.

Paso 4 Comprobar conectividad con protocolo BGP

Realice ping desde RT3-AS 300 a RT1-AS 100. ¿El ping fue exitoso? _____.

Realice ping desde RT2-AS 200 a RT1-AS 100. ¿El ping fue exitoso? _____.

Realice ping desde RT1-AS 100 a RT2-AS 200. ¿El ping fue exitoso? _____.

Si hago un show ip router, ¿puedo evidenciar las ip de los vecinos? _____.

Parte 4: Configurar y verificar la redundancia de primer salto mediante HSRP

Parte 1 Configurar HSRP

Esta configuración se va a realizar sobre los routers RT3- AS 300 y RT4-AS 400 en la interfaz G0/2 que se dejó destinada para la configuración de este protocolo.

Al momento de ingresar sobre los router, se debe de tener en cuenta que se debe seleccionar el router principal y el router back up, el cual, sobre la descripción de cada uno de los router, se señaló como:

Enlace Principal: RT3-AS 300 – Gig 0/2 – **PPAL**

Enlace Back Up: RT4-AS 400 – Gig 0/2 – **BK**

Configuración RT3- AS 300 – PPAL

RT3>**enable**
RT3#**configure terminal**
RT3(config)#**interface g0/2**
RT3(config-if)#**standby version 2**
RT3(config-if)#**standby 1 ip 10.10.80.1**
RT3(config-if)#**standby 1 priority 150**
RT3(config-if)#**standby 1 preempt**

Configuración RT4- AS 400 – BK

RT4>**enable**
RT4#**configure terminal**
RT4(config)#**interface g0/2**
RT4(config-if)#**standby version 2**
RT4(config-if)#**standby 1 ip 10.10.80.1**

Paso 2: Verificar protocolo HSRP

Ingresamos sobre los router, el cual ejecutamos el siguiente comando (show standby brief) y se debe evidenciar:

Para RT3 – AS 300 PPAL

```
RT3#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/2      1    150 P Active   local           10.10.80.3      10.10.80.1
```

Para RT4 – AS 400 BK

```
RT4#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/2      1    100   Standby  10.10.80.2      local           10.10.80.1
```

Es de recordar que este protocolo es para la redundancia sobre el primer salto de red y creación de “un router virtual “el cual está configurado con la IP 10.10.80.1 que si nos damos cuenta es el Gateway que tiene los equipos PC’S, debido a que, si se llega a tener una falla u incidente sobre el router PPAL o proveedor principal, se enrutara el tráfico sobre el router Back Up, siendo transparente para los equipos nivel LAN o cliente final.

Paso 3 Comprobar conectividad con HSRP

Realice ping desde PC1 a PC2. ¿El ping fue exitoso? _____.

Realice ping desde PC3 a RT1-AS 100. ¿El ping fue exitoso? _____.

Realice ping desde RT2-AS 200 a PC2. ¿El ping fue exitoso? _____.

Si realizo un tracert desde PC3 a RT1-AS 100 ¿a qué IP hace referencia el primer salto? _____.

Análisis de resultado

1. Realice un tracert desde PC1 a RT1 - AS 100. ¿Qué puede evidenciar sobre los saltos de red?

   _____

   _____

   _____.

2. Ingresa al RT3-AS 300 sobre la interfaz Gig 0/2 y baje la interfaz (shut), ahora realice un ping y un tracert desde PC1 a RT1-AS 100. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

3. Ingrese al RT4-AS 400 sobre la interfaz Gig 0/0 y baje la interfaz (shut), ahora realice un ping y un tracert desde PC1, PC2 y PC3 a RT1-AS 100. ¿Qué puede evidenciar sobre el ping y el tracert?

   Nota: Este proceso tiene un tiempo de demora, el cual puede variar entre 1 a 3 minutos, realice el proceso indicado después de este tiempo ya que los equipos deben de hacer la búsqueda de la ruta más rápida entre vecinos

   _____

   _____

   _____.

4. Restablezca todas las interfaces que se encuentra down (no shut), ahora ingrese a RT3-AS 300 sobre la interfaz Gig 0/1 y baje la interfaz, ahora realice un ping y un tracert desde PC3 a RT1-AS 100. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

5. Ingrese al RT4-AS 400 y realice un ping a RT1-AS 100. ¿Qué puede evidenciar sobre el ping?

   _____

   _____

   _____.

6. Ingrese sobre PC2 y realice un ping y un tracert para RT2-AS 200. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

7. Ingrese sobre RT4-AS 400 sobre la interfaz Gig 0/1 y baje la interfaz (shut), ahora realice ping y una tracer desde PC1 para RT1-AS 100 y RT2-AS 200. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

8. Restablezca todas las interfaces (no shut), ahora ingrese a RT3-AS 300 y bajes las interfacez (shut) Gig 0/0 y Gig 0/1, realice un ping y un tracert desde PC1 a RT1-AS 100 y RT2-AS 200. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

9. Ingrese a RT4-AS 400 e ingrese al protocolo HSRP y fuerce la prioridad del router BK a 160 con preempt, ahora realice de nuevo el ping y el tracert desde PC1 a RT1-AS 100 y RT2-AS 200. ¿Qué puede evidenciar sobre el ping y el tracert?

   _____

   _____

   _____.

10. Restablezca todas las interfaces (shut) y normalice la prioridad sobre el router BK de HSRP y quite el comando preempt, ¿fue clara la guía de practica para entender el protocolo BGP y HSRP sobre enlaces redundantes?

    _____

    _____

    _____.

12.3 Anexo 3. Encuesta de calificación: Guía de estudio - Configuración de BGP y HSRP. https://forms.gle/SR1Vx5eSNB8apGHXA

12.4 Anexo 4. Enlace de Guía de estudio PDF - Configuración de BGP y HSRP. https://drive.google.com/file/d/1knycRX7B8JTQ7yvwfwIYCx-QJ1n1tHqH/view?usp=drive_link

12.5 **Anexo 5.** Data sheet Router Router Cisco 2911

Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. Day-one device support provides immediate manageability support for the Integrated Services Router, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every Integrated Services Router. The new Integrated Services Routers continue a tradition of broad and deep manageability features such as IP Service-Level Agreement (IP SLA), Cisco IOS Embedded Event Manager (EEM), and NetFlow which allow you to know the status of your network at all times. These features, along with Simple Network Management Protocol (SNMP) and syslog, enable your organization's management applications.

Refer to Tables 4 and 5 below for details about network management and manageability support on Cisco 2900 Series Integrated Services Routers.

Table 4. Cisco 2900 ISR G2 Series IOS Software Features and Protocols Support

Feature	Support
Protocols	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulation	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic Management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS software refer to the Feature Navigator tool at https://www.cisco.com/go/fn.

Table 5 lists the embedded management features available with Cisco IOS Software.

Table 5. Embedded Management Features Available with Cisco IOS Software

Feature	Description
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP Service-Level Agreements (SLAs) enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video in an IP network.
SNMP, RMON, Syslog, NetFlow, and TR-069	Cisco 2900 Series Integrated Services Routers also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

The Cisco network management applications listed in Table 6 are standalone products that you can download or purchase to manage your Cisco network devices. The applications are built specifically for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Applications

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software–based access routers. This tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Network-wide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco Integrated Services Routers, using new instrumentation such as Cisco IOS EEM Generic Online Diagnostics (GOLD). In addition to supporting basic platform services of the Integrated Services Router, CiscoWorks also provides added-value support for the Cisco Services Ready Engine, enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Network-wide staging, configuration, and compliance	CiscoWorks NCM	CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Voice configuration and provisioning	Cisco Unified Provisioning Manager	Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	Easily manage Cisco IOS Software activation and licenses for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary

As your business strives to lower the total cost of ownership in running your network and increase your overall employee productivity with more centralized and collaborative network applications, you will need more intelligent branch-office solutions. The Cisco 2900 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 2900 Series is designed to consolidate the functions of many separate devices into a single, compact system.

Table 7. Cisco 2900 Integrated Services Router Product Specifications

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Services and Slot Density				
Embedded Hardware-Based Cryptography and Acceleration	Yes	Yes	Yes	Yes
Cisco Unified SRST Sessions	35	50	100	250

12.6 **Anexo 6.** Data sheet Switch Cisco 2660

Switch Configurations

Table 1. Cisco Catalyst 2960-S Series Switches Configurations

Model	10/100/1000 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power	FlexStack Stacking
Cisco Catalyst 2960S-48FPD-L	48	2 SFP+	LAN Base	740W	Optional
Cisco Catalyst 2960S-48LPD-L	48	2 SFP+	LAN Base	370W	Optional
Cisco Catalyst 2960S-24PD-L	24	2 SFP+	LAN Base	370W	Optional
Cisco Catalyst 2960S-48TD-L	48	2 SFP+	LAN Base	-	Optional
Cisco Catalyst 2960S-24TD-L	24	2 SFP+	LAN Base	-	Optional
Cisco Catalyst 2960S-48FPS-L	48	4 SFP	LAN Base	740W	Optional
Cisco Catalyst 2960S-48LPS-L	48	4 SFP	LAN Base	370W	Optional
Cisco Catalyst 2960S-24PS-L	24	4 SFP	LAN Base	370W	Optional
Cisco Catalyst 2960S-48TS-L	48	4 SFP	LAN Base	-	Optional
Cisco Catalyst 2960S-24TS-L	24	4 SFP	LAN Base	-	Optional
Cisco Catalyst 2960S-48TS-S	48	2 SFP	LAN Lite	-	No
Cisco Catalyst 2960S-24TS-S	24	2 SFP	LAN Lite	-	No

Cisco FlexStack

Cisco FlexStack provides stacking of up to four 2960-S switches through an optional module (Figure 2).

The FlexStack stack module is hot-swappable and can be added to any Cisco Catalyst 2960-S switch with LAN Base software. Switches connected to a stack will automatically upgrade to the stack's Cisco IOS Software version and transparently join the stack without additional intervention.

Cisco FlexStack and Cisco IOS Software provide true stacking, with all switches in a stack acting as a single switch unit. FlexStack provides a unified data plane, unified configuration, and single IP address for switch management. The advantages of true stacking include lower total cost of ownership and higher availability through simplified management and cross-stack features including EtherChannel, SPAN, and FlexLink. Note that cross-stack features must be disabled before removing the stack module from an active stack member switch.

FlexStack also allows mixed stacking: 2960-S and 2960-SF switches can be combined to provide a combination of Gigabit and Fast Ethernet ports in a single switch stack.

Figure 2. Cisco FlexStack Switch Stack

Power over Ethernet Plus - PoE+

Cisco Catalyst 2960-S switches support both IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at PoE+ (up to 30W per port) to deliver lower total cost of ownership for deployments that incorporate Cisco IP phones, Cisco

Aironet® wireless access points, or other standards-compliant PoE/PoE+ end devices. PoE removes the need to supply wall power to PoE-enabled devices and eliminates the cost of adding electrical cabling and circuits that would otherwise be necessary in IP phone and WLAN deployments. Table 2 shows the total PoE/PoE+ power available in each 2960-S model.

Table 2. Switch PoE and PoE+ Power Capacity

Switch Model	Maximum Number of PoE+ (IEEE 802.3at) Ports*	Maximum Number of PoE (IEEE 802.3af) Ports*	Available PoE Power
Cisco Catalyst 2960S-48FPD-L	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960S-48LPD-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960S-24PD-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960S-48FPS-L	24 ports up to 30W	48 ports up to 15.4W	740W
Cisco Catalyst 2960S-48LPS-L	12 ports up to 30W	24 ports up to 15.4W	370W
Cisco Catalyst 2960S-24PS-L	12 ports up to 30W	24 ports up to 15.4W	370W

* Intelligent power management allows flexible power allocation across all ports.

Network Security

The Cisco Catalyst 2960-S Series Switches provide a range of security features to limit access to the network and mitigate threats, including:

- Features to control access to the network, including Flexible Authentication, 802.1x Monitor Mode, and RADIUS Change of Authorization
- Cisco SXP to simplify security and policy enforcement throughout the network
- Threat defense features including Port Security, Dynamic ARP Inspection, and IP Source Guard
- IPv6 First-Hop Security to protect against rogue router advertisements, spoofing, and other risks introduced by IPv6

For more information about Cisco security solutions, visit http://www.cisco.com/go/trustsec.

Enhanced Quality of Service

The Cisco 2960-S Series Switches offers intelligent traffic management that keeps everything flowing smoothly. Flexible mechanisms for marking, classification, and scheduling deliver superior performance for data, voice, and video traffic, all at wire speed. Primary QoS features include:

- Four egress queues per port and strict priority queuing so that the highest priority packets are serviced ahead of all other traffic
- Shaped Round Robin (SRR) scheduling and Weighted Tail Drop (WTD) congestion avoidance
- Flow-based rate limiting and up to 64 aggregate or individual policers per port
- 802.1p class of service (CoS) and differentiated services code point (DSCP) field classification, with marking and reclassification on a per-packet basis by source and destination IP address, MAC address, or Layer 4 TCP/UDP port number
- Cross-stack QoS to allow QoS to be configured across a stack of 2960-S switches

Cisco Catalyst SmartOperations

Cisco Catalyst SmartOperations is a comprehensive set of capabilities that simplify LAN planning, deployment, monitoring, and troubleshooting. Deploying SmartOperations tools reduces the time and effort required to operate the network and lowers total cost of ownership (TCO).

- **Cisco Smart Install** enables zero-touch deployment by providing automated Cisco IOS Software image installation and configuration when new switches are connected to the network.
- **Cisco Auto Smartports** enables automatic configuration of switch ports as devices connect to the switch, with settings optimized for the device type.
- **Cisco Smart Troubleshooting** is an extensive array of diagnostic commands and system health checks within the switch, including Smart Call Home.

For more information about Cisco Catalyst SmartOperations, visit http://www.cisco.com/go/smartoperations.

Cisco EnergyWise

Cisco EnergyWise empowers IT teams to measure and manage the power consumed by devices connected to the network, providing measurable energy savings and reduced greenhouse gas emissions. EnergyWise policies can be used to control the power consumed by PoE-powered endpoints, desktop and data-center IT equipment, and a wide range of building infrastructure. EnergyWise technology is included on all Cisco Catalyst 2960-S Series Switches.

For more information about Cisco EnergyWise™, visit http://www.cisco.com/go/energywise.

Network Management

The Cisco Catalyst 2960-S Series Switches offer a superior CLI for detailed configuration and administration. 2960-S switches are also supported in the full range of Cisco network management solutions.

Cisco Prime Infrastructure

Cisco Prime™ network management solutions provide comprehensive network lifecycle management. Cisco Prime Infrastructure provides an extensive library of easy-to-use features to automate the initial and day-to-day management of your Cisco network. Cisco Prime integrates hardware and software platform expertise and operational experience into a powerful set of workflow-driven configuration, monitoring, troubleshooting, reporting, and administrative tools.

For detailed information about Cisco Prime, visit http://www.cisco.com/go/prime.

Cisco Network Assistant

A PC-based network management application designed for small and medium-sized business (SMB) networks with up to 250 users, Cisco Network Assistant offers centralized network management and configuration capabilities. This application also features an intuitive GUI where users can easily apply common services across Cisco switches, routers, and access points.

For detailed information about Cisco Network Assistant, visit http://www.cisco.com/go/cna.

Software Features

Cisco Catalyst 2960-S Series Switches are available with the LAN Base and LAN Lite feature sets. LAN Lite models provide reduced functionality and scalability for small deployments with basic requirements.