UNIVERSIDAD NACIONAL DE INGENIERÍA

RECINTO UNIVERSITARIO SIMÓN BOLIVAR

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

DEPARTAMENTO DE SISTEMAS DIGITALES Y TELECOMUNICACIONES

MONOGRAFIA PARA OPTAR AL TÍTULO DE:

INGENIERO DE TELECOMUNICACIONES

Título:

“IMPLEMENTACION DE LA TECNOLOGIA MPLS EN EL EMULADOR GNS3 CON PROPOSITOS ACADEMICOS”

Autores:

- **Br. Juan Francisco Fuentes Martínez Carnet 2011-39390**
- **Br. Rene José Antonio Guido Carnet 2010-35259**

Tutor: Ing. Marlovio José Sevilla Hernández

Managua, Nicaragua

Diciembre 2018

Dedicatoria

En primer lugar, dedicamos esta tesis monográfica a Dios por la fuerza y sabiduría que nos brindó para poder culminar este trabajo.

Posteriormente dedicamos esta tesis monográfica a nuestras familias quienes nos han apoyado a lo largo de todo este tiempo de manera constante, incondicional y desinteresada para poder terminar este trabajo.

Finalmente dedicamos este trabajo a todas las personas involucradas que nos apoyaron de distintas maneras directa e indirectamente quienes nos ayudaron a culminar este trabajo de tesis monográfica.

Con mucho aprecio:

Juan Fuentes y Rene Guido.

Agradecimientos

Agradezco primeramente a Dios por haberme permitido gozar de excelente salud y sabiduría para lograr terminar de manera satisfactoria mi carrera, a mis padres y familiares por haberme brindado el apoyo incondicional durante todo mi trayecto de formación personal. A mis amigos que siempre tuvieron una broma que decir para levantarme el ánimo y evitar el estrés. También a mi tutor y mi compañero de tesis por la paciencia que me han tenido.

-*Juan Francisco Fuentes Martínez*

En primer lugar, doy gracias a Dios por haberme mostrado el camino y haberme dado la voluntad y energía para culminar mis estudios. En segundo lugar, agradezco a mi familia quienes siempre me han apoyado económicamente y espiritualmente para continuar mis estudios, en especial agradezco a mi abuela quien ha sido la mayor responsable de que haya continuado y terminado la carrera de ingeniería. En último lugar, pero no menos importante agradezco a mi compañero de tesis quien junto a nuestro tutor han estado constantemente trabajando, motivando y presionando para lograr este pasó final.

-Rene José Antonio Guido

Resumen

El presente documento monográfico abarca de manera teórica y practica las tecnologías BGP, OSPF y MPLS. Además, se incluye la aplicación de MPLS-VPN. La monografía está estructurada de tal manera que primero se estudia de manera teórica las distintas tecnologías abarcando su funcionamiento, características y lógica de aplicación a través de los comandos. El primer capítulo consta de los conocimientos básicos de redes, el segundo capítulo abarca el protocolo OSPF tanto en un área como en múltiples áreas, el tercer capítulo es sobre el protocolo BGP y el ultimo capitulo abarca MPLS incluyendo la aplicación MPLS-VPN, en este último capítulo se enseña la teoría y la convergencia de MPLS, BGP y OSPF. Para las prácticas se diseñaron cuatro guías de laboratorio que están ubicadas al final de cada capítulo, siendo dos guías para OSPF, una guía para BGP y una guía para MPLS. En anexos se incluye dichas guías ya resueltas, donde se explica a detalle la lógica de cada comando.

Lista de Figuras

Lista de Tablas

Lista de Acrónimos

MPLS: Multiprotocol Label Switching
ISP: Internet Service Provider
UNI: Universidad Nacional de Ingeniería
OSPF: Open Shortest Path First
BGP: Border Gateway Protocol
TCP/IP: Transmission Control Protocol/Internet Protocol
VPN: Virtual Private Network
DHCP: Dynamic Host Configuration Protocol
RFC: Request for Comments
LSA: Link-State Advertisement
LSDB: Link-State Database
SPF: Shortest Path First
DR: Designate Router
BDR: Back Up Designate Router
DBD: Data Base Description
GNS3: Graphical Network Simulator Version 3
WAN: Wide Area Network
IOS: Internet and Operating System
FEC: Facultad de Electrotecnia y Computación
FEC: Forwarding Equivalence Class
EDGE: Enhanced Data for GSM Evolution
CISCO: Empresa estadounidense que se dedica a la creación de sistemas y routers, switches y hubs y su enseñanza.
LAN: Local Área Network
OSI: Open Systems Interconnection
QoS: Quality of Service
IPV4: Internet Protocol version 4
IPV6: Internet Protocol version 6
IETF: Internet Engineering Task-Force
VLAN: Virtual Local Area Network
MAC: Media Access Control
ID: Identificador
InterNIC: Internet Network Information Center
IANA: Internet Assigned Numbers Authority
CIDR: Classless Inter-Domain Routing
VSLM: Variable Stripe Length Method
CCNA: Cisco Certified Network Associate
CCNP: Cisco Certified Network Professional
CPU: Central Processing Unit
NBMA: Non-Broadcast Multiple Access
LSR: Link State Request
LSU: Link State Update
LSAck: Link State Acknowledgements
ABR: Area Border Routers

ASBR: Autonomous System Boundary Routers

CEF: Cisco Express Forwarding

RFC: Remote Function Call

NSSA: Not So Stubby Área

MD5: Message Digest 5

AS: Autonomous System

NLRI: Network Layer Reachability Information

EBGP: External Border Gateway Protocol

IBGP: Interior Border Gateway Protocol

IGP: Interior Gateway Protocol

ATM: asynchronous time-division multiplexing

TTL: Time to Live

TDP: Tag Distribution Protocol

LDP: Label Distribution Protocol

MTU: Maximum Transmission Unit

UDP: User Datagram Protocol

ACL: Access Control List

PE: Provider Edge

RD: Route Distinguisher

CE: Client Router

VRF: Virtual Routing and Forwarding Table

LFIB: Label Forwarding Information Base

LIB: Label Information Base

FIB: Forwarding Information Base

LSP: Label Switched Path

PHP: Penultimate Hop Popping

RD: Router Distinguisher

Tabla de Contenido

Introducción

Internet se ha convertido en una herramienta muy popular en los últimos años y esto ha impulsado un gran ritmo de crecimiento de las redes de datos. Con el presente trabajo monográfico titulado: “IMPLEMENTACION DE LA TECNOLOGIA MPLS EN EL EMULADOR GNS3 CON PROPOSITOS ACADEMICOS”, este se desarrollará para optar al título de Ingeniería de Telecomunicaciones.

Hoy en día la tecnología MPLS es la más utilizada por empresas ISP para sus estructuras WAN debido a su alta popularidad, velocidad, seguridad y eficacia. En la carrera de ingeniería de telecomunicaciones que ofrece la Universidad Nacional de Ingeniería, se instruye a los estudiantes sobre las diferentes ramas de redes de datos, la cual se imparte parcialmente en la clase de redes de computadoras II y redes telefónicas II. Cuando decimos parcialmente nos referimos a que solo se da la componente teórica en el caso de MPLS.

Como estudiantes egresados somos conscientes de las limitaciones que conlleva esto en el plano profesional, donde carecer de conocimiento práctico en la configuración de estas tecnologías en los diferentes equipos, realizando mención en la marca CISCO debido a que esta ofrece un programa de formación y estudio continuo. Elaboramos cuatro guías de laboratorio que sirven como herramientas para la efectividad en el modelo de enseñanza y aprendizaje a los futuros ingenieros en situaciones que conlleven la utilización de conocimientos de redes de datos.

Actualmente en Nicaragua, se están desarrollando proyectos para el despliegue de redes de banda ancha a nivel nacional, lo que tendrá un gran impacto para la población en cuanto a la modernización de la tecnología en el país. Por tanto, se cuenta con la infraestructura necesaria en todo el país, para que las empresas puedan interconectar sus sucursales geográficamente distantes, mediante el uso de redes MPLS, que permitirán la escalabilidad, óptimo desempeño y seguridad para el intercambio de información mediante el uso de VPN (Virtual Private Network). A

fin de demostrar los diferentes beneficios de la implementación de VPN MPLS, se procedió a la recopilación de información acerca de la tecnología MPLS, que permitió definir los requerimientos técnicos necesarios para realizar el diseño y emulación de una red MPLS, tales como: equipos que se deben emplear, comandos necesarios para su configuración. Para esto nosotros utilizamos la herramienta de emulación GNS3.

Estas cuatro guías servirán para las practicas de la materia de redes de computadoras II y redes telefónicas II con la ayuda del emulador GNS3. Esta herramienta nos permitió emular los IOS de los routers CISCO que son necesarios para crear redes WAN y emular las configuraciones que sean necesarias en estos equipos, esto ayuda al estudiante a experimentar simulando prácticas profesionales en un ambiente académico, tomando en cuenta los objetivos de la asignatura Redes de Computadoras II, que cada vez tiene mayor número de aplicaciones en situación de campo profesional.

Objetivo General

- Contribuir a la mejora del proceso de enseñanza-aprendizaje mediante la implementación de prácticas de laboratorio que faciliten la comprensión de los estudiantes de ingeniería de Telecomunicaciones en el área de redes de computadoras II haciendo uso de la tecnología WAN-MPLS.

Objetivos Específicos

- Elaborar guías de laboratorio donde se evidencie la utilización del software GNS3, por medio de la tecnología MPLS.

- Desarrollar topologías WAN que permitan a los alumnos el análisis y compresión de la tecnología MPLS.

- Utilizar el Router Cisco 7200 por ser la versión de IOS más reciente en el emulador GNS3 para la realización de dichas guías.

- Diseñar estructuras de red ISP, que le permitan a los estudiantes analizar y dar soluciones viables para la elaboración de una red WAN.

Justificación

Actualmente, en la carrera de Ingeniería de Telecomunicaciones se aborda el tópico de tecnologías WAN y protocolo de enrutamiento de gateway exterior (BGP). No obstante, se carece de la componente experimental o de laboratorio. Por tal motivo, desarrollamos 4 prácticas de laboratorio para contribuir a la mejorar del proceso de enseñanza-aprendizaje en los estudiantes de ingeniería de esta disciplina. Estas guías se plantean desarrollar con ayuda de la herramienta computacional GNS3 es uno de los emuladores más utilizados para estos fines. Sin embargo, al no tener antecedentes de guías de laboratorio sobre este tema, las mismas fueron hechas de forma tal que faciliten la comprensión y análisis para los estudiantes.

El uso de redes MPLS (Protocolo de Conmutación de Etiquetas) se ha convertido en una de las mejores soluciones a la creciente demanda de conectividad, trae consigo múltiples beneficios como: calidad de servicio, mejor ancho de banda y seguridad en el establecimiento de conexión punto a punto para clientes. La tecnología MPLS brinda soluciones de conectividad para empresas y clientes masivos, aprovechando las infraestructuras de redes desplegadas por los ISP (Internet Service Provider); las cuales pueden establecer enlaces dedicados mediante el uso VPN y redes virtuales que permitan el intercambio de información de manera segura por medio de arquitecturas de redes públicas.

Este documento permite conocer acerca del funcionamiento de las redes MPLS, cómo se configuran y la cantidad de beneficios que traen consigo, entre ellos está, el establecimiento de parámetros de seguridad mediante el uso de VPN a nivel lógico. También se mencionará como MPLS trabaja en conjunto con los protocolos de enrutamiento dinámico BGP Y OSPF sobre redes WAN (Wide Area Network), para garantizar la fiabilidad y privacidad en el envío y recepción de datos. Cabe destacar que con este estudio se contribuye en el desarrollo del conocimiento de los profesionales especializados en redes datos, cuentan con los detalles de cómo los ISP logran integrar múltiples servicios como voz, video y datos sobre una infraestructura de red para empresas y particulares.

Esta investigación se encuentra relacionada con las siguientes carreras de la FEC: computación, telecomunicaciones y electrónica en los campos de redes de datos, redes de computadoras y redes telefónicas. Dichos conocimientos son aplicados mediante el desarrollo de prácticas de laboratorio y la utilización de comandos de cisco por medio de las emulaciones en GNS3.

Planteamiento del Problema

Las redes MPLS son las más utilizadas tanto a nivel nacional como internacional, esta tecnología es la de más rápidas, seguras y robustas que se pueden implementar en redes WAN.

Estas redes WAN con tecnología MPLS presentan un comportamiento robusto y eficiente ante su aplicación en las telecomunicaciones, por lo tanto, es necesario que los profesionales tengan dentro de su formación la enseñanza de esta tecnología tanto a nivel teórico como practico para su compresión y que los profesionales tengan la capacidad de desempeñarse con este conocimiento en el ámbito laboral. Actualmente en la UNI se cubre las necesidades teóricas de la enseñanza de esta tecnología presentando cierta debilidad en el ámbito práctico.

Cabe señalar que la deficiencia de la enseñanza práctica, es decir, prácticas de laboratorio no se pueden llevar a cabo debido al alto costo de los equipos CISCO para redes WAN que utilizan MPLS. Teniendo en cuenta esta serie de antecedentes, nosotros elaboramos 4 guías de laboratorio sobre MPLS que pueden ser ejecutadas en un ambiente virtual.

Marco Teórico

Capítulo 1- TCP-IP (Transmission Control Protocol/Internet)

¿Qué es una red?

La primera tarea es definir qué una red, como se construye y comprender como es utilizada en los ámbitos profesionales y empresariales. Una red conecta una colección de equipos y sistemas, como computadoras y servidores. Que pueden comunicarse entre ellos. Esta transporta datos en todo tipo de ambientes, incluyendo casas, pequeños negocios y grandes compañías. En estas un número de locaciones necesitan comunicarse entre ellas, las cuales pueden describirse de la siguiente manera.

Oficina Principal: Es donde todos están conectados a la red, y se almacena la información corporativa. Es un lugar que puede tener muchas personas que dependen de la red para tener accesos a sus trabajos.

Ubicaciones Remotas: Es una variedad de locaciones con acceso remoto que utiliza la red para conectarse con la oficina principal o entre ellas.

- Sucursal: Son pequeños grupos de trabajo que se comunican entre ellos por medio de la red. Sin embargo en algunas compañías la información es almacenada estos lugares.
- Oficina en Casa: Las personas que trabajan en casa requieren que exista conexión hacia la oficina principal o sucursales para tener acceso a la información contenida en los servidores.
- Usuarios Móviles: Estos usuarios se pueden conectar en la oficina principal, sucursal o viajando. La red de acceso para usuarios móviles está basada en donde se encuentra localizado el usuario.

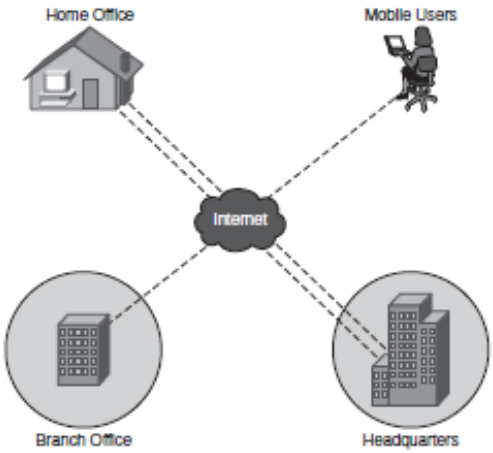


Figura 1 Ubicación de la Red

Existen diferentes tipos de redes y locaciones. Estas pueden ser utilizadas en casa u oficinas para comunicarse vía internet, para localizar información, realizar pedidos, comprar mercadería y enviar mensajes a tus amigos. Si se trabaja en una oficina pequeña que tiene configurada una red para conectar computadoras e impresoras. Así como su uso en grandes empresas con muchas computadoras, impresoras, dispositivos de almacenamiento, servidores que almacenan información de otros departamentos geográficamente distantes.

Características de una Red

Algunas características son usadas frecuentemente para describir y comparar varios diseños de red. Cuando se está determinando como construir una red.

Las redes pueden describirse y compararse de acuerdo a su funcionamiento y estructura, como:

- *Velocidad:* Esta depende de la velocidad con la que los datos son transmitidos a través de la red.

- *Costo:* Este indica en general el costo de los componentes. Como lo es la instalación y el mantenimiento de la red.

- *Seguridad:* indica que tan segura es una red, incluyendo los datos trasmitidos sobre esta.

- *Disponibilidad:* Se mide como la probabilidad en la que una red puede estar disponible para usarse cuando sea requerido. Para redes que se supone son utilizadas 24 horas al día, 7 días a la semana, 365 días al año. Esta disponibilidad es calculada dividiendo el tiempo que actualmente se encuentra disponible entre el tiempo total en el año por 100 para obtener el porcentaje.

  [(Numero de minutos en el año-tiempo de caída)/ (Numero de minutos en el año)]*100=Porcentaje de disponibilidad.

  Supongamos que una red tiene una indisponibilidad de 40 minutos al año, por interrupciones en la red. Este porcentaje puede ser calculado de la siguiente manera:

  [(525600-40)/ (525600)]*100=99.9923

- *Escalabilidad***:** Esta indica como la red se puede acomodarse para agregar más usuarios y requerimientos de transmisión de datos. Si una red es diseñada y optimizada para ciertos requerimientos. Reunir nuevos requerimientos para el crecimiento de la red podría elevar los costos, además de presentar un grado alto de dificultad para su implementación.

- *Confiabilidad:* Es indicada de acuerdo a los componentes (Routers, Switches, PCs, etc.) los cuales forman la red.

- *Topología:* Las redes tienen dos tipos topologías: Topología Física, los cuales son arreglos de cableado, dispositivos de red y dispositivos terminales. La topología lógica, es la trayectoria que toma las señales de datos a través de la topología física.

Diferencias entre topologías lógicas y físicas:

Para construir una red confiable y escalable depende de las topologías lógicas y físicas. Topología se define como un método de interconexión utilizado entre dispositivos, incluyendo diseño de cableado, la ruta principal y respaldo utilizadas para la transmisión de datos.

Las topologías físicas de red, refieren al diseño físico y cableado. Se debe de elegir la topología física apropiada para el tipo de cableado que se va a instalar. Por lo tanto entender el tipo de cableado utilizado es importante para saber el tipo de topología física. Estas son las tres categorías primarias de las topologías físicas.

- Bus: Computadoras e otros dispositivos de red cableados juntos en una línea.
- Ring: Computadoras e otros dispositivos de red cableados juntos, con el ultimo equipo conectado con el primero para formar un circulo.
- Star: Un dispositivo de cableado central conecta las computadoras e otros dispositivos. Esta categoría incluye topología de estrella y estrella extendida.

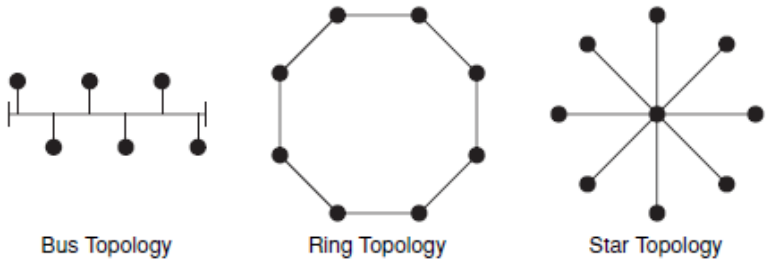


Figura 2 Topología Lógica

La topología lógica en una red que se refiere a la trayectoria de señales utilizadas para viajar de un punto a otro en la red.

Las topologías físicas y lógicas en una red pueden ser las mismas. Por ejemplo, en una topología formando un bus lineal, los datos viajan a lo largo de la longitud del cable. Por lo tanto, la red tiene dos topologías de bus una física y una lógica.

Por otra parte, una red puede tener ciertas diferencias entre topologías lógicas y físicas. Por ejemplo, una topología física en forma de estrella, en cuales segmentos del cable conecta todas las computadoras al hub central, pueden tener una topología de anillo lógica. Recordemos que, en un anillo, los datos viajan de una computadora hacia otra, dentro del hub, la conexión del cableado es tal que la señal actual viaje alrededor en el círculo de un puerto para el otro. Creando un anillo lógico. Por lo tanto, no se puede predecir siempre como los datos viajan en la red, simplemente observando su diseño fisco.

Topología de estrella es la implementación más común en LANs (Local Area Network) ahora. Ethernet usa topología de bus lineal ya sea en bus físico o estrella física. Un Ethernet hub es un ejemplo de topología física de estrella con una topología lógica de bus.

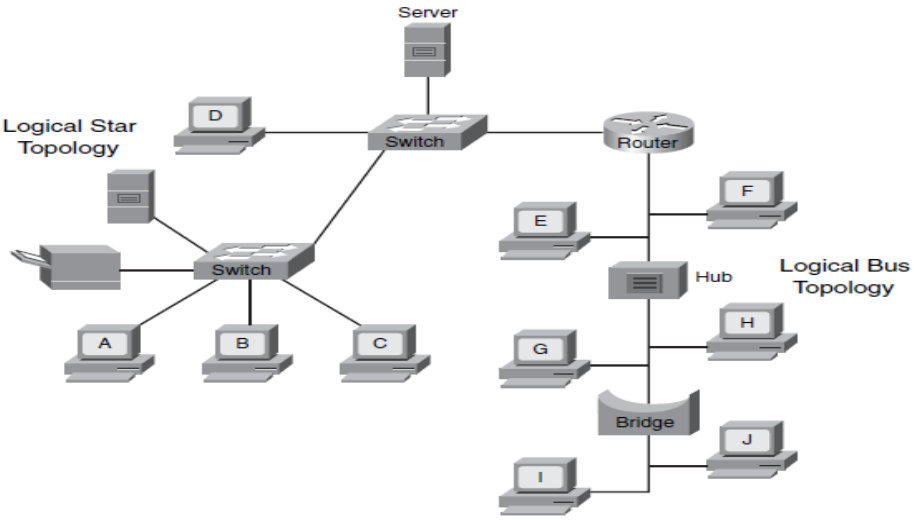


Figura 3 Topología Lógica Común

Modelo OSI

El modelo OSI consta de 7 capas, como se detalla en la imagen. Esta separación de funciones de red es llamada estratificación. Este define las funciones de red en cada capa. Así como facilitar el entendimiento de como la información viaja a través de la

red. Y describir como los datos viajan de una aplicación de programa, a través de una red mediana, para una aplicación localizada en otra computadora.

Aplicación
Presentacion
Sesion
Transporte
Red
Enlace de Datos
Fisica

Tabla 1 Capas del Modelo OSI

Dividir la red en 7 capas provee las siguientes ventajas:

- Reduce Complejidad. Esta particiona una red de comunicación en pequeñas simples partes.
- Interfaz estandarizada. Estandariza los componetes de red para permitir a los vendedores el desarrollo y soporte.
- Facilita ingeniería modular. Permite que diferentes tipos de equipos de red y software puedan comunicarse entre ellos.
- Asegura la interoperabilidad de las tecnologías. Previene que se realicen cambios en una capa que pueda afectar a las siguientes.
- Acelera la evolución. Provee efectivas actualizaciones y mejoras para componentes individuales, sin afectar otros componentes o tener que reescribir el protocolo completo.

Las 7 capas del modelo OSI se pueden describir de la siguiente Manera:

Capa 7: Capa de aplicación

La aplicación es la capa que está más cerca del usuario. Esta provee servicios de red para el usuario en aplicaciones.

Capa 6: Capa de presentación

La presentación asegura que la información de la capa de aplicación de un sistema se envié de manera confiable con la capa de aplicación de otro sistema.

Capa 5. Capa de sesión

La capa de sesión estableces, administra y termina sesiones entre 2 host. Este provee el servicio de la capa de presentación. Se encarga de sincronizar dialogo entre la capa de presentación entre los 2 host y administrar el intercambio de datos.

Capa 4. Capa de transporte

La capa de transporte segmenta los datos del sistema del host emisor y los vuelve a armar en una secuencia de datos en el sistema de host receptor. Esta capa trata de proveer un servicio de transporte de datos que proteja a las capas superiores para transportar detalles de implementación. La fiabilidad del transporte entre dos host, son la preocupación de esta capa. Así como establecer, mantener y terminar correctamente circuitos virtuales.

Capa 3. Capa de Red

La capa de red provee conectividad y selección de ruta entre dos sistemas de host los cuales pueden estar localizados en redes geográficamente separadas.

Capa 2. Capa de enlace de datos

La capa de enlace de datos se define como los datos son formateados para la transmisión y como se controla la red. Esta capa es responsable de definir como los dispositivos en un medio común puedan comunicarse con otros.

Capa 1. Capa física

La capa física define las especificaciones eléctricas, mecánicas, procesales y funcionales para activar, mantener y detectar links físicos entre los sistemas terminales. Comunicación Peer to Peer

El protocolo TCP/IP

El protocolo TCP/IP es un modelo de capas similar al modelo de referencia OSI. Este nombre es una combinación de dos protocolos individuales. Transmission Control Protocol (TCP) e Internet Protocol (IP). Está divido en capas, cada una de estas desempeña una función específica en el proceso de comunicación de datos.
El modelo OSI y el protocolo TCP/IP fueron creados por diferentes organizaciones aproximadamente al mismo tiempo, con el fin de organizar y comunicar componentes que guíen la transmisión de datos.

El protocolo TCP/IP se divide en las siguientes capas.

Aplicación
Transporte
Internet
Red

Tabla 2 Protocolo TCP/IP

El protocolo TCP/IP tiene 4 capas. Nótese que algunas capas en el protocolo TCP/IP tienen el mismo nombre que las capas del modelo OSI. Pero las Capas tienen diferentes funciones:

Capa de aplicación: La capa de aplicación se encarga de los protocolos de alto nivel, facilitando la representación, codificación y el control de dialogo. Este modelo

combina todas las aplicaciones en una capa y se encarga de revisar si la información se empaqueto adecuadamente para enviarla a la siguiente capa.

Capa de transporte: La capa de transporte se ocupa de los problemas de QoS, confiabilidad, Control de flujo y corrección de errores. Uno de estos protocolos, TCP, provee una conexión de red confiable.

Capa de internet: El propósito de la capa de internet es enviar datagramas desde su origen hacia cualquier red en el Internet y luego llegar a su destino.

Capa de Red: Esta incluye los protocolos LAN y WAN y todos los detalles del modelo OSI en su capa física y enlace de datos.

Modelo OSI y Protocolo TCP/IP

Similitudes entre el protocolo TCP/IP y el modelo OSI.

- Los dos tienen capa de aplicación, Sin embargo incluyen diferentes servicios.
- Los dos poseen capa de transporte y red.
- Los dos aceptan tecnología de conmutación de paquetes.

Sus diferencias

- TCP/IP combina las capas de presentación y sesión en la capa de aplicación.
- TCP/IP combina las capas de enlace de datos y física, en la capa de Red.

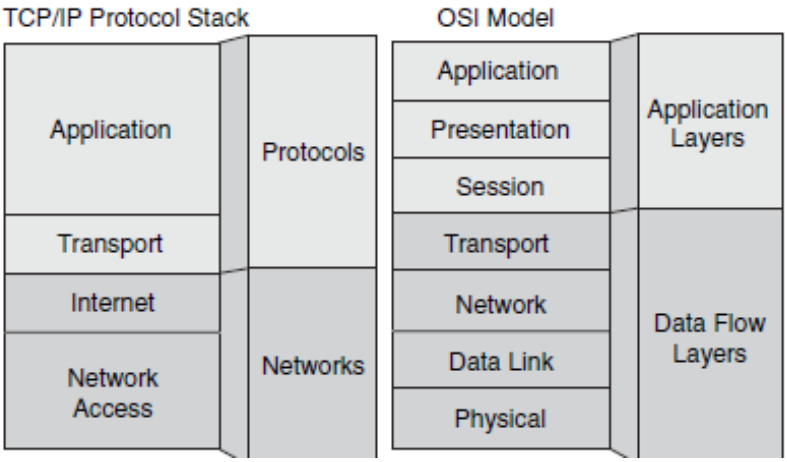


Figura 4 Modelo OSI & TCP/IP

Entendiendo TCP/IP capa de Internet

El protocolo TCP/IP incluye la capa de red y transporte. La capa de internet se encarga del ruteo de paquetes de datos utilizando direcciones IP para identificar el dispositivo en la red. Estos dispositivos pueden ser computadoras, routers, impresoras entre otros que pertenezcan a la red y tengan su propia dirección IP.
Cada dirección IP tiene una estructura específica, existen varias clases de direccionamiento IP. Adicionalmente las subredes y el subneteo tienen un rol importante en direccionamiento IP, y diferentes funciones de ruteo y protocolos involucrados en la transmisión de datos de una red hacia otra utilizando direcciones IP.

Existen dos tipos de direcciones: IP Versión 4 (IPV4) e IP versión 6 (IPV6). El direccionamiento IPV4 de 32 bits actualmente es el más utilizado, Pero el direccionamiento IPV6 de 128 bits está siendo utilizado en menor escala. Se espera que en futuro este desplace al protocolo IPV4, debido al agotamiento de direcciones IP.

Direccionamiento de Red IP

Las direcciones son utilizadas para identificar lugares específicos como hogares y negocios, este mensaje puede ser alcanzado eficientemente. Si se usa una dirección IP para identificar un equipo específico en una red, que puede enviar datos de manera correcta hacia otras localidades. El direccionamiento IP posee varios aspectos, incluyendo el cálculo para la construcción de una dirección IP. Las clases de direccionamiento IP esta designadas para un propósito de ruteo determinado y direccionamiento IP publico contra el privado.

El encabezado de la capa de internet del protocolo TCP/IP es conocido como encabezado IP. Se demuestra de la siguiente manera:

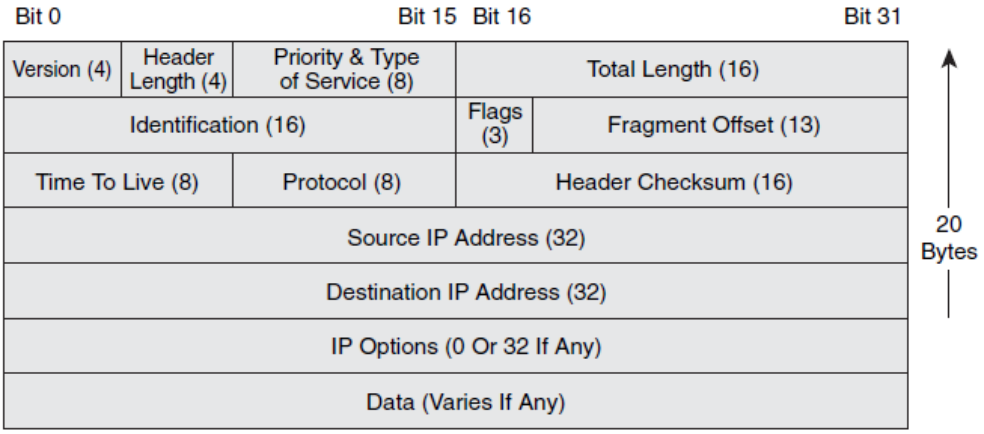


Figura 5 Encabezado IP

Nótese que cada datagrama IP lleva este encabezado, el cual incluye una dirección IP origen y una de destino, la cual identifica la de red de origen y destino del usuario.

La jerarquía del direccionamiento IP consiste en:

- Los bits de orden superior a la izquierda especifican el componente de dirección de red (Network ID) de la dirección.
- Los bits de orden inferior o derecha especifican el componente de dirección de host (ID Host) de la dirección.

Cada LAN física o virtual en una red interna corporativa, vista como una red única que debe alcanzarse antes de que un usuario dentro de la empresa pueda conectarse a esta. Cada LAN tiene un direccionamiento de red único. Los host que pertenecen a la red comparten los mismos bits, pero cada uno de estos es identificado por la singularidad de los bits restantes.

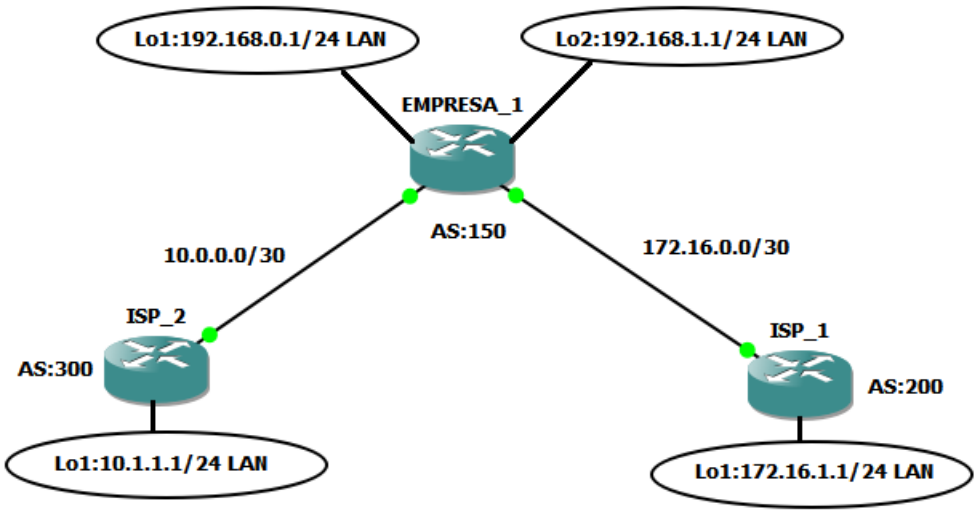


Figura 6 Esquema de red en GNS3

Las direcciones IP poseen una longitud de 32bits y son de naturaleza binaria, pero están expresadas en un formato fácil de comprender. Los 32bits se dividen en cuatro secciones de 8bits cada uno, las cuales se conocen como octetos o bytes. Cada uno de estos octetos es convertido en números decimales entre 0 y 255, cada uno de ellos están separados por puntos del siguiente.

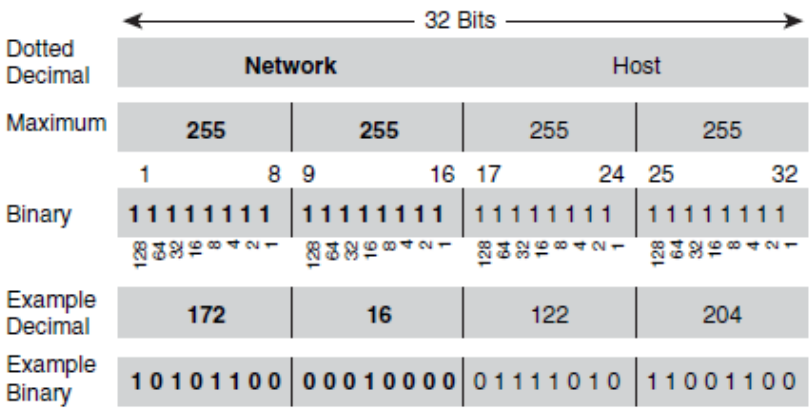


Figura 7 Formato de Direccionamiento IP

El formato de direccionamiento IP, es conocido como notación decimal punteada. Como se muestra en la figura anterior.

- Ejemplo de dirección: 172.16.0.0
- Cada bit en el octeto tiene un valor binario (Puede ser 128, 64, 32, 16, 8, 4,2 y 1), cuando todos los btis se encuentran en 1, la suma es de 255.
- El valor decimal mínimo para un octeto es 0; contiene todos bits en 0.
- El valor decimal máximo para un octeto es 255, contiene todos en 1.

Clases de direccionamiento IP

Cuando IP fue desarrollado por primera vez, no existían clases de direccionamiento, debido a que se asumió que 254 redes, iban a ser suficiente para la inter-network académico, militar e investigaciones de computadora. Cuando el número de redes fue incrementando, las direcciones IP fueron divididas en categorías llamadas clases para acomodar los diferentes tamaños de redes y ayudar a identificarlas.

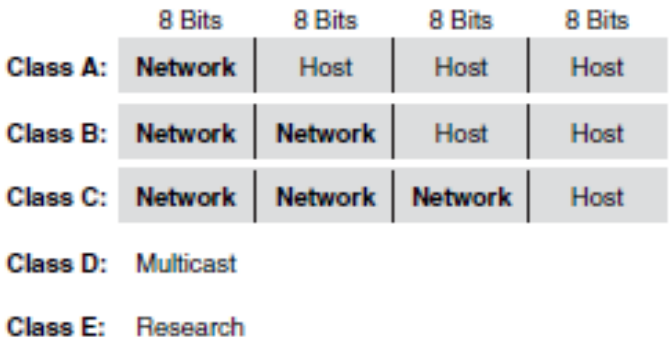


Figura 8 Clases de Direccionamiento

Se cuenta con 5 tipos de clases de direccionamiento IP, las cuales son:

Clase A: Esta fue diseñada para soportar extremadamente largas redes. La clase de direccionamiento A, usa solo el primer octeto para indicar direccionamiento de red. El restante de los tres octetos es utilizado parar direcciones de host.

Clase B: Esta fue diseñada para soportar un moderado largo y tamaño de redes. La clase de direccionamiento B usa 2 de los 4 octetos para indicar direccionamiento de red. Los otros octetos especifican direccionamiento de host.

Clase C: Esta categoría es las más utilizada para direccionamiento de clases. Esta intenta soportar un gran número pequeñas redes.

Clase D: Esta fue creada para habilitar multicasting en direccionamiento IP. Una dirección multicast es una única dirección de red que direcciona paquetes con una dirección de destino a un grupo predeterminado de direcciones IP.

Clase E: Este clase está definida por la Internet Engineering Task-Force (IETF), reserva direcciones en esta clase para sus propias investigaciones.

Direccionamiento Clase A	Direccionamiento Clase B	Direccionamiento Clase C
El primer bit es 0	Los primeros bits son 10	Los primeros 3 bits son 100
Rango de números de redes: 1.0.0.0 a 126.0.0.0	Rango de números de redes: 128.0.0.0 a 191.255.0.0	Rango de números de redes 192.0.0.0 a 233.255.255.0
Numero de posibles Redes:127 (1 a 126 son utilizables, 127 está reservada)	Numero de posibles redes: 16384.	Numero de posibles redes:2,097,152
El número de valores posibles para partición de host: 16, 777,216.	El número de valores posibles para partición de host: 65,536.	El número de valores posibles para partición de host: 256.

Tabla 3 Clases de direccionamiento

Direcciones de Red y Broadcast

Ciertas direcciones IP están reservadas y no se pueden asignar a dispositivos individuales en una red. Estas direcciones reservadas incluyen una dirección de red, que identifica la red en sí misma, y la dirección de difusión, que se utiliza para transmitir paquetes a todos los dispositivos en una red.

Una Dirección IP que tiene 0 binario en todas las posiciones bits para host está reservado para la dirección de red. Por ejemplo, una red clase A, 10.0.0.0 es una dirección IP de una red que contiene al host 10.1.2.3 Un Router usa la red direccionamiento IP, cuando este busca en su tabla de rutas la ubicación de la red destino. Un ejemplo de red clase B, la dirección 172.26.0.0 es una dirección de red.

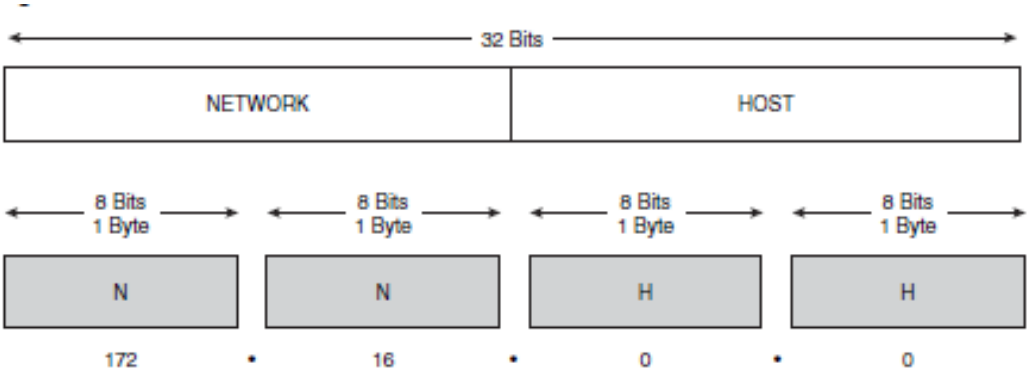


Figura 9 Dirección de Red

Los números decimales que llenan los primeros octetos en la redes de clase B están asignados. Los últimos dos octetos contienen 0, debido a que esos 16 bits son el número de host utilizados para que los dispositivos sean agregado a la red. Por ejemplo la dirección 172.16.0.0 está reservada para la dirección de red. Estaba no debe ser usada como dirección para ningún dispositivo agregados a esta.

La partición de red, de una dirección IP refiere a una ID de Red. Esto es importante, debido que los host en una red solo pueden comunicarse con los dispositivos en la misma red. Si se necesita comunicar equipos con interfaces asignadas para otros ID de red, Dentro de la capa 3. Los equipos pueden enrutar datos entre redes si esto es necesario. Estos eventos ocurren cuando los dispositivos comparten segmento de medios fiscos o VLAN.

Un ID de red habilita al router para poner paquetes en el segmento de red apropiado. El host ID ayuda al router entregar las tramas de capa 2, encapsulando el paquete a un host especifico en la red. Esto como resultado del mapeo de la dirección ip con la dirección MAC. El cual en necesario en el proceso de capa 2 del router para direccionar la trama.

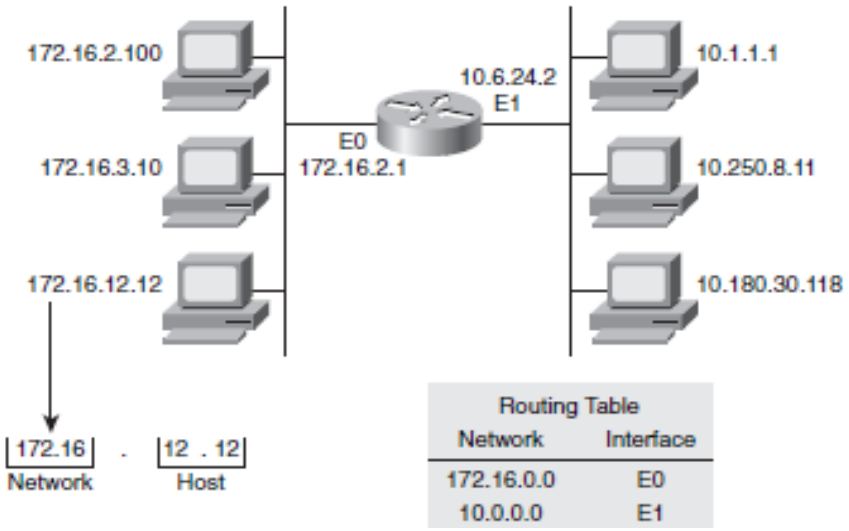


Figura 10 Direcciones de Host

La partición de una red es determinada por clasificación, se puede determinar el número total de host en la red, sumando todas las combinaciones posibles de 1 y 0 de la dirección y luego restar 2. Se debe restar 2 por que la dirección que constituye todos los 0 especifica la red, y la dirección de todos los bits en 1 es usada para la red de broadcasts.

Este puede ser calculado de la siguiente Manera:

2^N-2 (Donde N es el número de bits de la partición de host)

En redes de clase B, los 16 bits son utilizados para la partición de Host. Aplicando la formula 2^N-2 (en este caso, 2^{16}-2=65,534) como resultado se tiene 65,534 direcciones de host utilizables.

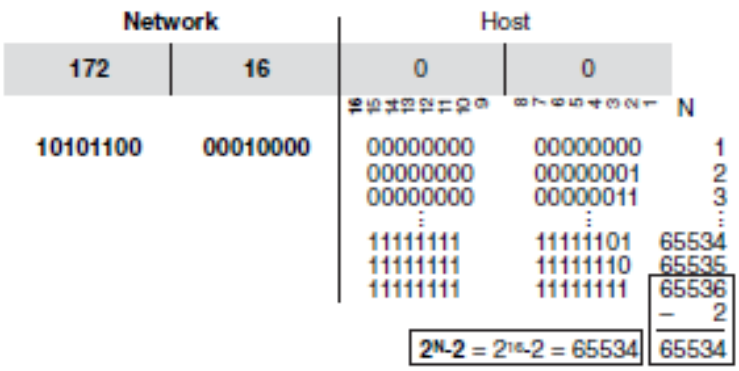


Figura 11 Determinando Direcciones Host Disponibles

En redes de clase C, los primeros 3 octetos son asignados para la red. Dejando el último de estos asignados para los hosts, el número máximo de host es 2^8-2, o 254.

Direcciones IP públicas y privadas

Las redes se conectan entre ellas a través de internet, y otras privadas. El direccionamiento IP públicas y privadas es requerido para los dos tipos de redes. La estabilidad del internet depende de las direcciones de red usada públicamente. Por lo tanto, son necesarios mecanismos para garantizar que las direcciones sean únicas. Esta responsabilidad recae sobre una organización conocida como InterNIC (Internet Network Information Center). Esta organización ha tenido éxito por la IANA (Internet Assigned Numbers Authority). La cual administra el suministro restante de direcciones IPV4, para garantizar que no se dupliquen las direcciones públicas.

Para obtener una dirección IP o bloquear un direccionamiento, se debe de contactar al proveedor de servicio (ISP). Ya que este asigna direcciones IP. Dentro de un rango de direcciones asignado de manera regional, el cual es administrado por IANA, de la siguiente manera.

- Asia Pacific Network Information Center (APNIC)
- American Registry for Internet Numbers (ARIN)
- Reseaux IP Europens Networks Coordination Centre (RIPE NCC)

Con el rápido crecimiento del Internet, las direcciones IP públicas comenzaron a agotarse, por lo que se desarrollaron nuevos esquemas de direccionamiento, como enrutamiento entre dominios sin clases (CIDR) e IPV6. Para solventar el problema.
Los anfitriones de internet requieren un direccionamiento IP global único, los host privados no se conectan a internet, por lo que estos pueden usar cualquier dirección valida, siempre y cuando sea exclusiva dentro de la red privada, ya que se tiene redes privadas junto a redes públicas, cualquier dirección en este rango no se enruta en la red troncal de internet, por tanto la IETF definió 3 bloques de direcciones IP (1 red clase A, 16 redes clases B, 256 redes Clase C) en RFC 1918 para uso interno privado. Como se muestra en la siguiente tabla.

Clases	**RFC 1918 Rango de direcciones**
A	10.0.0.0 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255
C	192.168.0.0 a 192.168.255.255

Tabla 4 Rangos de direccionamiento IP Privados

Comprendiendo la numeración binaria

Todas las computadoras funcionan usando un sistema de conmutación, el que puede ser una de dos posiciones, apagado o encendido, ese llamado sistema binario donde apagado es representado con el digito 0 y encendido con el digito 1.
El direccionamiento de los dispositivos de red, usan este sistema para definir su localización en la red. Una dirección IP está basada en una notación decimal punteada de números binarios. Es necesario tener conocimiento de las propiedades matemáticas del sistema binario para comprender redes. Se describirá como las matemáticas de sistema binario y explicar cómo convertir de decimal (base 10) a binario (base 2) y viceversa.

En el sistema decimal, se tienen los siguientes dígitos son 0,1,2,3,4,5,6,7,8,9, donde) es el valor más alto. Mientras el sistema binario solo tiene dos posiciones 1 o 0.

Numero Decimal	Numero Binario
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

Tabla 5 Números decimales y su notación binaria

Para comprender como números binarios son utilizados en el direccionamiento IP, se debe de comprender el proceso matemático para convertir de decimal a binario y viceversa.

	Calculo	Valor
2^0		1
2^1	2	2
2^2	2*2	4
2^3	2*2*2	8
2^4	2*2*2*2	16
2^5	2*2*2*2*2	32
2^6	2*2*2*2*2*2	64
2^7	2*2*2*2*2*2*2	128

Tabla 6 Múltiplos de 2

Conversión de decimal a binario

Los números decimales pueden ser convertidos a binarios a través de un proceso específico. Como se muestra en la siguiente tabla.

Base exponencial	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Valor	128	64	32	16	8	4	2	1
Numero binario	1	1	0	0	0	0	0	0
Numero decimal	128	64	0	0	0	0	0	0

Tabla 7 Conversión de binario a decimal

11000000= (128*1) + (64*1) + (32*0) + (16*0) + (8*0) + (4*0) + (2*0) + (1*0)
11000000=128+64+0+0+0+0+0+0
11000000=192

Para convertir de números binarios a decimal, es necesario descomponer en notación decimales según la posición con la formula $2^{n,}$ luego de realizar esto se

deberá multiplicar el valor decimal por el valor binario dígase 0 o 1, y luego realizar la sumatoria del resultado, de todas las posiciones que sean uno.

Como calcular máscaras de red

Existen 8 tipos de máscaras de subred validas por octeto. El campo de red siempre es seguido del número de red. Es decir, los bits prestados deben ser el primer bit, comenzando por el bit más significativo del campo de host predeterminado, donde n es el tamaño deseado del nuevo campo de subred. La máscara de subred es la herramienta utilizada por el enrutador para determinar qué bits son bits de enrutamiento (red o subred) y cuáles son bits de host.

Si los ochos bits en un octeto binario son 1. El octeto decimal es equivalente a 255. Esto es porque si 255 es una representación decimal de una red por defecto. En clase A, la máscara de subred por defecto es 255.0.0.0 en decimal, 11111111.00000000.00000000.0000000 en binario, y /8 de manera corta. Todos tienen el mismo significado. Si se toman prestados los tres más importantes del octeto principal de mayor orden (se agrega más 1 a la máscara predeterminada), he incrementa a 224 (128+64+32). Esto se traslada a 255.224.0.0, o 11111111.11100000.00000000.00000000.

Mascaras de subred

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Figura 12 Mascaras de Subred

En el direccionamiento IP, la máscara de subred identifica la información del direccionamiento de red, la cual es necesaria para él envió de paquetes hasta el destinatario final. La máscara de red determina cuales bits de la dirección IP están en la red y subred. **[1]**

Example Class A Address (Decimal):	10.0.0.0
Example Class A Address (Binary):	00001010.00000000.00000000.00000000
Default Class A Mask (Binary):	11111111.00000000.00000000.00000000
Default Class A Mask (Decimal):	255.0.0.0
Default Classful Prefix Length:	/8

Example Class B Address (Decimal):	172.16.0.0
Example Class B Address (Binary):	10010001.10101000.00000000.00000000
Default Class B Mask (Binary):	11111111.11111111.00000000.00000000
Default Class B Mask (Decimal):	255.255.0.0
Default Classful Prefix Length:	/16

Example Class C Address (Decimal):	192.168.42.0
Example Class C Address (Binary):	11000000.10101000.00101010.00000000
Default Class C Mask (Binary):	11111111.11111111.11111111.00000000
Default Class C Mask (Decimal):	255.255.255.0
Default Classful Prefix Length:	/24

Figura 13 Clase A, B, C y sus Máscaras de Red por Defecto

VSLM

Mascara de subred de longitud variable (VSLM). Es el mejor método para subnetear una red de manera eficiente donde se haga uso de todos los bits. Cuando se usa el método clásico de subneteo. En todas las subredes se tiene la misma porción de host, porque todas usan la misma mascara. Lo cual se convierte en ineficiente, Por ejemplo si prestamos 4 bits de una red clase C, tendríamos de resultado 14 subredes disponibles, con 14 host válidos. Donde en conexión wan punto a punto solo son necesarios 1 host configurados en ambos extremos de los enrutadores para garantizar conectividad, con este método se estaría desperdiciando 12 host de la partición, aun con la habilidad de usar NAT y direcciones privadas, lo que se busca es que no se agoten las direcciones IP en un diseño de red. Es donde se le da lugar al método VSLM. **[2]**

Emulador GNS3

Se utilizará el emulador GNS3, para demostrar los múltiples beneficios que ofrece la tecnología MPLS, mediante la emulación de equipos CISCO en dicha plataforma, y realizar una demostración lógica de la topología de red propuesta.

¿Qué es un emulador de redes?

Es una aplicación que permite al usuario administrador de una red, diseñar un sistema de redes entre computadoras, switches, router, impresoras, servidores, etc. Todo esto se realiza en nuestro monitor haciendo conexiones de cables agregando computadoras, y otros periféricos, e interconectándolos entre sí, para luego realizar una prueba virtual de la compatibilidad de nuestra conexión. Estas aplicaciones no solo permiten poner los periféricos y probarlos, sino que también podemos cambiar el tipo de placa de red que tengas (fibra óptica, Ethernet, inalámbrica, etc.), cada una con su respectivo soporte de velocidad, todo esto bien detallado. Además, es

posible configurar por individual a cada periférico con un IP, una máscara, un punto de enlace, etc., todo lo que puedas configurar en una PC normal con una placa de red.

¿Qué es y para qué sirve GNS3?

La herramienta de software GNS3, sirve de gran utilidad para los ingenieros enfocados en el área de redes. Este simulador permite configurar, probar y solucionar problemas de conectividad en redes virtuales y reales y se pueden llevar a cabo en pequeñas y grandes tipologías. **[3]**

Figura 14 GNS3 Logo

¿Qué nos permite GNS3?

GNS3 le permite al diseñador de redes visualizar, planificar y solucionar problemas de red. A través de la interacción gráfica de los diferentes equipos Cisco, los cuales pueden ser emulados por esta herramienta según las especificaciones técnicas requeridas por el proyecto en cuestión. Dicha plataforma puede ser descargada y utilizada de manera gratuita para computadoras tradicionales, lo que permite ampliar la experiencia y capacidades del operario.

¿Por qué usar GNS3?

Debido a que GNS3 es uno de los mejores emuladores gráficos de redes que podemos encontrar actualmente. Para profesionales interesados en las certificaciones de Cisco como el CCNA o CCNP de la parte de routing y switching, Esta herramienta de gran utilidad para el aprendizaje y la resolución de problemas de redes a nivel lógico, por poseer interacción con los diferentes IOS de cisco que asemejan el funcionamiento a un equipo de forma real. La principal característica de GNS3 es que es multiplataforma, podremos usarlo tanto en Microsoft Windows, Linux como en Mac OS X, y todo ello de forma completamente gratuita. **[4]**

Después de haber abordado los aspectos fundamentales de una red MPLS, sus beneficios y su gran utilidad para las redes de datos modernas, así como el establecimiento de la herramienta de software para proceder con la simulación de una red MPLS orientada a la conexión; basándonos en los equipos implementados por Cisco. Donde haremos uso de los router Core Cisco 7200.

Capítulo 2: Protocolo OSPF

El protocolo de enrutamiento OSPF es esencial para poder comprender y configurar MPLS, por lo cual es necesario su estudio.

OSPF (Open Shortest Path First) es un protocolo de enrutamiento estándar definido en la RFC 2328. Utiliza el algoritmo SPF (Shortest Path First) para encontrar las mejores rutas hacia los diferentes destinos y es capaz de converger rápidamente. Por lo que este presenta un alto uso de CPU del router por lo que se debe tener precauciones a la hora de diseñar. Por su característica de flexibilidad en el diseño de red y al ser un estándar soporta dispositivos de todos los fabricantes.

OSPF es un protocolo de estado enlace. Y estos se definen como protocolos sofisticados que utiliza el algoritmo de Dijkstra para determinar el camino más corto

hacia el destino, libre de bucles. Estos protocolos utilizan localmente mayores recursos que los protocolos de vector distancia, ya que deben más datos con el objetivo de reducir el tráfico de red.

Estas son algunas ventajas de utilizar OSPF sobre los otros protocolos de estado enlace.

- Es un protocolo Classless, que permite la sumarización de redes.
- Converge rápidamente.
- Es estándar, y permite ser configurado en un escenario con diferentes tipos de fabricantes.
- Aprovecha ancho de banda disponible.
- Utiliza multicast en lugar de broadcast.
- Envía actualizaciones incrementales.
- Utiliza el Costo como única métrica.

Funcionamiento de OSPF

Los protocolos vector distancia anuncian rutas hacia los vecinos, pero los protocolos estado enlace anuncian una lista de todas sus conexiones. Cuando un enlace se cae se envían LSA (LINK-State Advertisement), que son compartidas por los vecinos, como así también una base de datos lógica LSDB (Link-State Database). Las LSA se identifican con numero de secuencia para reconocer las más recientes, en un rango de 0X8000 0001 al 0XFFF FFFF. Cuando los routers convergen tienen la misma LSDB, a partir de ese momento SPF es capaz de determinar la mejor ruta hacia el destino.

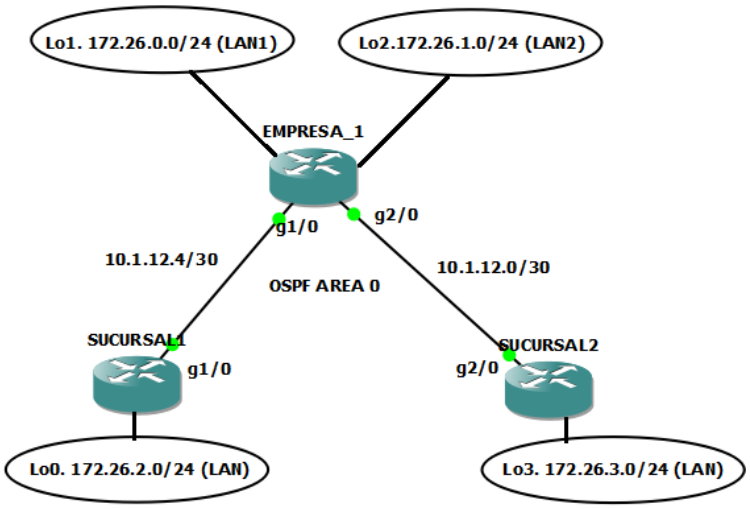


Figura 15 Topología OSPF con Área 0

La tabla de topología se actualiza por cada una de las LSA que envían los routers dentro de la misma área y que todos estos routers comparten la misma base de datos. Si existen inconsistencias en una base de datos podrían generarse bucles.

Algunas de estas pueden ser:

- Perdida de conexión física o link en algunas interfaces.
- No se reciben los “hello” en el tiempo establecido por sus vecinos.
- Se recibe un LSA con información de cambios de topología.

En cualquiera de los tres casos anteriores el router generará una LSA enviando a sus vecinos la siguiente información.

- Si la LSA es más reciente se añade a la base de datos. Se reenvían a todos los vecinos para que actualicen sus tablas y SPF comienza a funcionar.
- Si el número de secuencia es el mismo que el router ya tiene registrado en la base de datos, ignorara esta actualización.
- Si el número de secuencia es anterior al que está registrado, router enviara la versión nueva de router que envió el anterior. De esta manera se asegura que todos los routers poseen la última versión.

Métrica OSPF

El coste es la métrica utilizada por OSPF. Un factor importante en el intercambio de las LSA es la relativa a la métrica. La implementación de CISCO calcula el costo mediante la siguientes formula

$$Coste = \frac{100.000.000bps}{VelocidadEnlace} = \frac{10^8\,bps}{VelocidadEnlace}$$

Si existen varios caminos para llegar al destino con el mismo costo, OSPF efectúa por defecto un balanceo de cargas hasta 4 rutas diferentes. Este valor admite hasta 16 rutas diferentes. OSPF calcula el costo de manera acumulativa tomado en cuenta el costo de la interfaz de salida en cada router.

Tablas OSPF

Todas las operaciones OSPF se basan en tres tablas, las cuales deben mantenerse actualizadas.

- Tablas de vecinos.
- Tablas de Topologías.
- Tabla de enrutamiento.

Vecinos OSPF

OSPF establece relaciones con otros routers mediante el intercambio de mensajes “hello”. Luego del intercambio inicial de estos mensajes los routers elaboran sus tablas de vecinos, que lista todos los routers que están ejecutando OSPF y están directamente conectados. Los mensajes hello son enviados con la dirección multicast 2240.0.0.5 con una frecuencia en redes tipo broadcast cada 10 segundos, mientras que la redes no-broadcast cada 30 segundos.

El contenido de los “hello” se describe en la siguiente tabla:

Parámetro	Descripción
Router ID	Es un numero de 32 bit que identifica y hace único al router.
Hello and dead interval	Periodo de envió de los hello y su correspondiente timeout.
Neighbor list	Lista de todos los ID de los routers.
Area ID	Numero de área.
Priority	La prioridad que designa al DR y el BDR.
DR y BDR	Dirección IP del DR y BDR.
Authentication	Contraseña, si está habilitada
Stub Area Flag	Indica un Stub área.

Tabla 8 Contenidos de mensajes hello

Una vez que los routers hayan intercambiado los paquetes “hello”, comienzan a intercambiar información acerca de la red y una vez que esa información haya sincronizado los routers forman adyacencias.

Cuando el estado FULL es logrado, las tablas deben mantenerse actualizadas, las LSA son enviadas cuando exista algún cambio o cada 30 minutos como un tiempo de refresco.

Estados OSPF

Se describirá los estados de una relación de vecindad, a continuación:

- Down: es el primer estado de OSPF y significa que no se han escuchado “hellos” del vecino.
- Attempt: solo para redes NBMA, en este estado el router envía paquetes “hello” de tipo unicast hacia el vecino, aunque no se hayan recibido “hellos” de ese vecino.

- Init: se ha recibido un paquete “hello” de un vecino, pero el ID del router no está listado en ese paquete “hello”.
- 2-Way: se ha establecido una comunicación bidireccional entre dos routers.
- Exstart: una vez elegidos el DR y el BDR el verdadero proceso de intercambiar información del estado del enlace se hace entre los routers y sus DR y BDR
- Exchange: en este estado los routers intercambian la información de la base de datos de DBD.
- Loading: en este estado es cuando se produce el verdadero intercambio de la información de estado de enlace.
- Full: finalmente los routers son totalmente adyacentes, se intercambian las LSA y las bases de datos de los routers están sincronizadas.

Es debido mencionar que los mensajes “hello” se envían entres los router periódicamente para mantener las adyacencias, de no recibirse esos mensajes se pierden estas adyacencias. Cuando el protocolo OSPF detecta problema modifica las LSA correspondientes y envía actualizaciones a todos los vecinos, este proceso mejora el tiempo de convergencia y reduce al mínimo la cantidad de información que se envía a la red.

Router designado y router designado de reserva

En OSPF cuando varios routers están conectados en una red del tipo broadcast, uno de estos routers tomará el control y mantendrá las adyacencias entre todos los routers en esa red, a este router se le denomina DR o Designate Router, router desinado en inglés y será elegido a través de la información que contienen los mensajes “hello” que se intercambian los routers. Para una eficaz redundancia también se elige un router designado de reserva o BDR por sus siglas en ingles.

Los DR son creados en enlaces multi-acceso debido a que el número de adyacencias incrementaría de manera significativa el tráfico en la red, lo cual consumiría una gran cantidad de ancho de banda, recursos de memoria y CPU de los routers y la red misma, el objetivo final de los DR es reducir al máximo este consumo de recursos haciendo que los demás routers en la red establezcan adyacencia con él.

El roll del DR recibe actualizaciones y las distribuye a todos los demás routers de la red asegurándose con acuses de recibido de que estos han recibido correctamente dichas actualizaciones y que poseen una copia sincronizada de la LSDB. Estos routers notifican los cambios a través de la dirección multicast 224.0.0.6 a su ve el DR envía las LSA a los routers por la dirección multicast 224.0.0.5. El BDR escucha pasivamente y mantiene una tabla de relación con los demás routers, si en algún momento el DR deja de enviar mensajes “hellos” el BDR hará el trabajo del DR.

Es debido decir que estos dos router el DR y el BDR solo se usan en redes multiacceso, como anillos o con tres o más routers interconectados entre sí. En enlaces punto a punto estos no tienen sentido.

La elección del DR y el BDR dependerá de la interfaz de loopback más alta que está configurada en el router. En caso de que este configurado el comando “ip ospf priority”. Por defecto la prioridad es 1, en un rango de 0 a 255, a mayor prioridad mayores posibilidades de que sea elegido como DR. Si la prioridad del router es 0 entonces esta no participara en la elección.

El comando para realizar esta configuración es el siguiente:

Router(config-if)# ip ospf priority number

Se pueden dar casos de empate cuando la configuración de la prioridad no está hecha o tiene el mismo valor y también sucede lo mismo con la configuración de loopback. Cuando esto sucede se elegirá finalmente por la interfaz física más alta.

El comando *clear ip ospf process* se utiliza para forzar la elección del router designado y el router designado de respaldo.

Tipos de paquetes OSPF

El puerto 89 es por el cual se reconocen los paquetes IP del trafico OSPF. A continuación, se describen cinco tipos de paquetes OSPF diferentes:

- Hello: establecen la comunicación con vecinos conectados directamente.
- Database Descriptor (DBD): envían una lista de los ID de los routers, las LSA y el número de secuencia. Esta información se utiliza para testear la red.
- Link State Request (LSR): siguen a los paquetes DBD preguntando por cualquier paquete LSA que se haya perdido.
- Link State Update (LSU): son las respuestas a las LSR con los datos que se han pedido.
- Link State Acknowledgements (LSAck): confirma la recepción del paquete.

Todos los paquetes OSPF tienen el siguiente formato en común:

Campo	Descripción
Versión	Puede ser versión 2 o 3, según sea IPv4 o IPv6
Type	Hay 5 tipos de paquetes numerados del 1 al 5
Packet Length	Longitud medida en bytes
Router ID	Identificador del router de 32 bits
Area ID	Identificador del área de 32 bits
Checksum	Control estándar de 16 bits
Authentication Type	OSPFv2 soporta tres tipos de autenticación: • No autenticación • Texto plano • Encriptado MD5
Authentication Data	Son 64 bits de datos que pueden estar vacíos, contener texto plano o encriptación MD5
Data	Son los datos que se están enviando

Tabla 9 Paquetes OSPF

Áreas en OSPF

El área dentro de OSPF es una agrupación de routers que están ejecutando el mismo proceso y que tienen una base de datos idéntica o también se le conoce como subdivisión del dominio de enrutamiento de OSPF, donde cada área o subdivisión tiene en función su propio SPF (ruta más corta primero). También las áreas se intercambian las sumarizaciones de las redes.

Cuando una red OSPF crece, de debe tener en cuenta lo siguiente:

1. El algoritmo SPF se ejecuta con mayor frecuencia.
2. Cuento mayor sea el área mayor será la tabla de enrutamiento, cuanto más grande está más tiempo se tardará en hacer una búsqueda en ella, más gasto de recursos.
3. En una red de grandes dimensiones la tabla de topología puede ser inmanejables, intercambiándose entre los routers cada 30 minutos.

Cuando la base de datos se incrementa en tamaño y los cálculos aumentan en frecuencia, crece el procesamiento del CPU y memoria afectando directamente a la latencia de la red. Los efectos son congestiones de red, paquetes perdidos, malos tiempos de convergencia.

Las áreas en OSPF poseen dos niveles de jerarquía, el area 0 o de backbone y el resto de las áreas. Este diseño permite implementar sumarizaciones y minimizar la cantidad de entradas en las tablas, los routers del area 0 son llamados routers backbone, los routers que limitan entre el area 0 y las demás áreas se llaman ABR (Area Border Routers) y los routers que redistribuyen información desde algún otro protocolo de enrutamiento se llaman ASBR (Autonomous System Boundary Routers).

Configuración Básica de OSPF

Se denomina router interno a los routers que solo pertenecen a un área, su configuración a continuación:

- Proceso OSPF: establece en que numero de proceso se asocia el router.
- Interfaces: identifican a las interfaces usadas por OSPF.
- Área: define un área para cada interfaz, en este caso todas pertenecen a la misma.
- Router ID: identificador único de 32 bits.

Configuración OSPF en una sola área

Primero se identifica el número de proceso, este número tiene significado local y pueden existir varios procesos OSPF en un mismo router pero se debe tener en cuenta que entre más procesos más recursos se consumen en el router.

Router(config)#router ospf process-number

Luego de la habilitación se identifican las interfaces que participaran en el mismo, se debe tener cuidado en la utilización de la máscara comodín o wildcard.

Router(config-router)#network network-number wildcard-mask área área-number

La wildcard permite ser muy preciso, todas las interfaces que entran en el rango de la máscara wildcard participaran del proceso OSPF. El parámetro área, asocia las interfaces en un área en particular. El formato del parámetro área es un campo de 32 bits en decimal simple o notación decimal de punto.

El comando network aprovechando la flexibilidad de las wildcard se puede utilizar de la siguiente manera:

1. Configuración global de todas las interfaces.
2. Configuración de las redes a las que pertenecen las interfaces.
3. Configurando las interfaces una a una.

Estas opciones pueden aplicase de manera más eficiente dependiendo del caso. La opción uno puede ser de rápida configuración pero con el riesgo de que alguna interfaz no deseada se filtre en el proceso OSPF. El caso tres es más arduo para el administrador pero más selectivo y seguro.

Configuración de manera global todas las interfaces:

Router(router-config)#network 0.0.0.0 255.255.255.255 area 0

Configuración de las redes a las que pertenecen las inferfaces:

Configuración de router designado o DR:

Router(router-config)#router-id ip-address

Cisco no recomienda la utilización del comando router id, debido a que BGP también utiliza este comando y esto puede generar ciertos problemas entre las operaciones entre ambos protocolos. Para evitar esto se recomienda configurar una interfaz de loopback. Con una máscara de subred /32 para minimizar la cantidad de direcciones utilizadas.

Router(config)#interface loopback interface-number
Router(config-if)#ip address ip-address subnet-mask

Una vez que el router ID ha sido elegido se mantiene estable aunque las interfaces presenten altibajos; las interfaces de loopback al ser virtuales no son propensas a caerse, salvo que el administrador les haga un shutdown y las deje administrativamente inactivas. La interfaz de loopback se puede añadir al comando

network para poder hacer ping al router ID y de esta manera hacer más fácil la administración de la red.

Ejemplo de configuración de OSPF en una sola área

```
EMPRESA_1(config)#router ospf 1
EMPRESA_1(config-router)#router-id 1.1.1.1
EMPRESA_1(config-router)# network 10.1.12.0 0.0.0.3 area 0
EMPRESA_1(config-router)# network 10.1.12.4 0.0.0.3 area 0
EMPRESA_1(config-router)# network 172.26.0.0 0.0.0.255 area 0
EMPRESA_1(config-router)# network 172.26.1.0 0.0.0.255 area 0
```

Nota: se explica con mayor detalle en la guia de laboratorio No 1 resuelta, alojada en la seccion de anexos. Esta configuracion corresponde a la figura No. 15.

Verificación OSPF en una sola área

A continuación, se describe los comandos más importantes para la verificación y control de OSPF en un área simple:

Router#show ip ospf (process-id)

El comando enseña la configuración de OSPF en un router, es especialmente útil para saber el número de veces que se ha dejado ejecutado el algoritmo SPF que es un indicativo de la estabilidad de la red.

```
EMPRESA_1#sh ip ospf 1
 Routing Process "ospf 1" with ID 1.1.1.1
 Start time: 00:00:17.144, Time elapsed: 00:07:45.308
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
```

Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
Number of interfaces in this area is 4
Area has no authentication
SPF algorithm last executed 00:06:48.728 ago
SPF algorithm executed 3 times
Area ranges are
Number of LSA 5. Checksum Sum 0x02C367
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

A continuación, se explica con detalle el contenido del comando anterior:

Campo	Descripción
Routing Process "ospf 1" with ID 1.1.1.1	Muestra el ID del proceso local de OSPF y router ID de OSPF
SPF schedule delay	Tiempo que espera SPF para ejecutarse después de recibir un LSA. Previene ejecutar SPF de manera frecuente.
Hold time between two SPFs	Tiempo mínimo entre cálculos de SPF

Number of Dcbitless external LSA	Se usa en circuitos de OSPF "on demand"
Number of DoNotAge external LSA	Se usa en circuitos de OSPF "on demand" por ejemplo ISDN
Area BACKBONE(0) **Number of interfaces in this area is 4** **Area has no authentication** **SPF algorithm last executed 00:06:48.728 ago** **SPF algorithm executed 3 times** **Area ranges are**	Área a la que pertenece el router, como este router es interno solo pertenece a una. Cuantas interfaces hay en cada area. Autenticacion si la hay. Cuantas veces se ha ejecutado el algoritmo SPF. Si hay sumarizaciones.

Tabla 10 Comando show ip ospf

Router# **show ip ospf neighbor** (type number) (neighbor-id) (detail)

Este comando muestra los vecinos OSPF. Puede utilizarse listando todos los vecinos, por interfaces o con detalles más precisos de los vecinos.

EMPRESA_1#show ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*
3.3.3.3	*1*	*FULL/DR*	*00:00:36*	*10.1.12.6*	*GigabitEthernet1/0*
2.2.2.2	*1*	*FULL/DR*	*00:00:31*	*10.1.12.2*	*GigabitEthernet2/0*

EMPRESA_1#show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 10.1.12.6
In the area 0 via interface GigabitEthernet1/0
Neighbor priority is 1, State is FULL, 6 state changes
DR is 10.1.12.6 BDR is 10.1.12.5
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
LLS Options is 0x1 (LR)
Dead timer due in 00:00:35

Neighbor is up for 00:23:19
Index 2/2, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 2.2.2.2, interface address 10.1.12.2
In the area 0 via interface GigabitEthernet2/0
Neighbor priority is 1, State is FULL, 6 state changes
DR is 10.1.12.2 BDR is 10.1.12.1
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
LLS Options is 0x1 (LR)
Dead timer due in 00:00:35
Neighbor is up for 00:23:18
Index 1/1, retransmission queue length 0, number of retransmission 1
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 1, maximum is 1
Last retransmission scan time is 0 msec, maximum is 0 msec

A continuación, se explica con detalle el contenido de los comandos anteriores:

CAMPO	DESCRIPCIÓN
Neighbor	Router ID
Neighbor Priority	Prioridad enviada en el mensaje hello
State	Muestra el estado en que se encuentran el vecino: Down Attempt Init 2-Way Exstart Exchange Loading Full
Dead Time	Periodo de tiempo que el router espera sin escuchar hello para declarar al vecino como muerto

Address	Dirección IP del vecino. Hay que tener en cuenta que no tiene por qué ser la misma que la del Router ID
Interface	Interfaz por la cual se ha conocido al vecino
Options	Identifica una stub área

Tabla 11 Comando show ip ospf neighbor

Router# show ip protocols

Con el show ip protocols se muestran las configuraciones de los protocolos de enrutamiento que estén capacitados en el router. Además, se muestra cómo interactúan entre ellos y muestran cuándo ocurrirá la siguiente actualización:

EMPRESA_1#sh ip protocols
*** *IP Routing is NSF aware* ***

Routing Protocol is "ospf 1"
Sending updates every 0 second
Invalid after 0 second, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: ospf 1
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
10.1.12.0 0.0.0.3 area 0
10.1.12.4 0.0.0.3 area 0
172.26.0.0 0.0.0.255 area 0
172.26.1.0 0.0.0.255 area 0
Routing Information Sources:
Gateway Distance Last Update
3.3.3.3 110 00:25:38
2.2.2.2 110 00:25:48

A continuación, se explica con detalle el contenido del comando anterior:

CAMPO	DESCRIPCION
Routing Protocol is "ospf 1"	Protocolo de enrutamiento configurado
Sending updates every 0 seconds	Frecuencia de las actualizaciones
Invalid after 0 seconds **Hold down 0**	Para protocolos vectro-distancia indica el tiempo que una ruta es considerada valida Hold down es un tiempo usado en protocolos vector-distancia
flushed after 0	Tiempo en el que un protocolo vector-distancia eliminara una rata de la tabla de enrutamiento
Outgoing update filter list for all interfaces is not set	Indica si hay algún filtro de salida
Incoming update filter list for all interfaces is not set	Indica si hay algún filtro de entrada
Redistributing: ospf 1	Muestra información de redistribuciones
Routing for Networks: **10.1.12.0 0.0.0.3 area 0** **10.1.12.4 0.0.0.3 area 0** **172.26.0.0 0.0.0.255 area 0** **172.26.1.0 0.0.0.255 area 0**	Configuración del comando network
Routing Information Sources	Direcciones de origen de los router que envían actualizaciones a este router
Gateway	Dirección del router que nos proporciona actualizaciones
Distance	Distancia Administrativa
Last Update	Tiempo desde que el router recibio la última actualización
Distance: (default is 110)	La Distancia Administrativa se puede cambiar para todo el protocolo o por origen

Tabla 12 Comando show ip protocols

Router# show ip route

El comando enseña la tabla de enrutamiento del router, nos informa sobre cómo se alcanza una ruta y la interfaz:

EMPRESA_1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.12.0/30 is directly connected, GigabitEthernet2/0
L 10.1.12.1/32 is directly connected, GigabitEthernet2/0
C 10.1.12.4/30 is directly connected, GigabitEthernet1/0
L 10.1.12.5/32 is directly connected, GigabitEthernet1/0
172.26.0.0/16 is variably subnetted, 6 subnets, 2 masks
C 172.26.0.0/24 is directly connected, Loopback1
L 172.26.0.1/32 is directly connected, Loopback1
C 172.26.1.0/24 is directly connected, Loopback2
L 172.26.1.1/32 is directly connected, Loopback2
O 172.26.2.0/24 [110/2] via 10.1.12.6, 00:29:39, GigabitEthernet1/0
O 172.26.3.0/24 [110/2] via 10.1.12.2, 00:29:49, GigabitEthernet2/0

Router#show ip ospf database

Este comando nos muestra los contenidos de la base de datos topológica.

EMPRESA_1#sh ip ospf database

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 0)

Link ID	*ADV Router*	*Age*	*Seq#*	*Checksum*	*Link count*
1.1.1.1	*1.1.1.1*	*1827*	*0x80000003*	*0x00936A*	*4*
2.2.2.2	*2.2.2.2*	*1832*	*0x80000002*	*0x00D341*	*2*
3.3.3.3	*3.3.3.3*	*1829*	*0x80000002*	*0x003FC6*	*2*

Net Link States (Area 0)

Link ID ADV Router Age Seq# Checksum
10.1.12.2 2.2.2.2 1832 0x80000001 0x00A06F
10.1.12.6 3.3.3.3 1829 0x80000001 0x007C87

Router#show ip ospf interface (type number)

Muestra la configuración OSPF en cada interfaz.

EMPRESA_1#sh ip ospf interface gigabitEthernet 1/0
GigabitEthernet1/0 is up, line protocol is up
Internet Address 10.1.12.5/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 3.3.3.3, Interface address 10.1.12.6
Backup Designated router (ID) 1.1.1.1, Interface address 10.1.12.5
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:05
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 3.3.3.3 (Designated Router)
Suppress hello for 0 neighbor(s)

EMPRESA_1#sh ip ospf interface gigabitEthernet 2/0
GigabitEthernet2/0 is up, line protocol is up
Internet Address 10.1.12.1/30, Area 0, Attached via Network Statement
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
0 1 no no Base
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 2.2.2.2, Interface address 10.1.12.2
Backup Designated router (ID) 1.1.1.1, Interface address 10.1.12.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:06
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2 (Designated Router)
Suppress hello for 0 neighbor(s)

Comandos Debug

Estos dos comandos son utilizados para verificar y solucionar problemas en la red, pero estos consumen una gran cantidad de recursos de los CPU de los routers por lo que su uso debe ser moderado. Media ves se obtenga la información necesaria es recomendable deshabilitar el proceso con un "no" delante de los comandos.

Router#debug ip ospf events

Muestra información de eventos relativos a OSPF como son las adyacencias, flujo de información, selección de DR y BDR y cálculos de SPF.

Router#debug ip packet

Informa sobre paquetes recibidos, generados y enviados. No muestra el trafico si están habilitados CEF o Fast-switched de las interfaces correspondientes.

Topologías OSPF

El protocolo OSPF posee capacidad de enrutar cualquier medio de capa dos. Este protocolo asume que todos los routers en la red pueden comunicarse usando multicast y que ningún router ocupa una posición única o privilegiada dentro de la topología al menos a nivel lógico. Aunque en un entorno NBMA como por ejemplo Frame-Relay, donde multicast y broadcast no son soportados, es decir, redes OSPF NBMA, a afirmación anterior no es correcta.

Tipos de redes OSPF configurables en routers Cisco:

- Broadcast multi-access
- Point-to-point
- Point-to-multipoint. Nonbroadcast y broadcast
- Nonbradcast multiaccess (NBMA)

Multicast y broadcast se simulan a través de envíos a todos los vecinos, esto se hace para sustituir la falta de los mismos en las redes OSPF NBMA. En estos entornos el router designado DR debe ser capaz de comunicarse con los demás dispositivos de manera directa, este router debe definirse a la hora de diseñar la red.

Los router DR minimizan el tráfico de la red, estos siempre deben estar en comunicación con los demás dispositivos de la red. En una red de malla completa la selección del DR es automática, mientras que en las mallas parciales las configuraciones deberán asumirse manualmente. Esta configuración manual debe incluir cambiar propiedades del DR para que este en comunicación con los demás routers. Pero en redes punto a punto y punto a multipunto no se considera la selección de DR y BDR.

Tipos de redes OSPF funcionan con un estándar RFC o con estándares propiedades de cisco.

1. RFC-compliant (RFC 2328): compatible con cualquier tipo de fabricante y hace referencia a dos tipos de redes:
    - NBMA
    - Point-to-multipoint

2. Cisco-specific: específicas de Cisco para redes broadcast, point to multipoint (broadcast), point to multipoint nonbroadcast, point to point y NBMA de las cuales tres son propietarias:

    - Point to multipoint nonbroadcast
    - Broadcast

- Point to point

Reconocimiento de vecinos

Los routers no pueden identificar a sus vecinos de manera dinámica en las redes NBMA, eso debe hacerse de manera manual. En redes broadcast, el DR tiene un comportamiento similar que en el de las redes NBMA pero los vecinos se descubren dinámicamente.

En redes RFC point to multipoint los vecinos se descubren dinámicamente si la red es broadcast, si la red es nonbroadcast se hace la configuración manual de estos. Esta característica avanzada de configuración también se usa para designar diferentes tipos de costos OSPF debido a que en redes point to multipoint OSPF, por defecto, se tienen el mismo costo a cada vecino aunque en realidad el ancho de banda sea diferente.

En redes point to point el vecino es obviamente el otro router del otro extremo.

Temporizadores

OSPF envía intercaladamente paquetes hellos para descubrir nuevos vecinos y mantener la lista de los que ya conoce. Después de cuatro mensajes paquetes hello sin respuesta, este vecino se considera muerto “dead”. En las redes broadcast y point to point se mensajes hello son enviados cada 10 segundos y un dead cada 40 segundos. Los demás tipos de redes usan el mensaje hello cada 30 segundos y un dead cada 120 segundos.

Tabla resumen de los diferentes tipos de redes:

Tabla 13 Tipos de redes OSPF

	Non-broadcast	Point to Multipoint (Broadcast)	Point to Multipoint (Nonbroadcast)	Broadcast	Point to Point
DR/BDR	SI	NO	NO	SI	NO
Identificación de vecinos	SI	NO	SI	NO	NO
Intervalos de tiempos hello y dead	30/120	30/120	30/120	10/40*	10/40*
RFC 2328 Cisco	RFC	RFC	Cisco	Cisco	Cisco
Red soportada	Malla completa	Todas	Todas	Malla completa	Point to point

Múltiples áreas OSPF

El área OSPF es un conjunto de routers que están ejecutando OSPF y que comparten la misma información de la base de datos topológica. Además un área es una subdivisión de un dominio de OSPF. El uso de estas áreas elimina la necesidad de comunicar todos los detalles de la red en cada dispositivo de enrutamiento, de esta forma se mantiene el control y conectividad entre todos ellos.

Los routers mantienen sus bases de datos topológicas divididas en áreas por lo que les permite mayor eficiencia y reducir el tamaño de estas bases de datos. Cualquier cambio a la base de datos topológica debe ser comunicado a todos los dispositivos de un área. La comunicación entre áreas y redes fuera del sistema autónomo se realiza con los enlaces externos.

Cuando la red crece, también crecen las bases de datos topológicas lo cual genera grandes gastos de recursos de memoria y CPU, esto conlleva a congestión entre enlaces, pedidas de paquetes y sistemas saturados. Para evitar esto se debe dividir la red en áreas más pequeñas esto contribuye al mejor rendimiento de las mismas.

Tipos de router en múltiples áreas

Routers dentro del modelo jerárquico en las áreas:

- Internal router: mantiene base de datos actualizada y precisa cada una de las LSA en cada área. También envía datos hacia otras redes empleando la ruta más corta. Todas las interfaces de este router están dentro de la misma área.
- Backbone router: las normas de OSPF requieren que todas las areas estén conectadas a un área de Backbone o área 0. Un router dentro de esta área lleva este nombre.
- Area Border Router (ABR): este router es la conexión entre dos o más áreas, mantiene una base topológica de cada una de las áreas a la que pertenece y envía actualizaciones LSA a cada una de dichas áreas.
- Autonomous System Boundary Router (ASBR): este router conecta hacia otros dominios de enrutamiento, normalmente ubicados dentro del área de Backbone.

Tipos de anuncios de estado de enlace

Las LSA (Link-State Advertisements) listan todas las rutas posibles, a continuación, las más comunes:

- Router link LSA (tipo 1): cada router genera LSA listando cada vecino y el costo hacia cada uno. Las LSA de tipo 1 y de tipo 2 se envían dentro de toda el área y son empleadas por SPF para elegir rutas.
- Network link LSA (tipo 2): es enviada por el DR, contiene una lista de todos los routers con el que esta forma adyacencias.
- Network summary link LSA (tipo 3): son generadas por los ABR para ser enviadas entre areas. Estas LSA listan todos los prefijos en un área determinada, incluida también, si la hubiera, la sumarización.
- AS external ASBR summary link LSA (tipo 4): generan este tipo de LSA para advertir de su presencia. Informan a todos los demás routers como alcanzar al ASBR. Las LSA de tipo 3 y tipo 4 son denominadas inter-area porque pasan información entre areas.
- External link LSA (tipo 5): son originadas por ASBR e inundan todo el AS con información de rutas externas OSPF o rutas por defecto.

- NSSA external LSA (tipo 7): son creadas por un ASBR dentro de un NSSA (Not-So-Stubby Area) puesto que no permiten el uso de LSA de tipo 5. En una NSSA habrá LSA del tipo 7 informando sobre las rutas externas, el ABR es el encargado de convertirlas al tipo 5.

OSPF en múltiples áreas y selección de rutas entre áreas

OSPF funciona manteniendo la lógica del sistema autónomo en diferentes tipos de áreas.

El router siempre va a escoger la ruta que sea con menor costo administrativo. En caso en que existan rutas con el mismo costo OSPF balanceara la carga equitativamente en ambas rutas, este proceso es automático el máximo de rutas es cuatro.

Elementos importantes en la creación de una tabla de enrutamientos son:

- El router recibe las LSA
- El router construye una base de topología
- El router ejecuta el algoritmo de Dijkstra para calcular la ruta más corta y añadirla en la tabla de enrutamiento

El algoritmo de Dijkstra, también llamado algoritmo de caminos mínimos, es un algoritmo para la determinación del camino más corto, dado un vértice origen, hacia el resto de los vértices en un grafo que tiene pesos en cada arista. Su nombre alude a Edsger Dijkstra, científico de la computación de los Países Bajos que lo describió por primera vez en 1959.

Configuración de OSPF en múltiples áreas

Pasos para iniciar:

- Definir las interfaces en el router. Se identifica que interfaces participaran en el proceso de OSPF.
- Identificar el área. Definir a que área pertenecen dichas interfaces
- Router ID. Este parámetro identifica al router en la topología de OSPF

Router(config)#router ospf process-number

El comando anterior habilita la configuración del protocolo OSPF en el router. El process-number es un número que tiene carácter local, este digito puede variar entre los routers del domino, pero se recomienda usar el mismo número para mayor facilidad de administración.

Router(config-router)#network network-number wildcard-mask área área-number

Este comando es utilizado para agregar una red con su máscara de wildcard al proceso OSPF indicado en un área definida.

Router(config)#interface GigabitEthernet x/y
Router(config)#ip ospf process-number area area-number

Comandos opcionales para OSPF en múltiples áreas

- area range: para ABR
- summary-address: para ASBR
- area area-id stub: para definir un area stub
- area area-id stub no-summary: define un totally stubby area
- area default-cost: determina el valor de las rutas por defecto del area
- area virtual-link: utilizado para configurar enlaces virtuales

Router(config-router)#area area-id range address mask

El comando anterior se utiliza en router ABR, genera sumarizaciones reduciendo considerablemente el tamaño de las bases de datos.

Router(config-router)#summary-address address mask (not-advertise)(tag tag)

Este comando, es para sumarizar rutas en router ASBR. La IP es la dirección sumarizada con su máscara.

Router(config-router)#area area-id stub

Un área configurada como stub con el comando anterior requiere que todo los routers esten como stub o totally stub. Es conveniente tener áreas stub cuando los routers tienen poca capacidad de procesamiento.

Router(config-router)#area area-id stub no-summary

Este comando se configure al ABR de que no envié sumarizaciones, LSA tipo 3 y tipo 5 desde otras areas.

Ejemplo configuración OSPF en múltiples áreas

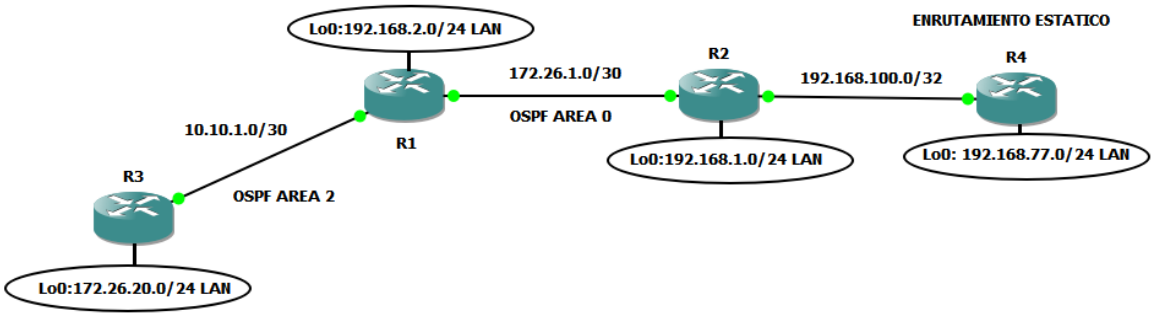


Figura 16 Topologia OSPF en Multiples Areas

R1(config)#interface Loopback1
R1(config-if)# description LAN_1
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)#!

R1(config-if)#interface GigabitEthernet1/0
R1(config-if)# ip address 172.26.1.1 255.255.255.252
R1(config-if)# ip ospf 1 area 0
R1(config-if)# negotiation auto
R1(config-if)#!

R1(config-if)#interface GigabitEthernet2/0
R1(config-if)# description R3_GI2/0
R1(config-if)# ip address 10.10.1.1 255.255.255.252
R1(config-if)# ip ospf 1 area 2
R1(config-if)# negotiation auto
R1(config-if)#!

R1(config-if)#router ospf 1
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0

R3(config)#interface Loopback1
R3(config-if)# description LAN_1
R3(config-if)# ip address 172.26.20.1 255.255.255.0
R3(config-if)#!

R3(config-if)#interface GigabitEthernet2/0
R3(config-if)# description R1_GI2/0
R3(config-if)# ip address 10.10.1.2 255.255.255.252
R3(config-if)# ip ospf 120 area 2
R3(config-if)# negotiation auto

R3(config-if)#router ospf 120
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 172.26.20.0 0.0.0.255 area 2

Nota: se explica con mayor detalle en guia de laboratorio No 2 resuelta, alojada en la seccion de anexos. Esta configuracion corresponde a la figura No. 16.

Comandos de verificación de OSPF en múltiples áreas

Router#show ip ospf border-routers

Muestra ABR y ASBR que el router interno tiene en su tabla de enrutamiento.

R3#sh ip ospf border-routers

OSPF Router with ID (3.3.3.3) (Process ID 120)

Base Topology (MTID 0)

Internal Router Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 1.1.1.1 [1] via 10.10.1.1, GigabitEthernet2/0, ABR, Area 2, SPF 2

I 2.2.2.2 [2] via 10.10.1.1, GigabitEthernet2/0, ASBR, Area 2, SPF 2

Campo	Descripción
OSPF process 120 internal routing table	Indica el ID del proceso de OSPF que está ejecutando el router
Destination	Router ID (RID) del destino, ya sea un ABR o un ASBR
Next Hop	Proximo salto para alcanzar al ABR O ASBR
Cost	Metrica hacia el destino
Type	Clasifica el router como ABR o ASBR o ambos
Rte Type	Tipo de ruta: intra-area o inter-area
Área	El área ID del área desde la cual la ruta es aprendida
SPF No	Número del cálculo de SPF que instalo la ruta en la tabla de enrutamiento

Tabla 14 Comando show ip ospf border-routers

El siguiente comando muestra todas las rutas dentro de su tabla de enrutamiento en el router.

Router#show ip route

Ejemplo del comando anterior, ejecutado en router R3 de la figura No 16.

R3# sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.10.1.1 to network 0.0.0.0

*O*E2 0.0.0.0/0 [110/1] via 10.10.1.1, 00:27:14, GigabitEthernet2/0*
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.1.0/30 is directly connected, GigabitEthernet2/0
L 10.10.1.2/32 is directly connected, GigabitEthernet2/0
172.26.0.0/16 is variably subnetted, 3 subnets, 3 masks
O IA 172.26.1.0/30 [110/2] via 10.10.1.1, 00:27:14, GigabitEthernet2/0
C 172.26.20.0/24 is directly connected, Loopback1
L 172.26.20.1/32 is directly connected, Loopback1
192.168.1.0/32 is subnetted, 1 subnets
O IA 192.168.1.1 [110/3] via 10.10.1.1, 00:27:14, GigabitEthernet2/0
192.168.2.0/32 is subnetted, 1 subnets
O IA 192.168.2.1 [110/2] via 10.10.1.1, 00:27:14, GigabitEthernet2/0
O E2 192.168.77.0/24 [110/20] via 10.10.1.1, 00:27:14, GigabitEthernet2/0

Ejemplo del comando anterior, ejecutado en router R1 de la figura No 16.

R1# sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 172.26.1.2 to network 0.0.0.0

*O*E2 0.0.0.0/0 [110/1] via 172.26.1.2, 00:29:04, GigabitEthernet1/0*
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.1.0/30 is directly connected, GigabitEthernet2/0
L 10.10.1.1/32 is directly connected, GigabitEthernet2/0
172.26.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.26.1.0/30 is directly connected, GigabitEthernet1/0
L 172.26.1.1/32 is directly connected, GigabitEthernet1/0
O 172.26.20.1/32 [110/2] via 10.10.1.2, 00:29:04, GigabitEthernet2/0
192.168.1.0/32 is subnetted, 1 subnets
O 192.168.1.1 [110/2] via 172.26.1.2, 00:29:04, GigabitEthernet1/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Loopback1
L 192.168.2.1/32 is directly connected, Loopback1
O E2 192.168.77.0/24 [110/20] via 172.26.1.2, 00:29:04, GigabitEthernet1/0

Tipo de LSA	Entrada en la tabla de enrutamiento	Descripción
1 Router Link	0	Generadas por el propio router, lista los enlaces que conectados, el estado y el coste. Son propagadas dentro del área
2 Network Link	0	Generadas por el DR en una red multi-acceso
3 or 4 Summary Link (between areas)	OIA	Incluye las redes generadas dentro de un area y que podrian ser sumarizadas y que son enviadas dentro del area 0 y entre ABR. Las de tipo 4 indican como encontrar al ASBR. Estas LSA no son enviadas dentro de totally stubby areas.
5 Summary Link / External Link (between autonomous systems)	OE1 o OE2	Rutas externas que pueden ser configuradas para tener uno o dos valores. E1 incluye el coste hacia el ASBR más el coste externo reportado por el ASBR. E2 solo incluye el coste externo.

Tabla 15 Comando show ip route

Router#show ip ospf database

Muestra entradas en la base de datos de estado de enlace y la información de las LSA que se tienen.

R1# sh ip ospf database

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 0)

Link ID ADV Router Age Seq# Checksum Link count

1.1.1.1 1.1.1.1 149 0x80000003 0x000C0C 2

2.2.2.2 2.2.2.2 2138 0x80000002 0x00D53A 2

Net Link States (Area 0)

Link ID ADV Router Age Seq# Checksum

172.26.1.2 2.2.2.2 2138 0x80000001 0x00AAB4

Summary Net Link States (Area 0)

Link ID ADV Router Age Seq# Checksum

10.10.1.0 1.1.1.1 149 0x80000002 0x005BC9

172.26.20.1 1.1.1.1 149 0x80000002 0x0098C1

Campo	Descripcion
Link ID 1.1.1.1	Router ID
ADV Router 1.1.1.1	Router ID del router que está advirtiendo
Age 149	Tiempo del estado de enlace
Seq# 0x80000003	Numero de secuencia del enlace
Checksum 0x000C0C	Control del contenido de la LSA
Link count 2	Numero de interfaces detectadas

Tabla 16 Comando show ip ospf database

Router#show ospf neighbor

El comando anterior, muestra a los vecinos activos del router que están configurados con OSPF.

Autenticación OSPF

En OSPF por defecto confía en todos los paquetes que recibe por lo tanto es susceptible a posibles ataques, por lo que los sistemas de redes pueden ser atacados sobre todo interceptando paquetes y así conseguir por ejemplo denegación de servicio o inyectar rutas que son maliciosas.

Tres niveles de autenticación:

- Null, sin autenticación.
- Texto plano, la contraseña no está cifrada
- Cifrado con el algoritmo MD5

Autenticación en texto plano: el nivel de seguridad que da es muy básico, todos los routers dentro del área puede tener contraseña por interfaz.

A continuación, los comandos en orden:

Router(config-if)#ip ospf authentication-key password
Router(config-if)#ip ospf authentication

Autenticación con MD5 (Message Digest): tiene un buen nivel de seguridad, ambos extremos conocen las claves de autenticación. En este sistema se crean claves y contraseñas que trabajan en paralelo, se puede tener más de una clave a la vez.
A continuación, los comandos en orden:

Router(config-if)#ip ospf message-digest-key key md5 password
Router(config-if)#ip ospf authentication message-digest

Para verificar que esté trabajando la autenticación, se utiliza los siguientes comandos:

- ip ospf neighbor: para ver que los vecinos completen las adyacencias
- ip ospf interface: muestra información de la autenticación en la interfaz
- debug ip ospf adjacency: muestra todos los estados de la autenticación **[5]**

GUIA DE LABORATORIO 1: Configuración de OSPF de área única para el intercambio de información de ruteo entre una empresa y sus sucursales.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Aplicar y reforzar conocimientos del protocolo de enrutamiento dinámico OSPF (Open Shortest Path First).
- Observar la manera que se intercambian la información de ruteo entre una empresa y sus sucursales.

INTRODUCCION

En la siguiente guía de laboratorio, se dará a conocer cómo funciona el protocolo de enrutamiento de dinámico OSPF. Mediante un ejemplo en el cual se evidencia como una empresa intercambia tablas de ruteo con sus sucursales de manera dinámica.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

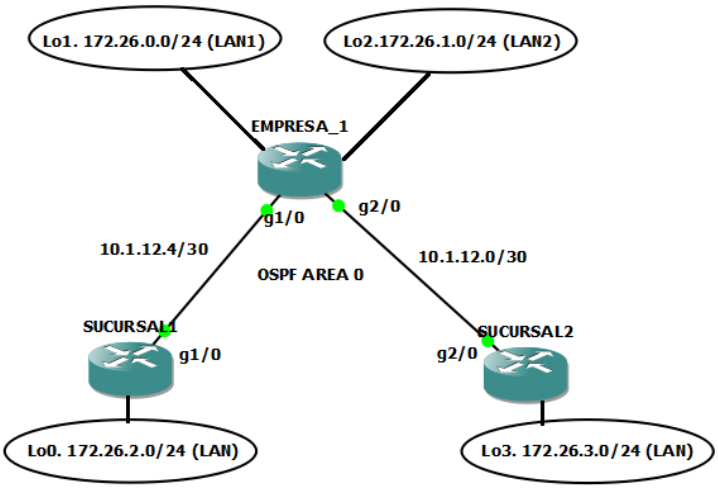


Tabla de direccionamiento

Equipo	Interfaz	Dirección IP	Mascara
EMPRESA_1	GigabitEthernet1/0	10.1.12.5	255.255.255.252
	GigabitEthernet2/0	10.1.12.1	255.255.255.252
	Loopback1 (LAN1)	172.26.0.1	255.255.255.0
	Loopback2 (LAN2)	172.26.1.1	255.255.255.0
SUCURSAL1	GigabitEthernet1/0	10.1.12.6	255.255.255.252
	Loopback0 (LAN)	172.26.2.1	255.255.255.0
SUCURSAL2	GigabitEthernet2/0	10.1.12.2	255.255.255.252
	Loopback3 (LAN)	172.26.3.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

Usando el direccionamiento propuesto en el diagrama anterior, crearemos interfaces loopback y aplicaremos el direccionamiento IPV4 para estas, así como la configuración de las interfaces gigabitEthernet asociadas a la empresa y sus sucursales. Las loopbacks configuradas en los routers simulan segmentos de redes reales utilizados por la empresa y sus sucursales para garantizar la conexión entre ellas.

Usar el comando ping para probar la conectividad entre los routers directamente conectados.

Paso 2.- Configurar OSPF en los routers.

Crear proceso OSPF 1 y defina OSPF router-id en los tres routers (*EMPRESA_1 = 1.1.1.1; SUCURSAL2 = 2.2.2.2; SUCURSAL1= 3.3.3.3).* Usando los comandos de redes, configurar las subredes en las interfaces eléctricas entre los routers antes

mencionados para agregarlos en el proceso ospf área 0. Así como enrutar las redes LAN simuladas en las interfaces loopback.

El comando **show ip ospf** es utilizado para verificar el OSPF router ID. Si el router ID está utilizando valores de 32-bit, otro que no haya sido especificado por el comando router-id. Se puede aplicar un reset router ID, mediante la utilización del comando **clear ip ospf *pid* process** y verificar nuevamente.

Nuevamente, el comando **show ip ospf** debe ser usado para verificar el OSPF router id. Que este sea igual al especificado por el comando router-id. En caso de que este no coincida se deberá aplicar reset al proceso OSPF en ambos routers R2 y R3. Mediante el comando **clear ip ospf process.** Luego verificar nuevamente.

Verificar que se observe los vecinos ospf, por medio del comando **show ip ospf neighbors** en la salida de los routers. Así como garantizar los routers puedan aprender las loopbacks declaradas entre ellos. Con el comando **show ip route.**

CUESTIONARIO

1. ¿Cuál son los ID de los vecinos con quien el equipo EMPRESA_1 con que el equipo hablaba OSPF?

2. ¿Cuantos prefijos son aprendidos mediante el protocolo dinámico OSPF en el equipo EMPRESA_1?

3. ¿Cuál es el ID del vecino para el Router SUCURSAL_1?

4. ¿Qué segmentos de red debe de aprender el equipo SUCURSAL_1? ¿Por qué?

5. ¿Cuál es el ID del vecino para el Router SUCURSAL_1?

6. ¿Qué segmentos de red debe de aprender el equipo SUCURSAL_2? ¿Por qué?

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

GUIA DE LABORATORIO 2: Configuración de OSPF Multi-Área y su compartimiento con la redistribución de rutas estáticas.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Aplicar y reforzar conocimientos del protocolo de enrutamiento dinámico OSPF (Open Shortest Path First).
- Configure OSPFv2 de áreas múltiples para IPv4
- Verificar el comportamiento de múltiples áreas.
- Observar la manera que se intercambian la información de ruteo entre diferentes áreas.

INTRODUCCION

En la siguiente guía de laboratorio, se realizara la configuración de OSPFv2 de áreas múltiples para IPv4. Y su comportamiento redistribuyendo ruta estáticas en el proceso OSPF.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

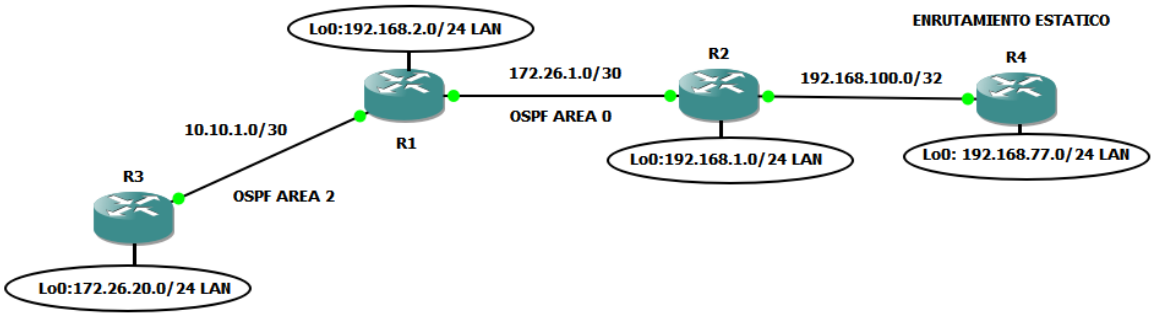


Tabla de direccionamiento

Equipo	Interfaz	Direccionamiento IP	Mascara
R1	GigabitEthernet1/0	172.26.1.1	255.255.255.252
	GigabitEthernet2/0	10.10.1.1	255.255.255.252
	Loopback1(LAN)	192.168.2.1	255.255.255.0
R2	GigabitEthernet1/0	172.26.1.2	255.255.255.252
	GigabitEthernet2/0	192.168.100.1	255.255.255.252
	Loopback1(LAN)	192.168.1.1	255.255.255.0
R3	GigabitEthernet2/0	10.10.1.2	255.255.255.252
	Loopback1(LAN)	172.26.20.1	255.255.255.0
R4	GigabitEthernet2/0	192.168.100.2	255.255.255.252
	Loopback1(LAN)	192.168.77.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

En este laboratorio, se configurara una red OSFPv2 Multi-area para IPV4. El área 2 se configurará como un área normal de OSPF, un área de código auxiliar y usando el direccionamiento propuesto en el diagrama anterior, aplicaremos el direccionamiento IPV4 para las interfaces gigabit Ethernet e interfaces virtuales. Las loopbacks configuradas en los routers simulan segmentos de redes reales.

Realizar pruebas de conectividad a nivel L3, mediante Ping.

Paso 2.- Configurar OSPF en los routers.

Crea proceso OSPFv2 1 en los router R1, R2 y proceso 120 en el router R3. Configurar el OSPF Router ID en cada uno de ellos. Habilitar redes directamente

conectadas en el proceso OSPF utilizando **ip ospf *process-id* área *área-id*** (R1=1.1.1.1; R2=2.2.2.2; R3=3.3.3.3).

El comando **show ip ospf** es utilizado para verificar el OSPF router ID. Si el router ID está utilizando valores de 32-bit, otro que no haya sido especificado por el comando Router-id. Se puede aplicar un reset router ID, mediante la utilización del comando **clear ip ospf *pid* process** y verificar nuevamente.

Configurar R2 con router OSPFv2 en área 0. Configurar R1, como router ABR para el área o y área 2. Interfaz Gi1/0 en el área 0 y la interfaz Gi2/0 en el área 2.

Paso 3.- Configurar R3 como router OSPFv2 interno en el área 2.

Verificar que los routers tengan vecinos OSPFv2. Utilizando el comando **show ip ospf neighbors**.

Verificar que el router R2 y R1 pueda ver todas las redes IPv4 en la tabla de enrutamiento OSPFv2 usando el comando **show ip route**.

Paso 4.- Configura una ruta estática IPV4 por defecto en el router ASBR R2 para reenviar tráfico para el router R4. Y propagar la ruta estática por defecto en el OSPFv2.

R2(config)#ip route 0.0.0.0 0.0.0.0 x.x.x.x
R2(config)#router ospf 1
R2(config-router)# default-information originate

Para el router R4 se deberá crear una ruta estatica por defecto para que pueda alcanzar todas rutas anunciados por los procesos OSPF multiarea.

R4(config)#ip route 0.0.0.0 0.0.0.0 x.x.x.x

Ejecute el comando **show ip route static** en el R2, para verificar la ruta estática la tabla de enrutamiento IPV4.

Se requiere la configuración de una ruta estática en el router ASBR, la cual simule un cliente que se encuentre fuera del proceso de enrutamiento dinámico. R2 para la red 192.168.77.0/24 y el gateway del R4. Redistribuye la ruta estática en el proceso OSPFv2 usando el comando **redistribute static subnets**. El parámetro de subredes se usa para incluir subredes y no solo direcciones de red con clase.

Utiliza el comando **show ip route ospf** en el R3, para verificar que la ruta predeterminada y la ruta estática redistribuida se anuncian en el proceso OSPFv2.

CUESTIONARIO

1. ¿Qué significa el "E2" para la ruta predeterminada y la ruta externa redistribuida?

2. ¿Por qué en el router R1 no tiene rutas inter-area en su tabla de enrutamiento?

3. ¿Cuantas rutas OSPFv2 intra-area hay en el router R2 dentro su tabla de enrutamiento IPV4? ¿Cuántas rutas inter-area hay en su tabla de enrutamiento?

4. ¿Qué direccionamiento en el R2 es utilizado para establecer adyacencia de vecindad con el R1?

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

Capítulo 3: Protocolo BGP

Border Gateway Protocol (BGP) por sus siglas en inglés; es un protocolo de enrutamiento que es usado para la información sobre la accesibilidad de la capa de red de intercambio o NLRI, entre dominios de enrutamiento. Un dominio de enrutamiento es frecuentemente llamado un sistema autónomo o autonomous system (AS), por diferentes controles de autoridades administrativas de sus dominios respectivos. El Internet actual es una red de sistemas autónomos interconectados, donde BGP versión 4 (BGP4) es de hecho el protocolo de enrutamiento más utilizado. BGP soporta VLSM (Variable Length Subnet Mask), CIDR (Classless Interdomain Routing) y sumarización.

Este protocolo se utiliza para principalmente para conectar grandes redes de organizaciones o sistemas autónomos y diferentes divisiones empresariales en Internet. BGP mantiene las rutas estables y para esto evita estar advirtiendo e intercambiándolas constantemente además deja despejadas las rutas de tráfico innecesario.

Los dispositivos, equipos y redes controlados por una organización son llamados sistemas autónomos (AS). Es decir que estos tienen independencia a la hora de elegir cualquier método o sistema para enrutar sus tráficos de datos en sus WAN por lo que estos utilizan BGP para comunicar a los AS independientemente de los sistemas que utilice cada organización.

Funcionamiento básico BGP

Dependiendo de los sistemas autónomos por donde va pasando así se registran las rutas y evita los bucles con los mismos números de AS. Los peers son los vecinos de los BGP y deben ser predefinidos.

Estos son los mensajes que se envían para construir las relaciones:

- Open
- Keepalive
- Update
- Notification

A través del mensaje BGP open utilizando el puerto TCP 179 se crean y mantienen las conexiones. En la tabla de vecinos separada se mantiene la información del peer. Las sesiones son mantenidas enviando constantemente mensajes de keepalive. En caso que se reseteo un peer esta envía un mensaje para finalizar la relación. Con el mensaje update los routers BGP intercambian sus tablas de enrutamiento completas cuando la relación de vecindad se establece por primera vez. Esas tablas solo recibirán actualizaciones de incremento cuando haya cambios en la red.

Jerarquías BGP

Para que la red se pueda organizar de manera jerárquica otros protocolos de enrutamiento soportan sumarizaciones también. BGP debe trabajar con cualquiera topología que le sea dada porque las organizaciones no tienen orden jerárquico. Las sumarizaciones en BGP funcionan igual que en otros protocolos, por lo que utilizan menos de recursos de memoria, CPU y tablas de rutas más pequeñas.

En una red BGP optimizada por sumarizaciones, no significa que lo este de manera jerárquica. BGP puede ser utilizado entre redes o dentro de una red, este identifica posibles caminos dentro de los sistemas autónomos. BGP detecta bucles mirando las rutas de los AS-Path.

¿Cuándo se utiliza BGP?

Este protocolo se utiliza en los siguientes casos:

- BGP es el único protocolo que puede conectar a una organización a diferentes sistemas autónomos.
- BGP debería ser considerado si se desea implementar una política de enrutamiento, como por ejemplo controlar un enlace hacia un ISP
- BGP es adecuado para un AS, usado como AS de transito que se interconecta a otros sistemas autónomos. Un ISP es un típico AS de tránsito.

Si los casos anteriores no se cumplen o no son requeridos es posible que otra opción más simple, económica y que utilice menos equipos y configuraciones complejas pueda ser implementado en vez de BGP.

Tablas BGP

Existen tres tipos de tablas:

Tipos de tablas	Descripción
Tablas de vecinos	tablas de vecinos configurados en el router, vecinos BGP
Tabla de BGP	rutas de BGP que son mantenidas en una tabla de BGP separada
Tabla de enrutamiento IP	las mejores rutas BGP son pasadas a la tabla de enrutamiento

Tabla 17 Tablas BGP

Herramientas como route-maps y listas de distribución son soportadas por BGP y estas permiten cambiar el flujo de tráfico basado en atributos de este protocolo.

Sincronización

Cuando un AS funciona como tránsito para otros AS, y este AS no posee router BGP estos podrían descargar el tráfico de transito dado que no conocen las rutas. Para evitar esta situación BGP utiliza IGP para enseñar a todos los routers dentro de ese AS de transito las rutas.

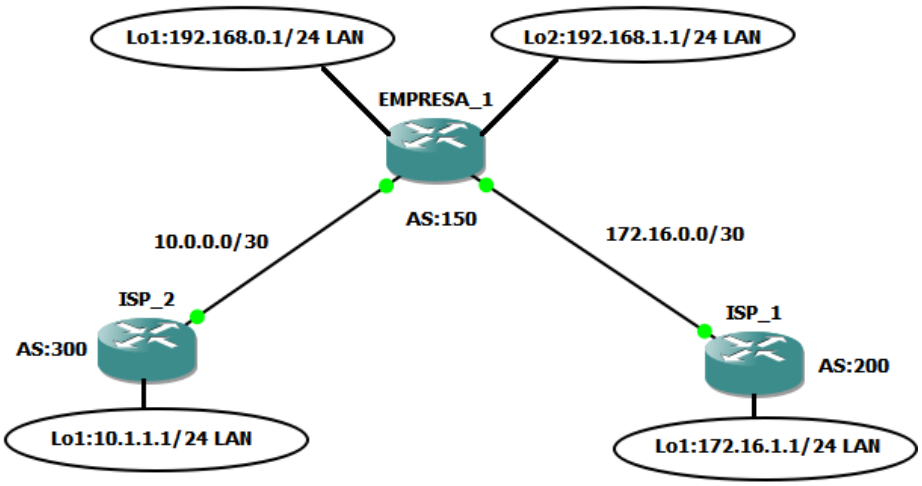


Figura 17 Topología de enrutamiento dinámico BGP

El router EMPRESA_1 envía actualizaciones acerca de la ruta 10.0.0.0/30 hacia el router ISP_2. Este a su vez este envía actualizaciones de la ruta 172.16.0.0/30 al router ISP_1 Utilizando EBGP. Internamente los proveedores de servicio antes mencionado ejecutan IGP e IBGP dentro de su infraestructura para lograr su conectividad a nivel interno.

La regla de sincronización pasa tráfico de un AS hacia otro AS y no advierte de una ruta antes de que todos los routers dentro del AS hayan aprendido esa ruta via IGP. Hay ciertas circunstancias donde es mejor deshabilitar la sincronización esto deja que BGP converja más eficiente, pero esto puede producir perdida de paquetes.

En las siguientes condiciones, se puede deshabilitar la sincronización:

- El sistema autónomo no pasa tráfico entre sistemas autónomos
- Todos los routers de transito ejecutan BGP

El siguiente comando se usa para deshabilitar la sincronización en routers BGP

Router(config-router)#no synchronization

Y el siguiente comando se utiliza para activarla

Router(config-router)#synchronization

Otra manera de solventar los problemas de la sincronización es utilizando MPLS junto a BGP a como se muestra en los capítulos siguientes.

Estados de BGP

Se explicará de manera detallada los Estados de BGP en la siguiente tabla:

Estados	Descripción
Idle	El router está buscando a los vecinos
Connect	Se está a la espera de que se complete la conexión TCP (protocolo de transporte) en puerto 179. El estado cambia a active sino logra completar la conexión, de lograse la fase siguiente será open sent.

Active	Iniciada una conexión a través de TCP se intenta establecer una vecindad. De lograrse el estado cambia a open sent. Cuando connect retray expira BGP lo reinicia y vuelve al estado connect. Si se crea un bucle entre los estados connect y active esto indica que la conexión TCP no se puede establecer.
Open Sent	Se esperan los mensajes open del vecino, estos mensajes se revisan para verificar datos y que las versiones de BGP sea las correctas, así como el número de sistemas autónomos.
Open Confirm	Se espera los menajes keepalive, si se reciben se pasa al siguiente estado.
Established	Es el estado final y el necesario para que BGP comience a funcionar, se intercambian rutas, actualizaciones o keepalives.

Tabla 18 Estados BGP

Nota: Si el router permanece en idle es necesario revisar si existe un salto antes del vecino con el que se quiere crear la vecindad. Si se está permanentemente en estado active habrá que verificar la posible existencia de un firewall que tenga bloqueado el puerto TCP 179.

Con el siguiente comando se muestra el estado de un router BGP:

EMPRESA_1#sh ip bgp neighbors

BGP neighbor is 10.0.0.2, remote AS 300, external link

BGP version 4, remote router ID 10.1.1.1

BGP state = Established, up for 00:20:57

Last read 00:00:40, last write 00:00:23, hold time is 180, keepalive interval is 60 seconds

Neighbor sessions:

Configuración de BGP

La configuración debe incluir las redes que se quieren anunciar, dado que BGP está diseñado para conectar sistemas autónomos entre sí, es requisito identificar el sistema autónomo propio y a los sistemas autónomos de vecinos.

Router(config)#router bgp autonomous-system-number

Este comando se utiliza para iniciar la configuración. BGP solo tiene la capacidad de ejecutar un proceso por router. Si se tiene más de un proceso BGP configurado, el router mostrara el número del proceso que está siendo usado en ese momento.

Identificar vecinos y definir grupos-peer

Se debe predefinir los routers que se conectaran a BGP dado que ese proceso no es automático. Se utiliza el comando neighbor para determinar a vecinos junto a sus sistemas autónomos. IBGP (Internal BGP) se da cuando ambos AS, el local y el vecino, son el mismo. EBGP (External BGP) se da cuando los AS son diferentes.

Router(config-router)#neighbor ip-address remote-as autonomous-system-number

Los peer-group simplifican la tarea pesada de listar a vecinos y sus políticas asociadas, dado los grandes bloques de configuraciones que se tendrían que realizar, esto complicaría la solución de fallas en la red también.

En estos grupos peer-group todos comparten la misma política de actualizaciones, aunque si es posible configurar cada vecino con parámetros personalizados además de aplicar las políticas generales del grupo. Pero si cada router se configurara individualmente el proceso de actualización tiene que ser individual también esto sobrecarga el trabajo de los routers, mientras que el efecto es contrario al hacerse en grupos, se alivia la carga a los routers. Los miembros del grupo deben ser externos e internos.

Se utiliza el comando neighbor peer-group-name para crear el grupo y asociar a los peer dentro de un AS.

Router(config-router)#neighbor peer-group-name peer-group

Router(config-router)#neighbor ip-address | peer-group-name remote-as autonomoussystem-number

Router(config-router)#neighbor ip-address peer-gruoup peer-group-name

Configuración de los router de la figura No. 17.

EMPRESA_1(config)#router bgp 150
EMPRESA_1(config-router)# bgp log-neighbor-changes
EMPRESA_1(config-router)# neighbor 10.0.0.2 remote-as 300
EMPRESA_1(config-router)# neighbor 172.16.0.2 remote-as 200

ISP_1(config)#router bgp 200

ISP_1(config-router)# bgp log-neighbor-changes
ISP_1(config-router)# neighbor 172.16.0.1 remote-as 150

ISP_2(config)#router bgp 300
ISP_2(config-router)# bgp log-neighbor-changes
ISP_2(config-router)# neighbor 10.0.0.1 remote-as 150

Características de BGP

El Internet ha crecido significativamente en las pasadas décadas. La actual tabla de BGP en el internet tiene más de 100,000 rutas. Muchas compañías tienen también implementado BGP para interconectar sus redes. Estos despliegues generalizados han probado la capacidad de BGP para soportar grandes y complejas redes.

La razón por la que BGP ha logrado su estatus en el internet hasta ahora es por las siguientes características:

- Accesibilidad
- Estabilidad
- Escalabilidad
- Flexibilidad

Capacidades de BGP

BGP, definido en RFC 1771, puede transportar solo información de accesibilidad en IPv4 entre peers. Para transportar otra información que no sea IPv4, BGP debe usar extensores. Esto se logra por las capacidades de intercambio y atributos de extensión. Así como está definido en RFC 1771, BGP soporta los siguientes cuatro tipos de mensajes. Explicados en la siguiente tabla: **[5]**

Funcionamiento	Descripción
Open	Este tipo de mensaje es usado para configurar lo inicial de las conexiones BGP.
Update	Estos mensajes son usados entre peers para intercambiar accesibilidad de información entre capas de red.
Notification	Estos mensajes se usan para comunicar condiciones de errores.
Keepalive	Estos mensajes son intercambiados periódicamente entre pares de peers para mantener la sesión abierta

Tabla 19 Mensajes de BGP

GUIA DE LABORATORIO 3: Configuración de BGP para el intercambio de información de ruteo entre dos ISP y un cliente.

OBJETIVOS

- Aprender a utilizar el programa GNS3
- Aplicar y reforzar conocimientos del protocolo de enrutamiento de Gateway exterior (BGP)
- Observar la manera que se intercambian la información de ruteo entre los ISP y un cliente que tiene distintos sistemas autónomos (AS)
- Aprender a configurar EBGP

INTRODUCCION

En la siguiente guía de laboratorio, se dará a conocer cómo funciona el protocolo de enrutamiento de dinámico de Gateway exterior BGP. Mediante un ejemplo en el que se evidencie como 3 empresas de proveedoras de servicios intercambian tablas de ruteo entre ellas.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt.

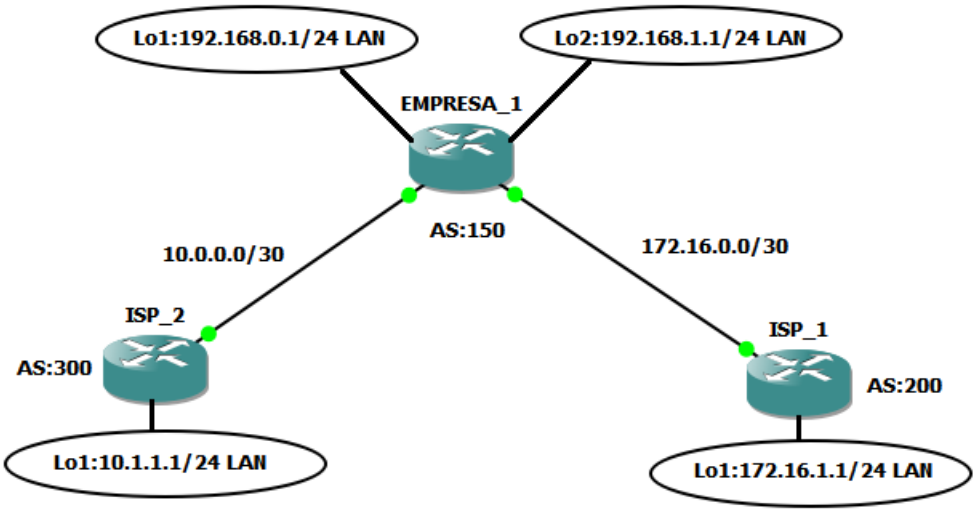


Tabla de direccionamiento

Equipo	Interfaz	Direccionamiento IP	Mascara
ENPRESA_1	GigabitEthernet1/0	10.0.0.1	255.255.255.252
	GigabitEthernet2/0	172.16.0.1	255.255.255.252
	Loopback0 (LAN)	192.168.0.1	255.255.255.0
	Loopback1 (LAN)	192.168.1.1	255.255.255.0
ISP_1	GigabitEthernet2/0	172.16.0.2	255.255.255.252
	Loopback0 (LAN)	172.16.1.1	255.255.255.0
ISP_2	GigabitEthernet1/0	10.0.0.2	255.255.255.252
	Loopback0 (LAN)	10.1.1.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

Usando el direccionamiento propuesto en el diagrama anterior, crearemos interfaces loopback y aplicaremos el direccionamiento IPV4 para estas, así como en las interfaces gigabitEthernet asociadas a ISP_1, ISP_2 y EMPRESA_1. Las loopbacks configuradas en los routers ISP simulan redes reales que pueden ser alcanzadas a través de los ISP.

Usar ping para probar la conectividad entre los routers directamente conectados. **Nota:** no se logra alcanzar las IP entre los router ISP_1 y ISP_2.

Paso 2.- Configurar BGP en los routers ISP (ISP_1, ISP_2)

En los routers ISP_1 y ISP_2. Configure BGP punto a punto con el router borde (EMPRESA_1) y anuncie las redes loopback de los ISP. Configure los AS según topología.

Paso 3.- Configurar BGP en el router borde EMPRESA_1.

Configurar el router EMPRESA_1 para que corra el protocolo BGP con los proveedores de servicio. Configure los AS según topología.

Para verificar que la configuración se encuentra aplicada correctamente. Se debe verificar la tabla de enrutamiento con el comando **show ip route**.

Pasó 3.- Verificar BGP en los routers

Para verificar la operatividad de BGP en el router EMPRESA_1, se utiliza el siguiente comando **show ip bgp**.

En EMPRESA_1. Usa el comando **show ip bgp neighbors**. Visualice los AS y id, versión de BGP.

CUESTIONARIO

1. ¿Cuál es el ID del router local? Demuestre con comandos
2. ¿Cuál es la versión de tabla mostrada?
3. ¿Cuál es la versión de tabla y es esta la misma versión de tabla bgp que la del router EMPRESA_1? Explique su respuesta
4. Para ISP_2, ¿Cuál es la ruta de la red 172.16.1.0/24?
5. ¿Cuál es la versión de la tabla mostrada? ¿Por qué?
6. ¿Qué paso con la ruta para la red 10.1.1.0/24?
7. ¿Cuál es el estado del bgp entre este router EMPRESA_1 y el ISP_2?
8. ¿Cuánto tiempo tiene de estar esta conexión activa?

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

Capítulo 4: MPLS

¿Qué es MPLS?

MPLS significa conmutación de Etiquetas Multiprotocolo. La cual es una tecnología que existe desde hace varios años y se ha vuelto muy popular, debido a que las etiquetas MPLS se anuncian entre routers para que puedan crear una asignación de etiqueta a etiqueta. Estas etiquetas se adjuntan a los paquetes IP, lo que permite a los enrutadores reenviar el tráfico mirando en la etiqueta y no en la dirección IP de destino. La idea general con MPLS es poner etiquetas en los paquetes de datos de entrada, basándose en su destino o cualquier otro criterio pre configurado. Con este tipo de tecnología se combina todo el tráfico de datos de paquetes de otras tecnologías en una estructura común. Siendo esta una gran ventaja que nos ofrece MPLS.

Beneficios de MPLS

- El uso de una infraestructura de red unificada.
- Mejor integración IP sobre ATM.
- Protocolo de puerta de enlace de frontera (BGP).
- El modelo peer-to-peer para MPLS VPN.
- Flujo de tráfico óptimo.
- Ingeniería de tráfico. **[6]**

La etiqueta MPLS.

Se basa en el enrutamiento de destino, las funciones de esta son separar las operaciones de envió desde los destinos de capa 3 que se encuentran en la cabecera de los paquetes con la asociación de una etiqueta con una FEC

(Forwarding Equivalence Class). La FEC son un grupo de paquetes IP enviados de la misma forma, sobre la misma ruta y con el mismo tratamiento salto por salto.

Las etiquetan definen el destino y el nivel del servicio. Esto proporciona un mecanismo por el cual los paquetes pueden ser ordenados en varios FEC sin necesidad de analizar la cabecera de capa 3. Dicho proceso se le conoce como Frame Mode MPLS.

20 bits	3 bits	1 bits	8 bits
Label	Exp Cos	S	TTL

Tabla 20 Etiqueta MPLS

- Label: 20 bits, esta es el propio campo de la etiquea. Puede tener valores desde 0 a 1048575.
- Experimental CoS: 3 bits, no está definido en la RFC 3031
- Bottom of Snack Indicator: 1 bit, es utilizado cuando existen multiples etiquetas MPLS en un mismo paquete. Puede tomar valores de 0 y 1. El valor 1 indica que esta etiqueta es la última del stack.
- Time to Live (TTL): 8 bits, cumple las mismas funciones que en la cabecera IP.

Envió de tráfico basado en etiquetas

Él envió de trafico MPLS es realizado por dispositivos que tiene la capacidad de realizar una búsqueda de etiquetas y sustituirla por la siguiente. Dichos dispositivos no analizan la cabecera IP. Sin embargo, la nomenclatura y su propósito es establecer la posición dentro de una arquitectura MPLS. Un LSR (Label Switching Routers) es un modo de MPLS para enviar tráfico de capa 3 basándose en la etiqueta correspondiente a cada paquete.

Los LSR deben tener la capacidad de funcionar en el plano de control y en el Data Plane, donde este último contiene la información de enrutamiento. Como ocurre en otros protocolos de enrutamiento.

MPLS funciona a través de etiquetas, incluso cuando cada LSR tenga una tabla de enrutamiento actualizada y en convergencia, este no tomara decisiones de envió de

enrutamiento. El LSR mantendrá su tabla de enrutamiento actualizada, para asegurar que la FIB este renovada a la versión más reciente. Con el objetivo de que las etiquetas sean asignadas de manera correcta y que los paquetes lleguen a su destino.

Un dispositivo LSR asume el envío de paquetes con el añadido funcional de tener que eliminar o remover etiquetas. Si un paquete etiquetado recibido se pierde, es debido a que faltan datos en la LFIB, incluso si el destino esta mapeado en la tabla de enrutamiento.

LIB, LFIB Y FIB

Estos tres términos están asociados, pero a su vez son independientes. La configuración correcta de un protocolo de enrutamiento avanzado puede limitar los efectos de convergencia en la red. MPLS depende del protocolo de routing subyacente para tomar la información necesaria y construir las LFIB (Label Forwarding Information Base). Las cuales constituyen la tabla de rutas de las etiquetas.

Las etiquetas son compartidas a través de protocolos de distribución, pero la información se construye inicialmente por medio de los protocolos de enrutamiento. Si la red IP experimenta problemas de convergencia u otras inestabilidades. Esto afectara de manera directa a la red MPLS. Tomando en cuenta lo anterior una vez que la tabla de enrutamiento se construye y la red converge. El LSR asigna etiquetas a cada destino reflejado en la tabla de enrutamiento, lo cual tiene un significado local y se almacenan en la LIB (Label Information Base).

Cada LSR anuncia sus etiquetas a los vecinos adyancentes quienes a su vez lo hacen con sus pares. Estos últimos asocian información de etiquetas recibidas asociándolas con el siguiente salto con el fin de alcanzar el destino deseado. Toda esta información se almacena en las FIB y LFIB.

La LIB forma parte del plano de control cuya base datos es utilizada por el LDP para la distribución de etiquetas. Esta también mantiene el enlace entre los prefijos IP, la etiqueta asignada y la etiqueta que se asignara.

La LFIB es parte del Data Plane y funciona como base de datos utilizada para enviar paquetes ya etiquetados. El IGP se utiliza para publicar la tabla enrutamiento a todos los router MPLS a través de la red.

Distribución de Etiquetas

MPLS anexa una sobrecarga adicional para la comunicación entre routers adyacentes, sumada a la propagación de prefijos de enrutamiento se agregan funcionalidades de mantenimiento de las LIB y LFIB junto con tablas de adyacencia, generando un consumo de recursos extras CEF (Cisco Express Forwarding), LDP y otros procesos que contribuyen al aumento de recursos.

Se tiene que tomar en cuenta que la arquitectura MPLS permite dos formas de propagar la información necesaria.

- Extender la funcionalidad de los protocolos existentes.
- Crear nuevos protocolos dedicados a la tarea de intercambio de etiquetas.

En una arquitectura MPLS la decisión de asignar una etiqueta en particular a una FEC es propiedad el LSR en cada host a lo largo del camino. El LSR anterior informa al siguiente LSR sobre las etiquetas decidas para esa FEC. Esto conlleva a que las etiquetas sean asignadas en orden ascendente hacia el destino.

El flujo se tráfico es un factor importante tomando en cuenta que se da en un sentido bidireccional, lo que quiere decir que las etiquetas serán propagadas en ambas direcciones. Split Horizon hace que las etiquetas sean distribuidas en orden descendentes evitando que se propaguen hacia el vecino que las propago. La FIB está sujeta a las normas de horizonte dividido por defecto desde el punto de vista de enrutamiento.

Propagación de paquetes

Un paquete de entrada puede ser enviado de múltiples maneras incluyendo con o sin imposición de etiquetas. El dispositivo LSR frontera será el encargado de ejecutar Pop para quitar la etiqueta.

Cuando un paquete llega a un LSR antes de que tenga conocimiento de la etiqueta asociada a la FEC para reenviar el paquete ya etiquetado, el envío se realizara basándose en la información almacenada en la FIB. Este paquete será enviado al próximo salto según dicha información. El router siguiente realizara una búsqueda tratando de encontrar la información del mapeo de la etiqueta con la FEC correspondiente. En caso que la tenga incluye la etiqueta y envía el paquete. En caso contrario se repetirá el proceso.

PHP

Cuando existe una ruta MPLS desde el origen hacia un destino se crea un LSP (Label Switched path), que es un túnel entre ambos extremos basándose en una FEC particular. Se puede decir que este túnel asocia varios caminos posibles debido a que pueden existir varias FEC que compartan etiquetas en algún punto en particular de este camino. Los LSR frontera contienen una FEC en especial, que permite ejecutar un mecanismo llamado PHP (Penultimate hop popping).

PHP es característica propia de MPLS la cual es habilitada por defecto. Un LSR frontera de salida realiza una búsqueda en la LFIB para localizar paquetes etiquetados. En caso de que la red se encuentre directamente conectada no incluye ninguna etiqueta para este destino en particular. Por tanto, la etiqueta es removida y se realiza una búsqueda en la FIB.

Configuración de MPLS

La configuración en los routers MPLS es simple, teniendo en cuenta el tamaño de la red y el número de prefijos que serán propagados. En un entorno de proveedor de servicio, el router debe mantener toda la tabla de internet sumando más de 300,000 prefijos.

La idea del protocolo MPLS es aplicar etiquetas entre los campos de capa 3 y capa 2, aunque la adición de 4 Bytes podría causar que tramas mayores de lo permitido por las MTU configuradas en la interfaz no permitieran pasar dichas tramas. Esta es una de las configuraciones que se deben tomar en cuenta.

Configuración de CEF

Es un sistema de conmutación rápido y eficiente. CEF (Cisco Express Forwarding) proporciona un mecanismo de conmutación en capa 3 que optimiza el rendimiento y estabilidad en redes grandes. Ya que consume menos recursos de CPU que otros mecanismos, lo que permite liberar CPU para el uso de otras aplicaciones.

CEF puede ser ejecutado de modo central o modo distribuido. En modo central solo es permitida una sola instancia en cada router. Mientas CEF en modo distribuido (dCEF) está diseñado para ser ejecutado por un router gama alta, permitiendo a cada tarjeta del router ejecutar y mantener su propio mecanismo de conmutación.

CEF utiliza la FIB para mantener actualizada su tabla de adyacencia. Donde la FIB es utilizada para tomar decisiones a nivel IP y la tabla de adyacencia proporciona información a nivel de capa 2 incluyendo la información del próximo salto de dicha capa. Ambas constituyen la base operacional de CEF.

Para Habilitar CEF de manera global se realiza de la siguiente manera, esto se aplica en la figura 18:

```
PE1(config)#ip cef
```

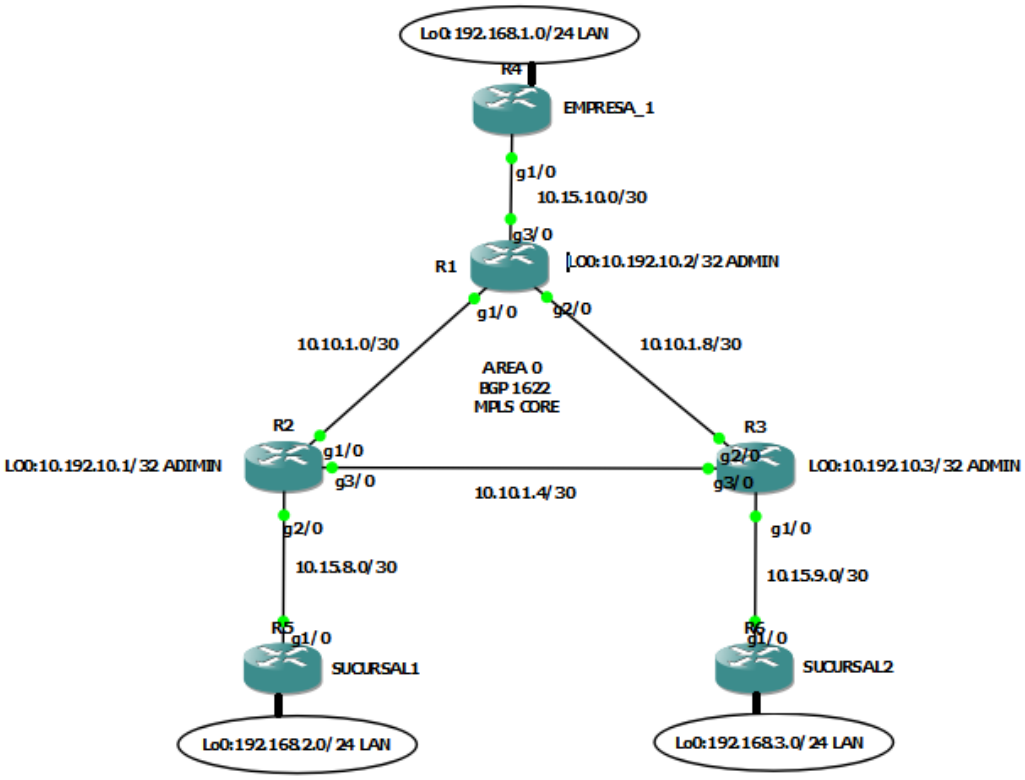


Figura 18 Topología de red con MPLS

La implementación de MPLS consiste en la configuración de los parámetros de la interfaz, esto significa la habilitación de un protocolo de etiquetas en algunos entornos se utiliza el protocolo propietario de cisco TDP (Tag Distribution Protocol). Pero este no es un estándar compatible con otros fabricantes. Por lo que posteriormente fue estandarizado el protocolo LDP (Label Distribution Protocol).

Para habilitar MPLS en un router basta con el comando *mpls ip* en el modo de configuración global o en cada una de las interfaces donde se ejecute. Este debe de configurarse de manera individual en cada interfaz que participen en el entorno MPLS, para proceder a habilitar un protocolo de distribución con el comando *mpls label protocol*.

La siguiente Tabla muestra los parámetros que pude tener el comando.

Parámetro	Descripción
Both	Para utilizar LDP o TDP
Ldp	Para LDP
Tdp	Para TDP

Tabla 21 Tipos de MPLS

El parámetro both es utilizado en interfaces multi-acceso donde el vecino pueda ejecutar ambos protocolos.

Se recomienda aplicar ACL en las interfaces que no son MPLS, para bloquear tráfico TDP o LDP. Ambos utilizan puertos UDP para excluir a los vecinos y posteriormente TCP establece sesiones que funcionan como transporte de este protocolo. TDP utiliza los puertos TCP/UDP 711 y LDP utiliza los puertos TCP/UDP 646. UDP se utiliza para el descubrimiento de vecinos.

Sin el comando *mpls ip* habilitado en las interfaces las adyacencias no se establecerán. En un entorno con varios fabricantes se debe tener la precaución de no ejecutar TDP debido a que solo tiene funcionalidad dentro de los routers cisco.

A continuación, los comandos:

```
PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id Loopback0

PE1(config)#interface GigabitEthernet1/0
PE1(config-if)#mpls ip

PE1(config)#interface GigabitEthernet2/0
PE1(config-if)#mpls ip
```

Configuración de la MTU

El agregado de una o más etiquetas al paquete que va atravesando la red MPLS podría causar un exceso de tamaño de la MTU en las interfaces. Esto suele ocurrir en las interfaces LAN donde la MTU es de 1500 bytes. La mayoría de las interfaces WAN poseen un MTU mayor.

El tamaño del MTU debe ser incrementado por una cantidad igual o superior a los bytes del agregado de etiquetas. Pero si se añaden 4 bytes solo será posible insertar una sola etiqueta. Por lo que se aconseja dejar el MTU en 1512 bytes o mayor.

Se utiliza el siguiente comando dentro interfaz para cambiar en valor MTU

PE1(config-if)#mpls mtu override 1512

El rango posible para el tamaño de MTU es de 64 a 65535 bytes.

Una solución brindada por MPLS para la interconexión de sucursales de clientes es lograda mediante la utilización de la tecnología VPN. **[5]**

¿Qué es una VPN?

VPN emula una red privada sobre una estructura común. Las VPN pueden proveer comunicación en la capa 2 o 3 del modelo OSI. Usualmente pertenecen a una compañía, que posee varios enlaces interconectados a través de una infraestructura común de proveedores de servicios. Las redes privadas requieren que todos los sitios de clientes puedan interconectarse y estar completamente separados de otras VPN. Este el requerimiento mínimo de conectividad. Sin embargo, los modelos VPN en la capa IP pueden tener mayores requerimientos. Estas pueden proveer conectividad entre diferentes VPN cuando esto se requerido y brindar conectividad hacia internet. **[6]**

Tipos de VPN

Sevilla (2010) este ha determinado los siguientes tipos:

•Overlay VPN o tradicionales. Incluyen tecnologías como X.25, Frame Relay, ATM, para VPN capa 2 y túneles GRE e IPsec para VPN 3.

•Peer to peer VPN. Son implementadas con ISP compartidos y las infraestructuras son realizadas con ACL para la separación de distintos clientes.

MPLS-VPN

La combinación de las tecnologías MPLS y VPN brindan una solución WAN de capa 3 o red, para solventar los problemas WAN de la capa de enlace datos (capa 2). Estas aportan una conectividad entre muchos sitios de manera asequible y competente. Mediante el establecimiento de redes WAN en los circuitos existentes a nivel de capa 2. Este beneficio ha sido de gran utilidad para los ISP.

¿Por qué usar MPLS-VPN?

El uso de esta tecnología trae consigo grandes aportes en las redes de datos, ya que engloba las VPN tradicionales y las VPN peer to peer al mismo tiempo. Estas son precisamente implementaciones de VPN peer to peer en las que la información de enrutamiento de cada cliente es guardada de manera segura y separada del resto de la información de los otros clientes mediante los RD (Route Distinguisher), que hacen que cada cliente sea único. El uso de los RD permite al ISP darle a cada cliente una separación lógica del resto, aunque no estén físicamente separados puesto que comparten la misma infraestructura.

Terminología de MPLS-VPN

Sevilla (2010). Resume las siguientes terminologías sobre MPLS VPN:

- C network**:** red interna del cliente.
- CE**:** router del cliente que se conecta al PE.
- Label-Switched Path (LSP): es la ruta establecida para el uso de etiquetas en los paquetes a través de la red P en el tránsito hacia un destino en particular.
- P network: red del proveedor de servicio.
- P router**:** es el router MPLS en el core o backbone de la red y nunca está de cara al cliente. No lleva rutas VPN.
- PE router: es el router MPLS del ISP, contiene rutas VPN y es el dispositivo que se conecta al router CE.
- Penultimate Hop Pop (PHP): es el router P anterior al router P de destino y que se encarga de quitar la etiqueta y entregar el paquete al router PE.
- PoP**:** punto de presencia del ISP.
- Route Distinguisher (RD): es un identificador de 64 bits que se antepone delante de la dirección IPv4 haciendo que este sea globalmente única.
- Route Target (RT): es un atributo que se asocia a las rutas VPNv4 BGP.
- Virtual Routing and Forwarding table (VRF): es una instancia de enrutamiento específica para un cliente.

A continuacio se muestra una topología con la terminología de MPLS, ejemplo que ayuda a visualizar a una empresa, las sucursales y la red del ISP.

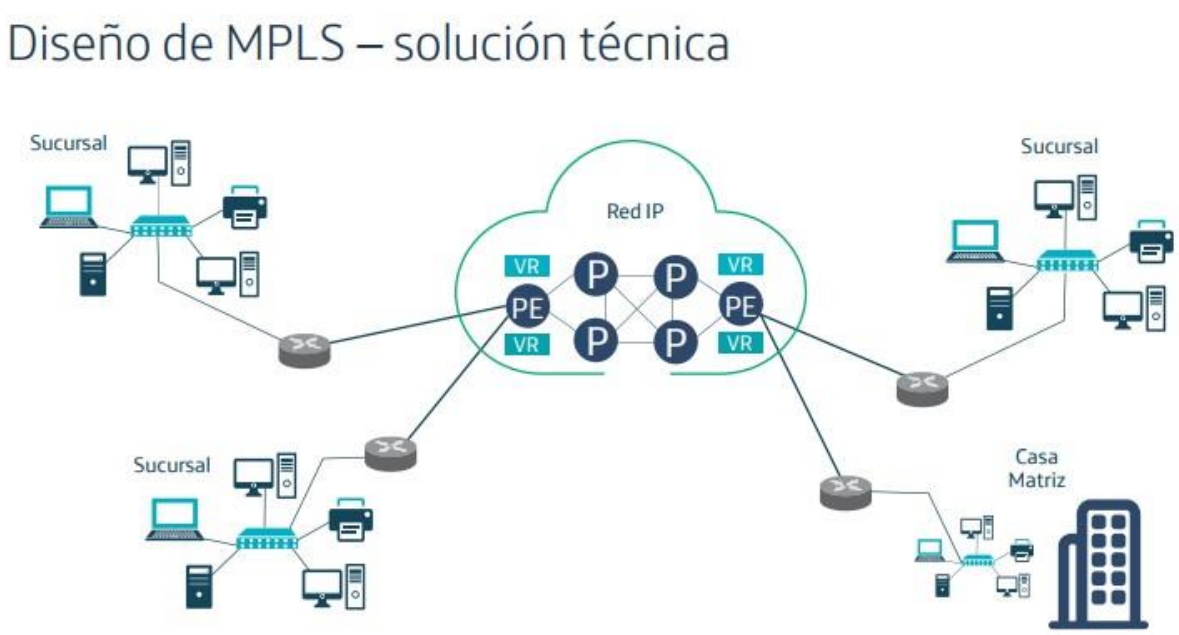


Figura 19 Ejemplo de Red MPLS-VPN

Tipos de Router en MPLS-VPN

Arquitectura del Router CE: Este es el equipo terminal de cliente el cual se encarga de intercambiar tablas de enrutamiento con su respectivo PE independiente del protocolo que se tenga configurado. Cabe mencionar que el CE no conoce el mecanismo MPLS y no participa en la arquitectura.

Arquitectura del Router PE: Están integrados por dispositivos de gama alta, donde se encuentra comprimida su arquitectura en un solo equipo.

Dichos equipos son capaces de asignar al cliente un RD y su tabla VRF dedicados para mantener los procesos de enrutamiento dentro de la infraestructura del proveedor o ISP. Donde el PE se encarga de ejecutar múltiples instancias de protocolos de enrutamiento para mantener rutas específicas del cliente y dentro del Core ISP. Las VRF se encargan de proporcionar el aislamiento de rutas al cliente y la información que estas contienen las cuales serán intercambiadas por distintos PE.

El Protocolo BGP. Proporciona escalabilidad y flexibilidad requeridas para mantener el enrutamiento entre todos los PE, lo que les permite intercambiar los prefijos de un cliente.

Arquitectura P: Estos forman parte de la red Backbone. Y no llevan información de clientes debidos a que estos utilizan protocolo como OSPF y BGP. Los cuales funcionan únicamente sobre la red del proveedor y solo poseen información de la red P en sus tablas de enrutamiento. Así como interactuar con los PE para el intercambio de tráfico BGP y trasladar información de enrutamiento a los PE remotos. BGP es el protocolo preferido por la red P. **[5]**

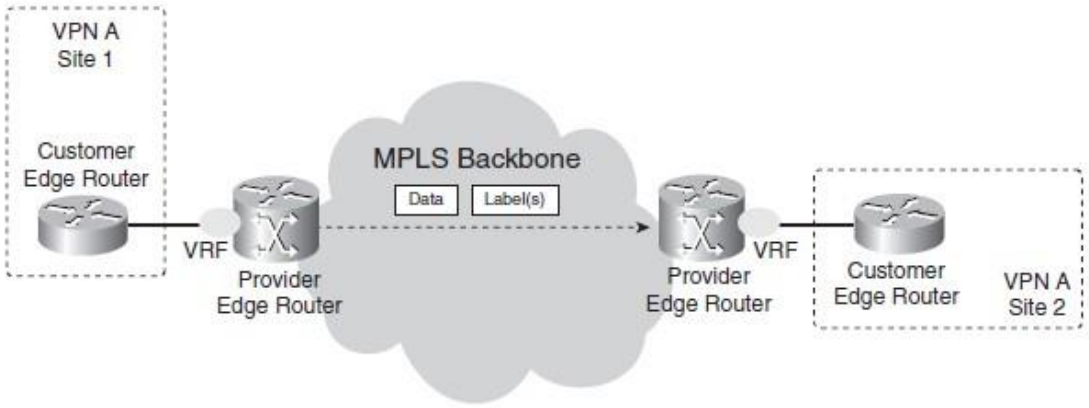


Figura 20 Peer to peer MPLS-VPN Backbone

Como funciona MPLS VPN

MPLS VPN habilita las siguientes funciones en el dispositivo PE.

- Intercambiar actualizaciones de enrutamiento con el dispositivo perimetral del cliente (CE).
- Traduce la información de enrutamiento del CE a rutas VPNv4.
- Intercambia rutas VPNv4 con otros dispositivos PE a través del protocolo de puerta de enlace multiprotocolo (MP-BGP).

Estas VPN pueden estar asociadas con una o más VRF (Virtual routing forwarding) instancias. Una VRF define los miembros de una VPN de un sitio del cliente conectado al dispositivo PE. Esta puede constar de los siguientes componentes.

- Tabla de enrutamiento IP.
- Tabla de CEF (Cisco Express Forwarding)
- Establecer interfaces que usaran la tabla de reenvió de rutas.
- Establecer regalas y parámetros de protocolo de enrutamiento que controlan la información que se agrega la tabla de enrutamiento.

La distribución de la información de enrutamiento de las VPN es controlada mediante el uso de VPN router target communities. Implementado por BGP extended communities. Esta información es distribuida:

- Cuando una ruta VPN es aprendida por el dispositivo CE es inyectado al BGP, a una lista de VPN route target extended community al cual está asociado.
- Una lista de importación route extended communities esta asociada con cada VRF. Dicha lista define los atributos que debe de tener una ruta para que esta sea importada a la VRF.

Distribución del BGP en la información de enrutamiento VPN
Para que un dispositivo PE pueda aprenderá prefijos IP debe seguir lo siguiente:

- Configuración estática del dispositivo CE.
- Sesión de BGP con el dispositivo CE.
- Intercambio de información enrutamiento con el dispositivo CE.

El prefijo IP es miembro del IPV4 address family. Luego que el dispositivo PE aprende el prefijo, lo convierte en un prefijo VPN-IPv4 mediante la combinación con los 8 bytes de RD. Lo que genera un prefijo miembro de VPN-IPv4 address family. Esto identifica de forma exclusiva la dirección del cliente. Incluso si el cliente no utiliza direcciones IP no únicas (Privadas). El RD es utilizado par generar el prefijo VPN-

IPv4 especificado por el comando asociado con la instancia VRF en el dispositivo PE.

BGP distribuye información de accesibilidad para los prefijos VPN-IPv4 para cada VPN. Esta comunicación se produce en dos niveles:

- Dentro de un dominio IP, conocido como AS (BGP Interior [IBGP]).
- Entre Sistemas autónomos (BGP external, [EBGP]).

MPLS basado en VPN tiene tres componentes principales:

- VPN route target communities: Es una lista de todos los miembros de la comunidad VPN. VPN route targets deben configurarse para cada VPN community member.
- Multiprotocol BGP (MP-BGP): Este propaga la información de accesibilidad de las VRF a todos los miembros de la comunidad VPN. MP-BGP peerring debe de estar configurado en todos los dispositivos PE dentro de una comunidad VPN.
- MPLS forwarding: transporta todo el tráfico entre todos los miembros de la comunidad VPN a través de una red de proveedores de servcios VPN. **[7]**

Se describirá la configuración de MP-BGP en la siguiente tabla:

Comando	Propósito
PE1(config)#router bgp 1622	Configuración del proceso BGP y accesar al modo de configuración.

PE1(config-router)#neighbor 10.192.10.2 remote-as 1622 **PE1(config-router)#neighbor 10.192.10.2 update-source Loopback0** **PE1(config-router)#neighbor 10.192.10.3 remote-as 1622** **PE1(config-router)#neighbor 10.192.10.3 update-source Loopback0**	Se agrega una tabla de adyacencia BGP o multiprotocolo BGP. Se especifica la dirección IP del vecino. El argumento as-number define el sistema autónomo al que pertenece el vecino.
PE1(config-router)# address-family ipv4 **PE1(config-router-af)#neighbor 10.192.10.2 activate** **PE1(config-router-af)#neighbor 10.192.10.3 activate** **PE1(config-router-af)#exit-address-family**	Permite el intercambio de información con un dispositivo BGP vecino. El argumento de la dirección ip especifica la dirección IP del vecino. El argumento nombre-grupo-igual especifica el nombre de un grupo igualitario de BGP.
PE1(config-router)#address-family vpnv4	Entra en el modo de configuración de la familia de direcciones para configurar sesiones de enrutamiento, como BGP, que usan prefijos de dirección VPNv4 estándar. La palabra clave unicast opcional especifica los prefijos de dirección de unicast VPNv4.
PE1(config-router-af)# neighbor 10.192.10.2 send-community extended	Especifica que un atributo de comunidades debe enviarse a un vecino BGP.

PE1(config-router-af)# neighbor 10.192.10.3 send-community extended	El argumento de dirección ip especifica la dirección IP del vecino que habla BGP. El argumento nombre-grupo-igual especifica el nombre de un grupo igualitario de BGP.
PE1(config-router-af)#neighbor 10.192.10.2 activate **PE1(config-router-af)#neighbor 10.192.10.3 activate**	Permite el intercambio de información con un dispositivo BGP vecino. El argumento de la dirección ip especifica la dirección IP del vecino. El argumento nombre-grupo-igual especifica el nombre de un grupo igualitario de BGP.

Tabla 22 Configuración de MP-BGP

VRF o Virtual Route Forward es una técnica que crea múltiples redes virtuales dentro de una sola entidad de red. En un solo componente de red, múltiples recursos VRF crean el aislamiento entre redes virtuales.

La seguridad se puede mejorar implementando la virtualización en el nivel de la red. La tecnología VRF puede ser utilizada con las reglas y políticas para que cada red VRF logre el nivel de seguridad esperado. Estas pueden ser configuradas de la siguiente manera. **[8]**

Comando	Propósito
PE1(config)#Vrf definition *EMPRESA_1*	Define la instancia de enrutamiento de VPN asignando un nombre VRF e ingresa VRF modo de configuración. El argumento *vrf-name* es el nombre asignado a la VRF.
PE1(config-vrf)# rd 16:22	Crea tablas de enrutamiento y reenvío. • El argumento diferenciador de ruta agrega un valor de 8 bytes a un prefijo IPv4 para crear un prefijo VPN IPv4. Puede ingresar un RD en cualquiera de estos formatos: • Número AS de 16 bits: su número de 32 bits, por ejemplo, 101: 3 • Dirección IP de 32 bits: su número de 16 bits, por ejemplo, 10.0.0.1:1
PE1(config-vrf)# address-family ipv4 **PE1(config-vrf-af)#route-target export 16:22**	Crea una comunidad extendida de destino de ruta para un VRF.

PE1(config-vrf-af)#route-target import 16:22	• La palabra clave de **import** importa información de enrutamiento desde la VPN objetivo comunidad extendida • La palabra clave de **export** exporta información de enrutamiento a la VPN objetivo comunidad extendida. • La palabra clave **both** importa información de enrutamiento y exporta enrutamiento Información a la comunidad extendida VPN objetivo. • El argumento route-target-ext-community agrega la ruta-target extendida atributos de la comunidad a la lista de VRF de importación, exportación o ambos (importación y exportar) comunidades extendidas de ruta-destino.
PE1(config)#interface GigabitEthernet3/0 **PE1(config-if)# vrf forwarding EMPRESA_1** **PE1(config-if)#ip address10.15.10.1 255.255.255.252** **PE1(config-if)# negotiation auto**	Estos comandos son utilizados para asociar una interfaz a una VRF, con su debido direccionamiento hacia el CPE o equipo del cliente.
PE1(config)#router bgp 1622 **PE1(config-router)# address-family ipv4 vrf EMPRESA_1** **PE1(config-router-af)# redistribute connected**	Especifica el tipo de familia de direcciones IPv4 e ingresa en el modo de configuración de la familia de direcciones.

PE1(config-router-af)# redistribute static **PE1(config-router-af)# exit-address-family**	• La palabra clave de multidifusión especifica los prefijos de dirección de multidifusión IPv4. • La palabra clave de unidifusión especifica los prefijos de direcciones de unidifusión IPv4. • La palabra clave y el argumento vrf vrf-name especifican el nombre del VRF para asociarlo con los siguientes comandos del modo de configuración de la familia de direcciones IPv4.

Tabla 23 Configuración VRF

GUIA DE LABORATORIO 4: Configuración de MPLS L3, VPN-MPLS para cliente EMPRESA_1.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Configurar OSPFv2 de área única IPv4.
- Configurar el protocolo de etiqueta MPLS LDP.
- Configurar el protocolo dinámico BGP.
- Configuración de VRF para servicios de clientes. Haciendo uso de la tecnología MPLS L3 VPN.

INTRODUCCION

En la siguiente guía de laboratorio, se realizarán las configuraciones de una red MPLS-VPN donde se configura la casa matriz junto con sus sucursales del cliente EMPRESA_1 para que posean conectividad utilizando la infraestructura del proveedor. Igualmente se configura un anillo MPLS con redundancia, este simula una red WAN de un ISP.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

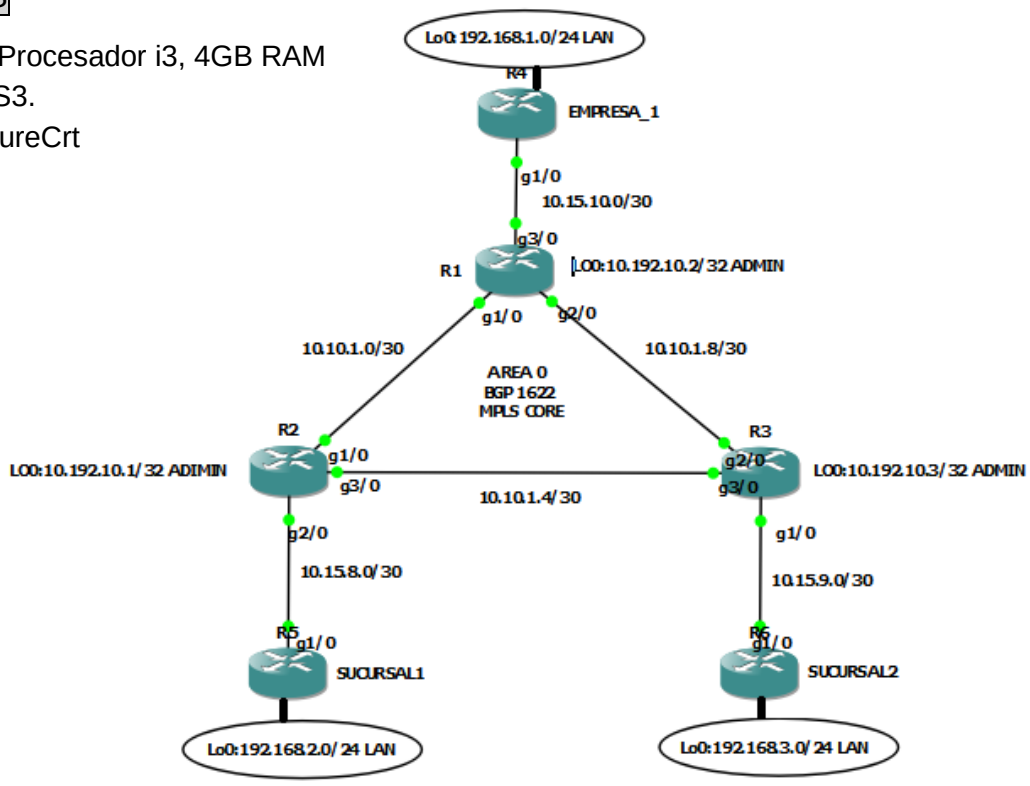


Tabla de direccionamiento

Equipo	Interfaz	Dirección IP	Mascara
R1	Loopback0 (Admin)	10.192.10.1	255.255.255.255
	GigabitEthernet1/0	10.10.1.1	255.255.255.252
	GigabitEthernet2/0	10.10.1.9	255.255.255.252
	GigabitEthernet3/0	10.15.10.1	255.255.255.252
R2	Loopback0(Admin)	10.192.10.2	255.255.255.255
	GigabitEthernet1/0	10.10.1.2	255.255.255.252
	GigabitEthernet3/0	10.10.1.5	255.255.255.252
	GigabitEthernet2/0	10.15.8.1	255.255.255.252
R3	Loopback0(Admin)	10.192.10.3	255.255.255.255
	GigabitEthernet2/0	10.10.1.10	255.255.255.252
	GigabitEthernet3/0	10.10.1.6	255.255.255.252
	GigabitEthernet1/0	10.15.9.1	255.255.255.252
R4	GigabitEthernet1/0	10.15.10.2	255.255.255.252
	Loopback0 (LAN)	192.168.1.1	255.255.255.0
R5	GigabitEthernet1/0	10.15.8.2	255.255.255.252
	Loopback0 (LAN)	192.168.2.1	255.255.255.0
R6	GigabitEthernet1/0	10.15.9.2	255.255.255.252
	Loopback0 (LAN)	192.168.3.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

En este laboratorio, se configurara una red OSFPv2 multi-área para IPV4. El área 2 se configurará como un área normal de OSPF, un área de código auxiliar y usando el direccionamiento propuesto en el diagrama anterior, aplicaremos el

direccionamiento IPV4 para las interfaces gigabit Ethernet e interfaces virtuales. Las loopbacks configuradas en los routers simulan segmentos de redes reales.

Realizar pruebas de conectividad a nivel L3, mediante ping.

Paso 2.- Configurar OSPF en los routers.

Crea proceso (1) OSPFv2 en los router PE1, PE2 y PE3. Configurar el OSPF Router ID en cada uno de ellos (*PE1=10.192.10.1, PE2=10.192.10.2, PE3=10.192.10.3*). Habilitar redes directamente conectadas en el proceso OSPF utilizando **ip ospf *process-id* área *área-id***. En este caso se utilizara como ***router-id*** la Lo0 de admin.

Configurar router OSPFv2 en área 0 para los equipos PE

Nota: se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro del proceso OSPF 1 para que este redistribuya las rutas estáticas y las conectadas directamente al equipo.

Verificar que los routers tengan vecinos OSPFv2. Utilizando el **comando show ip ospf neighbors**.

Verificar que el router R1 pueda ver todas las redes IPv4 en la tabla de enrutamiento OSPFv2 usando el comando **show ip route**.

Paso 3.- Habilitar el protocolo MPLS LDP en los Router PE.

Se procederá a habilitar MPLS en los equipos PE1, PE2 y PE3. Antes de comenzar con dichas configuraciones se debe de aplicar el comando ***ip cef***. Luego se deberá activar el protocolo LDP con el comando ***mpls label protocol ldp*** dentro del modo de configuración, seguido del comando ***mpls ldp router-id Loopback0*** en el cual se le indica al router que recibirá actualizaciones por medio de la Lo0. Esto se realiza

para evitar que el router tenga conflictos por elección de IP, y que pueda quedar desactualizado por esta razón.

Luego se debe definir y configurar las interfaces que van a participar dentro del protocolo MPLS, con el siguiente comando ***mpls ip*** dentro de la interfaz en cuestión. Esto habilitara el protocolo y permitirá agregar un encabezado a la trama IP que servirá como etiqueta. Con la facilidad que se permita intercambiar paquetes entres los equipos PE (CORE) e identificar el destino de cada paquete sin tener que analizar toda la trama. Lo que evita que el equipo sature su CPU.

Deberá agregarse dentro el proceso OSPF 1 el comando ***mpls ldp sync*** para que MPLS tenga sincronía a través del protocolo de enrutamiento dinámico. Y el comando ***mpls ldp autoconfig*** lo que hace referencia que tendrá una configuración automática con sus demás adyacencias.

Procederemos a verificar las vecindades de MPLS en el equipo PE1, utilice el comando **show mpls ldp neighbor.**

Paso 4. -Se habilitará protocolo de Gateway Exterior BGP.

Dentro de los equipos PE se habilitará el proceso BGP con el AS de 1622. Utilizando el comando ***router bgp*** dentro del modo de configuración. Seguido del comando ***bgp log-neighbor-changes*** el que permite que el equipo reciba actualizaciones de base de datos de rutas aprendidas por sus vecinos. Sus peers de vecinos serán configurados mediante el comando **neighbor x.x.x.x remote-as xxxx** y recibirán actualizaciones de cambio por la interfaz **lo0**. Utilizando el comando **neighbor x.x.x.x update-source lo0**.

Luego se debe ingresar al modo de configuración **address-family ipv4**, habilita el intercambio de información con un peer BGP, posteriormente se define las redes vecinas con sus máscaras con el comando **network *x.x.x.x*** (Red) **mask *x.x.x.x***

(Mascara). Despues se procederá a definir a los peers vecinos en modo activo usando el comando **neighbor *x.x.x.x*** (Lo0 vecinos) **active.** Utilice **exit-address-family** para salir de ese modo de configuración.

Habilitar en los routers PE en el modo de configuración de BGP el comando **address-family vpnv4**, el cual habilita secciones de enrutamiento para prefijos de direcciones VPNv4. Se declara nuevamente los peers vecinos en modo activo y luego de cada peer vecino se utiliza el comando **neighbor *x.x.x.x*** (Lo0 vecinos) **send-community extended**, el cual especifica las comunidades que deben ser enviadas a un peer BGP vecino.

Nota: se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro del modo de configuracion family-addess para que este redistribuya las rutas estáticas y las conectadas directamente al equipo

Una vez configurado los peer vecinos para intercambio de rutas a nivel BGP. Se deberá confirmar las tablas de IP BGP en cada PE de la topología. Para identificar las vecindades, el sistema autónomo al que pertenecen, el tipo de tabla y la versión que está utilizando. Para esto se usarán los comandos **show ip bgp summary, show ip bgp**.

Paso 5. –Configuración de MPLS-VPN.

Una vez configurado los enrutamientos dinámicos en cada PE, se procederá con las configuraciones de MPLS L3 VPN. Donde se configurará las VRF o virtual route forward con el comando **vrf definition** *NombredelaVRFdelCliente* (EMPRESA_1) y se definirá el route-distinguisher con el comando **rd** (16:22). Utilizando el comando **address-family** indicaremos que este cliente intercambiara rutas en IPv4. Usar los comandos **route-target export** y **route-targe import** para indicar al address-family por cual RD se importará y exportaran las direcciones IPv4. Utilice **exit-address-family** para salir de ese modo de configuración.

Nota: El sistema autónomo (AS) de BGP es 1622 y el RD (route-distinguisher) del cliente es 16:22, estos no tienen relación y pueden ser distintos números, pero por casualidad son los mismo en esta topología. El RD dentro de la VRF es el ID único de cada cliente para identificarlos en la red MPLS.

Después de que se definió el nombre de la VRF y su RD (route-distinguisher). Se debe configurar las rutas que se van a importar y exportar IPv4 dentro del proceso BGP 1622. Para esto se utilizan los comandos **address-family** *familiaIP* **vrf** *NombredelaVRFdelCliente*. Para luego ser aprendidas por los PE vecinos. Se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro de la address-family asociada vrf del cliente en proceso BGP, para que este redistribuya las rutas estáticas y las conectadas directamente al equipo.

Luego de distribuir la VRF para el cliente EMPRESA_1 dentro del BGP 1622. Donde se tomará en cuenta las rutas estáticas y directamente conectadas para crear conectividad entre las 2 sucursales y la casa matriz haciendo uso de la infraestructura de un proveedor. Se deberá definir interfaces WAN y direccionamiento a utilizar entre el PE y el CPE, según tabla de direccionamiento y topología. Dentro de las interfaces físicas se debe configurar el **comando vrf forwarding** *NombredelaVRFdelCliente, con esto se asocia la interfaz física a la vrf del cliente.*

Se deberá crear una ruta estática asociada a la IP WAN del CPE del cliente para lograr enrutar el segmento LAN interno del cliente. Mediante el comando **ip route vrf** *NombredelaVRFdelCliente* ***x.x.x.x*** *(LAN)* ***x.x.x.x*** *(Mask)* ***x.x.x.x*** *(WAN CPE)* **name** *Descripcion,* dentro del modo de configuración de los routers core MPLS. Use tabla de direccionamiento y topología.

Se debe configurar las interfaces físicas y virtuales en los CPE del cliente, utilice tabla de direccionamiento y topología. Luego configure una ruta estatica por defecto en cada CPE con el comando **ip route 0.0.0.0 0.0.0.0** ***x.x.x.x*** (Gateway).

Una vez detallada la configuración de cada CPE del cliente. Observamos que no presenta mayor complejidad, más que una interfaz como enlace WAN hacia el proveedor, la creación de una lo0 para simular la LAN del cliente por ultimo, pero no menos importante una ruta por defecto apuntando hacia el siguiente salto, que permita que todas las redes sean alcanzadas desde cualquier sucursal o casa Matriz. Realizar pruebas de conectividad de entre los equipos de la casa matriz y sus sucursales.

Como practica final se deberá habilitar los comandos ***debug ip ospf adj, debug ip bgp events*** *y* ***debug mpls ldp bindings*** en el R1, seguido del apagado la interfaz GI2/0 en el R3. Se deberán observar los cambios de estados de los protocolos OSPF, BGP y MPLS.

CUESTIONARIO

1. Si se pregunta por la red 192.168.3.1 configurada como puerta de enlace para la LAN de la sucursal SUCURSAL2 en el PE1 sobre la vrf EMPRESA_1 ¿Qué resultado obtenemos como respuesta?

2. ¿Debería de haber conexión vía ping entre las sucursales y la EMPRESA_1? ¿Por qué?

3. ¿Cuantas rutas OSPFv2 intra-area hay en el router PE1 dentro su tabla de enrutamiento IPV4?

4. ¿Por qué el Router PE3 se encuentra en estado FULL/BDR?

5. ¿Qué direccionamiento en el PE2 es utilizado para establecer adyacencia de vecindad con el PE1?

6. ¿Qué direccionamiento en el PE3 es utilizado para establecer adyacencia de vecindad con el PE1?

7. ¿Qué comportamiento se observa en el PE1 para los protocolos OSPF, BGP Y MPLS cuando se realiza el apagado del puerto GI2/0? Explique cada uno

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

Diseño Metodológico

Tipo de Investigación

Esta investigación tiene un alcance aplicado en el campo educativo, en las clases de Redes de Computadoras II y Redes Telefonicas II de la carrera de Ingenieria de Telecomunicaciones. Este tipo de investigación permite que se desarolle la parte experimental de conocimientos teóricos adquiridos. Donde se procedio a realizar 4 guias de laboratorio en la que se evidencia el funcionamiento de las tecnologías WAN, Protocolos OSPF, BGP y MPLS. Asi como las ventajas que se obtienen mediante la integración de estos para las redes MPLS-VPN.

- Enfoque aplicado: Debido a que buscamos aplicar resultados a una determinada situación. En este caso aplicaremos 4 guias de laboratorio en el emulador GNS3, que vengan a complementar la componente teorica con la practica.

Este esta investigación constará de 6 etapas:

Investigación Académica

Se consultó con docentes encargados de impartir las clases de redes de computadoras I y II, sobre el material y temas impartidos hacia los estudiantes en estas materias y la manera de ampliar el conocimiento práctico y teórico en las tecnologías de redes WAN.

Documentación

Se recopilo información precisa y confiable acerca de la tecnología MPLS, como funciona, de qué manera es implementada y con qué protocolos de enrutamiento se

relaciona. Esto con el objetivo de brindar una base teórica sólida para la mejor comprensión de las prácticas de laboratorios.

Selección de temas para guías de laboratorio

En esta sección se realizó la selección de temas, luego se elaboró 4 las guías de laboratorios, sobre estos mismos. La selección se basó en los resultados obtenidos en la etapa de investigación académica.

Selección de topologías de redes

Se escogió topologías de redes adecuadas, que permitieron demostrar el funcionamiento de MPLS y protocolos de enrutamiento relacionados con esta tecnología.

Elaboración de Guías de Laboratorio

Las 4 guías se crearon según los resultados de las etapas de topología y selección de temas. Las guías tienen el objetivo de evaluar el conocimiento adquirido por los estudiantes según la teoría dada con anterioridad.

Análisis de Resultados

Los docentes cuentan con las guías resueltas y con estas podrán evaluar los resultados de los estudiantes. Así como saber lo que se obtendrá de cada práctica que contengan las guías.

Conclusión

Mediante el estudio y análisis de las cuatro guías de laboratorio se logra mejorar y aportar en el proceso de enseñanza-aprendizaje en el área de redes con ayuda de la herramienta computacional GNS3 usando el IOS del router cisco 7200.

Se logra evidenciar el uso de la herramienta GNS3 para la enseñanza de MPLS en prácticas profesionales simuladas en un ambiente académico. Se desarrollaron topologías que permiten al estudiante entender cómo funciona cada tecnología WAN involucrada con MPLS por separado y cómo funcionan en convergencia.

Recomendaciones

- Validar que las cuatros guías propuestas en el documento monográfico sirvan de apoyo a los estudiantes en el proceso de aprendizaje y comprensión en las prácticas en una ambiente virtual en los laboratorios de la UNI.

- Recomendamos realizar las 4 guías antes mencionadas, con direccionamiento IPV6 ya que es la solución al agotamiento de direcciones IPV4. Y la nueva tendencia a nivel global.

Bibliografía

[1] McQuerry, S. (2008). Interconnecting Cisco Network Devices, Part 1 (ICND1). Indianapolis, USA: Cisco Press. ISBN: 978-1-58705-462-4

[2] Empson, S. (2008). CCNA Portable Command Guide. ndianapolis, USA: Cisco Press. ISBN: 978-1-58720-193-6

[3] Duponchelle, D. B. (20 de Febrero de 2017). https://docs.gns3.com.

Recuperado de https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html

[4] GNS3. (s.f.). Obtenido de https://www.gns3.com/software/faq

[5] Sevilla, E. A. (2010). Redes Cisco. CCNP a Fondo. Guia de estudio para Profesionales. D.F., Mexico: Alfaomega Grupo Editor, S.A. de C.V. ISBN: 978-6077854-79-1

[6] Ghein, L. D. (2007). MPLS Fundamentals. Indianapolis, Indiana, USA: Cisco Press, ISBN: 1-58705-197-4

[7] Headquarters, A. (2013). MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T. San Jose: CISCO PRESS. www.cisco.com

[8] Headquarters, Virtual Route Forwarding Design Guide for VRF-Aware Cisco Unified Communications Manager Express, 2008. www.cisco.com

Anexos

Entrevista: Tecnologias WAN en la UNI

Enseñanza sobre tecnologías WAN en la Universidad Nacional de Ingeniería (UNI) en la Carrera de Ingeniería en Telecomunicaciones.

Realizada a: MSC. Carlos Ortega
Realizada por: Br. Juan Fuentes y Br. Rene Guido
Fecha: 20/07/2018

1. **¿Considera usted que se están implementando las tecnologías WAN apropiadamente en el entorno académico?**

La Universidad implementa a medias algunas de las tecnologías de conexión WAN por lo que el programa se ve limitado solo a PPP, Frame Relay y ATM sin tomar en cuenta por ejemplo MPLS. Esto es necesario para lograr un entendimiento general de lo que actualmente se encuentra en el campo laboral en el mundo de las redes WAN.

2. **¿Qué importancia, considera usted, tiene el conocimiento de las tecnologías WAN para el ámbito profesional?**

Es necesario este tipo de conocimientos desde las tecnologías más básicas de conexión hasta las más nuevas teniendo en cuenta que algunos proveedores de servicios de internet poseen clientes que aún conservan enlaces como Frame Relay y que posiblemente esos mismos clientes hagan la migración a una tecnología más nueva.

3. **¿Considera necesario la enseñanza de protocolos de enrutamientos dinámicos para el desarrollo de futuros profesionales orientados a área de redes? ¿por qué?**

Es necesaria la enseñanza de este tipo de protocolos porque algunos de ellos como OSPF y BGP pueden trabajar de manera más organizada, incluir parámetros en dependencia del tipo de red y son altamente escalables.

4. **Actualmente, ¿qué protocolos de enrutamiento dinámico son impartidos para la clase de Redes de Computadoras II?**

Dentro de la categoría de protocolos dinámicos en la asignatura se imparten RIPv2 y OSPF de una sola área como protocolos IGP y BGP a nivel básico en la interconexión de redes grandes como protocolo EGP teniendo en cuenta el acompañamiento de un protocolo OSPF como IGP. Se hace mención que OSPF puede trabajar con múltiples áreas y podría funcionar como protocolo EGP.

5. **¿Qué emuladores son utilizados para realizar prácticas de laboratorio?**

A nivel básico se utiliza Packet Tracer y profundizando un poco más por su potencial se usa el GNS3. Este último su nivel de complejidad de topologías varia en dependencia de las características de las computadoras.

6. **¿Se desarrollan de manera teórica y práctica los protocolos de enrutamiento dinámico OSPF y BGP?**

De manera teórica se trabaja ambos protocolos OSPF de una sola área y múltiples áreas, así mismo BGP. En la práctica se hacen topologías separadas de OSPF y BGP, teniendo en cuenta el tiempo y las condiciones (características de las computadoras) se complementa con una topología más compleja involucrando características más avanzadas o incluso combinación de ambos protocolos.

7. **¿Considera que la tecnología MPLS se aborda a fondo en las carreras universitarias?**

No se aborda a fondo, ni en el programa de la asignatura ni en los contenidos impartidos.

8. **¿Qué beneficios tendría para el estudiante la enseñanza de MPLS en su formación profesional?**

Conocimiento palpable de una tecnología presente en el campo laboral y que está teniendo grandes beneficios en su implementación.

9. **¿Considera de interés implementar guías de laboratorio sobre esta tecnología para que los estudiantes puedan analizar y resolver problemas de red? ¿Por qué?**

Es necesario complementar toda la teoría con algo práctico, aunque sea en modo de emulación, así mismo que la guía tenga la característica de detectar y resolver fallas en la implementación (troubleshooting)

10. **¿De qué manera, considera usted, se puede resolver la creciente demanda de personal técnico capacitado en esta área de parte de proveedores de servicio (ISP)?**

La demanda de personal altamente capacitado siempre existirá por lo que la universidad como tal tiene que generar ingenieros capaces de poder resolver problemas en el menor tiempo teniendo los conocimientos y herramientas que le ayuden en su proceso. Dichos conocimientos e incluso experiencia se forjarán mejor en el ámbito laboral.

Universidad Nacional de Ingeniería
Facultad de Electrotécnica y Computación

Plan de clases redes de computadoras II

PROCESO DE MEJORAMIENTO Y ACTUALIZACIÓN CURRICULAR 2015

NOMBRE DE LA ASIGNATURA: Redes de Computadoras II

MEJORA Y ACTUALIZACIÓN:

Ing. Juan Miguel Mairena
Docente

REVISADO POR:

Ing. Marlon Robleto Alemán
Jefe de Departamento

APROBADO POR:

Ing. Ronald Torres Torres
Decano de la Facultad

VISTO BUENO:

Msc. Ing. Freddy Marín Serrano
Vice-Rectoría Académica

OFICIALIZACIÓN:

Ing. Diego Muñoz Latino
Secretaría General

Managua, Nicaragua

30/Noviembre/15

I. INFORMACIÓN GENERAL

1.1 Carrera	Ingeniería en Telecomunicaciones
1.2 Año y código del Diseño Curricular	2016 – DICUTELE16
1.3 Disciplina	Redes
1.4 Nombre de la Asignatura	Redes de Computadoras II
1.5 Fecha última actualización aprobada por Consejo Universitario	FEBRERO 2016
1.6 Nombre de docentes autores previo al PMAC	Ing. Verónica Norori
1.7 Código de la Asignatura	T042
1.8 Tipo de Asignatura[1]	Ejercicio profesional
1.9 Semestre académico en que se impartirá	VII
1.10 Frecuencia semanal	3
1.11 Total de horas	102
1.12 Créditos	5
1.13 Asignatura (as) pre-requisitos	No tiene
1.14 Asignatura (as) precedentes	Redes de Computadoras I
1.15 Asignatura (as) correquisitos	No tiene
1.16 Turno (diurno, nocturno)	Diurno y Nocturno
1.17 Modalidad (regular y especial)	Regular

[1] Clasificación de Asignaturas: Formación General, Básica, Básica Específica, Ejercicio Profesional, Optativas. Metodología y Normativa Curricular para la Transformación Curricular. Aprobada por el Consejo Universitario de la UNI, en Sesión 8-95, del 20 de Julio de 1995. Managua.

II. INTRODUCCIÓN

Esta asignatura continúa desarrollando el mundo de las redes que se inició con la asignatura de Redes de Computadoras I, contempla el estudio de temas que no se abordaron en la clase de prerrequisito.

La primera unidad fortalecerá los conocimientos de Enrutamiento introduciendo al estudiante en los protocolos EGP muy especialmente en el protocolo BGP e IBGP los cuales son utilizados para enrutar los paquetes en redes troncales las cuales comunican decenas o cientos de redes que se agrupan en sistemas autónomos.

En la segunda unidad se trata el tema de la conmutación en las redes de datos un conocimiento esencial para saber cómo funcionan las redes y los métodos de control de congestión, cómo se segmentan en redes virtuales auxiliándose de un método de capa 2 del modelo OSI.

La unidad de servicios de redes de área amplia introduce a los estudiantes en los protocolos de capa 2 del modelo OSI como es el PPP, HDLC y Frame relay y algunos servicios de direccionamiento IP como DHCP y NAT, servicios primordiales para la comunicación.

Las dos últimas unidades son introductorias a los temas de seguridad que debido a su complejidad es necesario abordarla en otra asignatura o como un curso extracurricular, se pretende que el estudiante tenga las bases para implementar redes segura y redes privadas virtuales.

De esta manera la asignatura de Redes de Computadoras II, aporta de forma significativa al desarrollo de los siguientes conocimientos, habilidades y actitudes del perfil de egreso de la carrera de Ingeniería en Telecomunicaciones:

Conocimientos	
Estudio de los Protocolos de pasarela exterior y su funcionamiento para redes troncales o principales.	▲
Estudio de la redes conmutadas y su utilización para el manejo de congestión.	▲
Estudio de los protocolos de Capa 2 como PPP,HDLC y Frame Relay	▲
Introducción a la seguridad de redes de datos.	
Habilidades	
Aplica los métodos y técnicas para implementar protocolos de pasarela Exterior.	▲
Implementa redes conmutadas de forma eficiente teniendo en cuenta las normas y procedimientos establecidos por parámetros de referencia internacional.	▲
Diseño de redes de área extensa según complejidad y necesidad.	▲
Trabaja en equipo de forma colaborativa.	▲

Implementa redes seguras con herramientas y procedimientos adecuados.	
Comunicarse efectivamente de forma oral, escrita, y gráfica para presentar proyectos de redes de datos.	▲
Usar técnicas, destrezas, y modernas herramientas para la práctica de la ingeniería.	▲
Actitudes	
Responsabilidad ética y profesional.	▲
Compromiso con el aprendizaje para toda la vida.	▲
Preocupación acerca del impacto de las soluciones de ingeniería en un contexto global, económico, ambiental, y social.	▲
Responsabilidad en la importancia de la toma de decisiones.	▲
Alto espíritu emprendedor.	▲
Actitud innovadora.	▲
Actuación responsable respecto al ambiente y su conciencia social sensible a la problemática de la sociedad nicaragüense.	▲

Para una adecuada asimilación de esta asignatura los estudiantes deberán haber aprobado Redes de Computadoras I donde se presentan la base para poder desarrollar los temas de esta asignatura.

Deberá de tener bien afianzado los conocimientos en los protocolos de pasarela Interior como RIP, EIGRP, OSPF para poder entender los de pasarela exterior que en esta materia se imparten y que son BGP e IBGP.

Debe dominarse direccionamiento IP tanto IPv4 como IPv6 en su totalidad desde subredes a VLSM, los conocimientos del modelo OSI y cómo trabajan las capas es importante para entender los servicios WAN como son PPP, HDLC y Frame Relay.

El programa de Redes de Computadoras II puede incluir todos los componentes formativos algunos en más profundidad que otros pero si cada componente formativo puede estar incluido en cada unidad o bien en general en toda la materia.

Investigación

La materia de redes intrínsecamente necesita de la investigación para poder desarrollar algunos tópicos que en clase se verán hasta cierto nivel de conocimiento, el estudiante puede comenzar a aplicar un método científico a medida que se apropia de los temas como los protocolos de comunicación y servicios de redes WAN y métodos de seguridad. La

asignatura no tiene integrado en su contenido ningún método científico en particular, por lo que el estudiante deberá ser guiado para este fin.

Extensión
El desarrollo de la clase tiene que estar vinculado con la realidad del país por lo que es necesario desarrollar en cada unidad casos prácticos, una gira de campo a una infraestructura de red es importante para tener una visión práctica de este objeto de estudio.

Responsabilidad Ambiental
En el diseño de las redes es necesario considerar el impacto ambiental que puede tener en el medio ambiente que está próximo a la infraestructura de las redes a implementarse, por eso es necesario incluir en el diseño la mitigación de este impacto.

Espíritu Emprendedor
La materia de redes brinda las herramientas, técnicas y conocimiento para poder ser un profesional que se desarrolle en el área de la consultoría o bien para formar iniciativas que logren desarrollarlo en el mundo laboral.

Tecnologías de la Información y las Comunicación (TIC)
En el desarrollo de la asignatura Redes de Computadoras I se hace uso de varios elementos de las Tecnologías de la Información y la Comunicación. En la tabla a continuación se muestran los principales elementos.

CONFERENCIAS	SOFTWARE	DOCUMENTOS	OTROS
PowerPoint	Packet Tracer	Dropbox	Youtube
Videos	GNS3,Teraterm,IP calculator	Email	Google Drive
Imágenes	Putty, clientes SSH	INTERNET	
	Visio 2013	Bosón Simulator	

III. OBJETIVOS GENERALES

- Analizar los protocolos de pasarela exterior y los métodos de conmutación para el diseño adecuado de redes de datos.

- Aplicar los métodos y técnicas adecuadas para comunicar redes de área amplia con los servicios adecuados y de forma segura.

IV. PLAN TEMÁTICO

N°	UNIDADES TEMÁTICAS	FORMAS DE ORGANIZACIÓN DE LA ENSEÑANZA (F.O.E.) [2]								Total de horas
		TEORÍA	PRÁCTICA							
		C	S	C.P	LAB	G.C	T	T.C	P.C	

[2] C (Conferencia), S (Seminario), CP (Clase Práctica), Lab (Laboratorio), GC (Gira de campo), T (Taller), TC (trabajo de curso), PC (Proyecto de Curso).

I	Enrutamiento con Protocolos de Pasarela Exterior (BGP)	10		8	8					**26**
II	Conmutación En redes de Datos	10		8	8					**26**
III	Servicios WAN	10		2	4					**16**
IV	Seguridad Perimetral de Redes	8		4	2					**14**
V	Redes Privadas Virtuales.	10		2	2					**14**
Total de horas presenciales		**48**		**24**	**24**					**96**
2da evaluación parcial, 1ra y 2daconvocatoria										**6**
TOTAL										**102**

V. UNIDADES TEMÁTICAS: NOMBRE DE LA UNIDAD, OBJETIVOS PARTICULARES, CONTENIDOS Y RECOMENDACIONES METODOLÓGICAS

UNIDAD I: ENRUTAMIENTO CON PROTOCOLOS DE PASARELA EXTERIOR (BGP)

OBJETIVOS PARTICULARES

- Comprender como los protocolos de enrutamiento de Pasarela exterior garantizan la comunicación en redes de gran escala.
- Diseñar Redes de gran escala con herramientas y procedimientos establecidos para protocolos de enrutamiento de pasarela exterior.
- Colaborar en tareas asignadas para realizar trabajos de diseño en grupos de trabajo.

CONTENIDOS

1.1 Introducción a Protocolos de Pasarela Exterior.
- 1.1.1 El Internet y Enrutamiento BGPT
- 1.1.2 Topologías de Internet
- 1.1.3 Redes con más de una interconexión WAN (Multihoming)

1.1.1 Direccionamiento IP y el protocolo BGP
- 1.1.1.1 Enrutamiento Interdominios.
- 1.1.1.2 El Protocolo BGP
- 1.1.1.3

1.1.2 Consideraciones de diseño WAN

1.1.3 Disponibilidad y Confiabilidad de la Conexión WAN.
- 1.1.3.1 Como Seleccionar el Proveedor de Servicios (ISP)
- 1.1.3.2 Cálculos de Ancho de Banda.
- 1.1.3.3 Características del Hardware para Interconexión WAN
- 1.1.3.4 Riesgos y supuestos del Diseño.

1.1.4 Espacio de direcciones IP y Los números e Sistema Autónomo (AS)

1.1.4.1 Los diferentes tipos espacios de direcciones.
1.1.4.2 Solicitud de espacio de Direcciones
1.1.4.3 Los números de Sistema autónomo
1.1.4.4 Registros de Enrutamiento y Políticas.

1.2 Funcionamiento del Protocolo BGP
1.2.1 Habilitando Y Monitoreo de BGP
1.2.2 Filtrando Rutas
1.2.3 BGP Interno
1.2.4 Redes Internas
1.2.5 eBGP Multisaltos (Multihop)

1.3 Ingeniería de Tráfico
1.3.1 Parámetros para escoger la mejor ruta.
1.3.2 Preferencia Local
1.3.3 Administrando las rutas de AS entrantes
1.3.4 Comunidades de entrada
1.3.5 Balanceando cargas en BGP
1.3.6 Parámetros de Discriminación de múltiples salidas MED
1.3.7 Anunciar Rutas más especificas

1.4 BGP para grandes Redes
1.4.1 Buena Practicas de BGP
1.4.2 Usando Interfaces de LOOPBACK
1.4.3 Escalando iBGP
1.4.4 OSPF o ISIS como IGP

1.5 Servicio de Transito con BGP

1.6 Filtro de rutas en el Transito
1.6.1 Comunidades en Transito BGP
1.6.2 Clientes con Conexiones de Respaldo
1.6.3 Proveer Clientes IPV6

RECOMENDACIONES METODOLÓGICAS

Para Desarrollar esta Unidad se debe utilizar presentaciones en PowerPoint auxiliándose de Packettracer, GNS3 incluso de Boson Simulator para reforzar los conocimientos.

En los laboratorios se recomienda montar un servidor con Dynamips o GNS3 y establecer escenarios prácticos para implementar el protocolo BGP en redes de gran escala.

Se debe de hacer énfasis en cómo una organización puede solicitar sus IPv4, IPv6, un sistema autónomo al registrador de la región llamado RIR por sus siglas de Registro Regional de Internet.

Al final de la unidad el estudiante deberá presentar en trabajos colaborativos una red de gran escala diseñada y configurada con el protocolo BGP un plan de direccionamiento para solicitar un bloque de direcciones y un sistema autónomo.

UNIDAD II: CONMUTACIÓN EN REDES DE DATOS

OBJETIVOS PARTICULARES

- Comprender el funcionamiento y uso de la conmutación para mejorar el rendimiento de las redes de datos.
- Diseñar redes conmutadas con las herramientas y procedimientos que permitan un rendimiento óptimo.
- Valorar el impacto que tienen una adecuada conmutación en las redes corporativas y educativas.

CONTENIDOS

2.1 Introducción A Redes Conmutadas

2.2 Introducción a Redes Convergentes
- 2.2.1 Complejidad creciente de las redes
- 2.2.2 Elementos de una red convergente
- 2.2.3 Redes conmutadas sin fronteras
- 2.2.4 Jerarquía en las redes conmutadas sin fronteras
- 2.2.5 Núcleo, distribución y acceso

2.3 Redes conmutadas
- 2.3.1 Función de las redes conmutadas
- 2.3.2 Factores de forma

2.4 El entorno conmutado
- 2.4.1 Reenvío de tramas
  - 2.4.1.1 Completado dinámico de la tabla de direcciones MAC de un conmutador
  - 2.4.1.2 Métodos de reenvío del conmutador
  - 2.4.1.3 Conmutación por almacenamiento y envío
  - 2.4.1.4 Conmutación por método de corte
- 2.4.2 Dominios de Conmutación
  - 2.4.2.1 Dominios de colisiones
  - 2.4.2.2 Dominios de broadcast
  - 2.4.2.3 Alivio de la congestión en la red

2.5 EL conmutador como elemento Básico de una Red

2.6 Configuración básica del switch
- 2.6.1.1 Preparación para la administración básica de un switch
- 2.6.1.2 Configuración de acceso a la administración Básica de un switch con IPv4
- 2.6.1.3 Configuración de puertos de un switch
- 2.6.1.4 Comunicación dúplex
- 2.6.2 Configuración de puertos de switch en la capa física
- 2.6.3 Auto-MDIX
- 2.6.4 Verificación de la configuración de puertos de un switch
- 2.6.5 Problemas de la capa de acceso a la red

2.7 Seguridad de Conmutadores
- 2.7.1 Acceso remoto seguro
- 2.7.2 Funcionamiento de SSH
- 2.7.3 Seguridad de puertos de switch
- 2.7.4 Snooping de DHCP
- 2.7.5 Protocolo de hora de red (NTP)

2.8 Red de Área local Virtual (VLAN)

2.9 Descripción general de las (VLAN)
- 2.9.1 Definiciones de VLAN
- 2.9.2 Beneficios de las redes VLAN
- 2.9.3 Tipos de VLAN
- 2.9.4 VLAN de voz

2.10 VLAN en un entorno conmutado múltiple
- 2.10.1 Enlaces troncales de la VLAN
- 2.10.2 Control de los dominios de broadcast con las VLAN
- 2.10.3 Etiquetado de tramas de Ethernet para la identificación de VLAN
- 2.10.4 VLAN nativas y etiquetado de 802.1Q

2.11 Implementaciones de VLAN
- 2.11.1 Asignación de red VLAN
  - 2.11.1.1 Rangos de VLAN
  - 2.11.1.2 Creación de una VLAN
  - 2.11.1.3 Asignación de puertos a las redes VLAN

2.11.2 Enlaces troncales de la VLAN
- 2.11.2.1 Configuración de enlaces troncales IEEE 802.1Q
- 2.11.2.2
- 2.11.3 Protocolo de enlace troncal dinámico
- 2.11.3.1 Introducción a DTP
- 2.11.3.2 Modos de interfaz negociados

2.12 Enrutamiento entre VLAN
- 2.12.1 Funcionamiento del routing entre VLAN

2.12.2¿Qué es el enrutamiento entre VLAN?
2.12.3Routing entre VLAN antiguo
2.12.4Routing entre VLAN con router-on-a-stick
2.12.5Routing entre VLAN con switch multicapa

2.13 Conmutación de capa 3
2.13.1 Funcionamiento y configuración del switching de capa 3
2.13.2 Introducción al switching de capa 3
2.13.3 Routing entre VLAN con interfaces virtuales de switch
2.13.4 Routing entre VLAN con puertos enrutados

RECOMENDACIONES METODOLÓGICAS

Para una mejor asimilación de esta unidad es importante combinar las conferencias con ejemplos prácticos el uso combinado de PowerPoint y un simulador como PacketTracer y GNS3, en algunos casos se recomienda que el profesor realice configuraciones en el simulador previo a los laboratorios para dar ver el entorno de trabajo práctico.

Es importante dejar claro cómo funciona la conmutación en la Capa 2 de Modelo OSI y los métodos utilizaos para optimizarlas así como los dominios de Broadcast, Colisión y como controlar la congestión en la capa de enlace de datos.

Las prácticas deberán hacerse en switches de capa 2 administrables según recursos al alcance se recomienda si hay algún laboratorio de la academia CISCO de la UNI gestionar para realizar las prácticas de lo contrario realizarlo en modo simulación o emulación.

Los temas 3 son una herramienta básica para el área de conmutación y debe enfatizarse en cómo las redes virtuales de área local logran controlar la congestión y como agregar un método de seguridad al usuario final al poder segmentar con ayuda de la capa 3 las redes conmutadas.

El último tema es para introducir al estudiante y complemente los conocimientos de capa 2 con equipos de capa tres como son los switches que enrutan VLAN.

UNIDAD III: SERVICIOS WAN
OBJETIVOS PARTICULARES

- Comprender los servicios de red de área amplia (WAN) y su funcionamiento para las comunicaciones a nivel Mundial.

- Diseñar redes de área amplia (WAN) con técnicas, métodos y herramientas para una mejor comunicación.

- Colaborar en trabajos de grupos para el diseño de Redes WAN.

CONTENIDOS

3.1 Introducción a las redes WAN
3.1.1 Introducción de redes de área extensa (WAN)
3.1.2 El modelo de red en evolución

3.1.3 Conceptos de tecnología WAN
3.1.4 Descripción general de la tecnología WAN
3.1.5 Conceptos de capa física de la WAN
3.1.6 Conceptos de la capa de enlace de datos de la WAN
3.1.7 Conceptos de conmutación WAN
3.1.8 Opciones de conexión WAN
3.1.9 Opciones de conexión de enlace dedicado
3.1.10 Opciones de conexión por conmutación de circuitos
3.1.11 Opciones de conexión por conmutación de paquetes
3.1.12 Opciones de conexión por Internet

3.2 Protocolo Punto a Punto (PPP)
- 3.2.1 Enlaces seriales punto a punto
- 3.2.2 Introducción a las comunicaciones seriales
- 3.2.3 Multiplicación por división temporal (TDM)
- 3.2.4 Punto de demarcación
- 3.2.5 Equipo Terminal de Datos (DTE) y Equipo de Comunicación de Datos (DCE)
- 3.2.6 Encapsulación control de enlace de Datos de alto Nivel (HDLC)

3.3 Conceptos del PPP
- 3.3.1 Introducción al PPP
- 3.3.2 Arquitectura de capas PPP
- 3.3.3 Estructura de trama PPP
- 3.3.4 Establecimiento de una sesión PPP
- 3.3.5 Establecimiento de un enlace con el LCP
- 3.3.6 Explicación de NCP

3.4 Configuración de PPP con autenticación
- 3.4.1 Protocolos de autenticación
- 3.4.2 Protocolo de autenticación de contraseña (PAP)
- 3.4.3 Protocolo de autenticación de intercambio de señales (CHAP)
- 3.4.4 Encapsulación y proceso de autenticación del PPP

3.5 Protocolo Frame Relay
- 3.5.1 Conceptos básicos de Frame Relay
- 3.5.2 Introducción a la tecnología Frame Relay
- 3.5.3 Circuitos virtuales
- 3.5.4 Encapsulación Frame Relay
- 3.5.5 Topologías de Frame Relay
- 3.5.6 Asignación de direcciones Frame Relay
- 3.5.7 Conceptos avanzados de Frame Relay
- 3.5.8 Control de flujo de Frame Relay
- 3.5.9 Configuración avanzada de Frame Relay

3.6 Servicios de direccionamiento IP
3.7 DHCP
- 3.7.1 Introducción a DHCP
- 3.7.2 Funcionamiento de DHCP
- 3.7.3 BOOTP y DHCP
- 3.7.4 Configuración de un servidor de DHCP
- 3.7.5 Configuración del cliente DHCP

3.7.6 Relay DHCP
3.8 Escalamiento de redes con NAT
3.8.1 Direccionamiento IP público y privado
3.8.2 Ventajas y desventajas del uso de NAT
3.8.3 Configuración de NAT estática
3.8.4 Configuración de NAT dinámica 206
3.8.5 Configuración de la sobrecarga de NAT
3.8.6 Configuración de reenvío de puertos
3.8.7 Verificación y resolución de problemas de configuraciones NAT
3.8.8
3.9 Problemas frecuentes en la implementación de WAN
3.9.1 Comunicaciones en las WAN
3.9.2 Pasos en el diseño de las WAN
3.9.3 Consideraciones sobre el tráfico de WAN
3.9.4 Consideraciones sobre la topología de WAN
3.9.5 Consideraciones sobre el ancho de banda de WAN
3.9.6 Problemas frecuentes en la implementación de WAN
3.9.7 Estudio de caso: resolución de problemas.

RECOMENDACIONES METODOLÓGICAS

En esta unidad es necesario realizar conferencias auxiliadas de PowerPoint para exponer los conceptos básicos de las redes de área amplia y los tipos de conexión más usada, se recomienda exponer ejemplos prácticos de conexión de las instituciones educativas e instituciones privadas es importante que el estudiante quede claro como escoger la conexión WAN adecuada a cada necesidad.

En el tema 2 es importante auxiliarse de PowerPoint pero agregando simuladores como PacketTracer o Boson Simulator para entender cómo funciona este protocolo Punto a Punto de igual forma para el tema 3 es necesario el uso de estas herramientas para desarrollar la clase tanto en las conferencias, clases prácticas y laboratorios.

Es importante realizar trabajos colaborativos para implementar los servicios de direccionamiento IP los cuales podrán dejarse tareas en grupos a defender utilizando simuladores o emuladores como Packetracer y GNS3 respectivamente.

Al final de esta unidad deberán diseñar o analizar redes WAN para una implementación que cubra una necesidad, para ello el docente dará estudios de casos para que los estudiantes los resuelvan.

UNIDAD IV: SEGURIDAD PERIMETRAL DE REDES
OBJETIVOS PARTICULARES
Implementación de la Tecnología MPLS en el Emulador
GNS3 con Propósitos Académicos

- Analizar las diferentes amenazas, vulnerabilidades y sus implicaciones en las redes de datos.

- Implementar buenas prácticas y métodos para lograr redes seguras mitigando el impacto de los ataques.

- Colaborar en trabajos asignados por el docente con los compañeros del grupo.

CONTENIDOS

4.1 Amenazas de seguridad a Redes Actuales
- 4.1.1 Principios Fundamentales de una red segura
- 4.1.2 Los virus, gusanos y caballos de Troya
- 4.1.3 Metodologías de ataque
- 4.1.4 Aplicación de los principios de seguridad fundamentales para el diseño de redes.

4.2 Implementando Tecnología de Firewall
4.1 Tecnologías de Firewall
4.2 Políticas de firewall basadas en zonas

4.3 Listas de Acceso como Método de Seguridad

4.4 Cómo utilizar las ACL para la protección de redes
- 4.2.1 Una conversación TCP
- 4.2.2 Filtrado de paquetes
- 4.2.3 Funcionamiento de las ACL
- 4.2.4 Tipos de ACL de Cisco
- 4.2.5 Funcionamiento de una ACL estándar
- 4.2.6 Numeración y denominación de las ACL
- 4.2.7 Ubicación Dónde ubicar las ACL
- 4.2.8 Pautas generales para la creación de las ACL
- 4.2.9 Configuración de las ACL estándar 146
- 4.2.10 Máscara wildcard de las ACL 147
- 4.2.11 Monitoreo y verificación de ACL 153

4.5 Listas de Acceso extendidas
4.6 Listas de Acceso complejas
4.7 Listas de Acceso dinámicas
4.8 Listas de Acceso reflexivas
4.9 Listas de Acceso basadas en el tiempo

RECOMENDACIONES METODOLÓGICAS

Esta unidad es introductoria a la seguridad de las redes ya que es un área muy compleja que requiere incluso una carga horaria de dos asignaturas para cubrir la temática completa.

Se deberá enfatizar en las diferentes amenazas y vulnerabilidades que presentan las redes de datos en el tema 1 se recomienda auxiliarse de PowerPoint, videos y estudios de casos prácticos para entender mejor cómo impacta esto e las redes.

En laboratorio es importante hacer prácticas de Firewall específicamente en el área de la infraestructura como los routers o algún dispositivo directamente diseñado para este fin como un ASA de cisco, asegurar los switches y los routers con buenas prácticas, se recomienda utilizar equipos, de no contar con estos recursos se pude usar simuladores o emuladores como packetracer y GNS3.

UNIDAD V: REDES PRIVADAS VIRTUALES
OBJETIVOS PARTICULARES

- Comprender como las redes privadas virtuales facilitan las comunicaciones de forma segura y confiable.
- Implementar redes seguras a través de redes privadas virtuales, garantizando la privacidad de la información.
- Colaborar con sus compañeros de clase en los trabajos asignados por el docente.

CONTENIDOS

5.1 Requisitos para los servicios de redes Privadas Virtuales.
- 5.1.1 Los requisitos los servicios de trabajo a distancia
- 5.1.2 La solución del trabajador a distancia

5.2 Servicios de banda ancha
- 5.2.1 Conexión a la WAN para VPN
- 5.2.2 Conexión por Cable
- 5.2.3 Conexión por DSL
- 5.2.4 Conexión inalámbrica de banda ancha

5.3 Tecnología de Redes Privadas Virtuales VPN
5.4 Las redes VPN y sus beneficios
5.5 Tipos de VPN
5.6 Componentes de la VPN
5.7 Características de las VPN seguras
5.8 Tunneling de VPN
5.9 Integridad de datos de la VPN
5.10 Protocolos de seguridad IPsec

5.11 Implementación de Redes Privadas Virtuales
- 5.11.1 Red VPN de Sitio a Sitio
- 5.11.2 Red VPN de Acceso Remoto
- 5.11.3 Red VPN en dispositivos Móviles

RECOMENDACIONES METODOLÓGICAS

Esta unidad refuerza la unidad IV implementando mecanismos de comunicación segura.

En esta unidad se podrá auxiliar de PowerPoint, PacketTracer y GNS3. Las conferencias deberán enfatizar en las características de los enlaces y ancho de banda para implementar redes privadas virtuales y en el funcionamiento del protocolo IPsec como base para las redes privadas virtuales.

En la parte práctica se deberá hacer uso de una conexión inalámbrica para las conexiones sitio a sitio y las conexiones remotas con routers o ASA de no contar con estos recursos podrá usarse un simulador como Packetracer o un emulador como GNS3.

Al final de la clase el estudiante deberá implementar una red VPN con todas las herramientas y procedimientos aprendidos.

VI. EVALUACIÓN DEL APRENDIZAJE: [3]

EVALUACIONES ORDINARIAS [4]		
I Evaluación Parcial	Evaluaciones Sistemáticas[5]	15%
	Examen	35%
II Evaluación Parcial	Evaluaciones Sistemáticas	15%
	Examen	35%
Total		100%
EVALUACIONES EXTRAORDINARIAS		
Evaluación de I Convocatoria	Examen (70%) Evaluaciones Sistemáticas (30%)	100%
Evaluación de II Convocatoria	Examen	100 %
Evaluación por Suficiencia	Examen	100 %

[3] UNI (2006): Reglamento de Régimen Académico de la Universidad Nacional de Ingeniería. Aprobado por el Consejo Universitario el 27 de octubre del 2006. Managua.
[4] Adecuar de conformidad con la naturaleza de cada programa de asignatura (Arto. 24 del Reglamento de Régimen Académico). Ver guía metodològica
5 Preguntas de control, seminarios, clases prácticas, laboratorios, giras de campo, talleres, trabajos extra-clase, pruebas cortas. (Arto. 27 del Reglamento de Régimen Académico).

Evaluación Cursos de Verano[6]	Examen (4 pruebas de 25 puntos cada una)	100%

VII. BIBLIOGRAFÍA

7.1 Textos básicos

Ariganello Ariganello, Ernesto. (2013). Redes Cisco. Guía De Estudio Para La Certificación CCNA Security. RA-MA EDITORIAL.

Johnson, Alan. (2009).*LAN inalámbrica y conmutada.* Primera edición. Pearson-PHH, Cisco Press.

Van Beijnum Iljitsch. (2002). BGP. 1005 Gravenstein Highway North, Sebastopol, CA 95472. O'Reilly Media .

Varios Autores. (2011).*Acceso a la WAN*.México. Pearson Educación.

http://www.ugr.es/~recfpro/rev173COL9.pdf.

[6] Se establecen de conformidad con los criterios definidos en el plan de estudio y las disposiciones institucionales vigentes (Arto. 44 del Reglamento de Régimen Académico).

Universidad Nacional de Ingeniería
Facultad de Electrotécnica y Computación

Plan de clases redes de telefonicas II

PROCESO DE MEJORAMIENTO Y ACTUALIZACIÓN CURRICULAR 2015

NOMBRE DE LA ASIGNATURA: REDES TELEFONICAS II

CÓDIGO: T051

MEJORA Y ACTUALIZACIÓN:

Ing. David Montenegro Blandino
Docente

REVISADO POR:

Ing. Luis Francisco López Bravo
Coordinador de la carrera Ingeniería en Telecomunicaciones

APROBADO POR:

Ing. Ronald Torres Torres
Decano de la Facultad

VISTO BUENO:

Msc. Ing. Freddy Tomás Marín Serrano
Vice-Rectoría Académica

OFICIALIZACIÓN:

Msc. Ing. Diego Muñoz Latino
Secretaría General

Managua, Nicaragua

30/11 /2015

VIII. INFORMACIÓN GENERAL

1.9 Carrera	Ingeniería en Telecomunicaciones
1.10 Año y código del Diseño Curricular	2016 – DICUTELE16
1.11 Disciplina	Telecomunicaciones
1.12 Nombre de la Asignatura	Redes Telefónicas II
1.13 Fecha última actualización aprobada por Consejo Universitario	Febrero 2016
1.14 Nombre de docentes autores previo al PMAC	Ing. Marlon Robleto Alemán
1.15 Código de la Asignatura	T051
1.16 Tipo de Asignatura[7]	Ejercicio Profesional
1.18 Semestre académico en que se impartirá	X
1.19 Frecuencia semanal	3
1.20 Total de horas	102
1.21 Créditos	5
1.22 Asignatura (as) pre-requisitos	Redes Telefónica I
1.23 Asignatura (as) precedentes	No Tiene
1.24 Asignatura (as) correquisitos	No Tiene
1.25 Turno	Diurno
1.26 Modalidad	Regular

[7] Clasificación de Asignaturas: Formación General, Básica, Básica Específica, Ejercicio Profesional, Optativas. Metodología y Normativa Curricular para la Transformación Curricular. Aprobada por el Consejo Universitario de la UNI, en Sesión 8-95, del 20 de Julio de 1995. Managua.

IX. INTRODUCCIÓN

Uno de los medios de trasmisión más usados en el sector de las Telecomunicaciones son las Redes Telefónicas. La asignatura **Redes Telefónicas II** complementa el estudio de las recapitulaciones de las distintas tecnologías y servicios de las redes telefónicas o de telecomunicaciones existentes, actuales y emergentes.

Estos conocimientos son de mucha importancia para el estudiante ya que le serán de gran utilidad para su futuro desempeño profesional en áreas donde se requiera implantar, administrar, evaluar tecnología o servicios en redes telefónicas.

El enfoque de esta asignatura es basado en los sistemas de telecomunicaciones y servicios que se prestan a partir de la infraestructura de las redes Telefónicas, tales como telefonía básica, celular, VoIP, mensajería de texto, transmisión de datos etc.

En la siguiente tabla se describe la contribución de la asignatura **Redes Telefónicas II** a la formación de los siguientes conocimientos, habilidades y actitudes del perfil de egreso:

Conocimientos	
Domina los fundamentos, métodos, técnicas y procedimientos para el análisis, planeación y desarrollo de sistemas de telecomunicaciones para sus diferentes servicios, así como los aspectos legales y normativas de las telecomunicaciones.	▲
Principios, métodos, herramientas de las ciencias básicas, de las ciencias específicas de la ingeniería, así como de las telecomunicaciones en sus distintas áreas temáticas (telecomunicaciones por radio, telecomunicaciones por líneas, sistemas telemáticos y sistemas electrónicos de telecomunicaciones).	▲
Conoce y entiende las tecnologías en que están basadas las redes modernas de telecomunicaciones fijas y móviles.	▲
Comprende los principios económicos fundamentales, así como la formulación de proyectos relacionada con Ingeniería en Telecomunicaciones.	▲
Habilidades	
Utiliza adecuadamente los servicios de telecomunicaciones que se emplean de forma cada vez más intensiva, tales como el comercio y el gobierno electrónico, la telemedicina, la tele-educación e instituciones privadas en el área de producción y de servicio.	▲
Diseña y evalúa sistemas de telecomunicaciones, considerando los estándares normativas y leyes que regulan el sector de las telecomunicaciones.	▲
Diagnostica y diseña soluciones para los problemas en el campo de las telecomunicaciones.	▲

Diseña, administra y evalúa proyectos de telecomunicaciones.	▲
Investiga, innova y adapta tecnología para el desarrollo de las telecomunicaciones en correspondencia con las necesidades del país.	▲
Toma decisiones acerca de requerimientos y especificaciones para el diseño, instalación y mantenimiento de sistemas y equipos de telecomunicaciones.	▲
Se comunica de forma oral y escrita, aplicando las normas del lenguaje, así como las Tecnologías de la Información y Comunicación (TIC).	▲
Utiliza software especializado en su desarrollo profesional.	▲
Actitudes	
Es portador de valores morales y éticos.	▲
Presenta una actitud responsable y comprometida con el desarrollo de la sociedad y el medio ambiente.	▲
Enfrenta los nuevos desafíos que surgen con los avances de la tecnología.	▲
Demuestra conciencia responsable en la sociedad y el ambiente, valorando la importancia del cumplimiento de normativas, regulaciones y leyes del área de las telecomunicaciones.	▲
Muestra interés por el trabajo individual y en equipo, actuando en correspondencia con valores y principios asumidos en el modelo educativo institucional y el perfil de la carrera.	▲
Se apropia de las normas de seguridad e higiene concernientes al ámbito de las telecomunicaciones.	▲
Demuestra un espíritu emprendedor ante los problemas del ejercicio de la profesión y el cambio en el entorno personal y social.	▲
Asume compromisos con la superación personal, el aprendizaje permanente y el logro de las metas propuestas.	▲

Esta asignatura tiene como pre-requisito la asignatura de **Redes Telefónicas I,** ya que, por ende, esta ofrece los conocimientos necesarios que el estudiante necesita para llevar esta segunda materia de redes Telefónicas debido a que ambas asignaturas establecen una sinergia de conocimientos habilidades y destrezas que le serán de gran utilidad para el futuro desempeño profesional al egresado.

En la asignatura **Redes Telefónicas II** se encuentran presentes algunos de los componentes formativos establecidos por la institución, entre ellos están:

Investigación

En el desarrollo del programa de la asignatura se realizarán seminarios, laboratorios y Trabajo de Curso que estimularán al estudiante a la búsqueda de información sobre temas

específicos relacionados al área de la asignatura, para lo cual deberán hacer uso de técnicas y herramientas de investigación científica, esto le permitirá complementar y profundizar sobre los tópicos desarrollados en el aula de clase.

Tecnologías de la Información y las Comunicación (TIC)

En el desarrollo de la asignatura se hace uso de la comunicación con los estudiantes vía dropbox, e-mail. Se utiliza equipo informático de apoyo como portátil, datashow; también deberá de redactar reportes de laboratorios, el cual será impreso al igual que el del Trabajo de Curso. Estos reportes deberán de cumplir con la rigurosidad ética, estética y de contenido correspondiente al nivel de un estudiante de un quinto año de una carrera de Ingeniería.

Extensión

El Proyecto de Curso contribuye como estrategias didácticas que permitirá al estudiante la vinculación con la realidad práctica, contraponiéndola con la teoría vista en el salón de clases; así mismo suscita a resolver un problema específico de la sociedad, vinculando de esta manera sus conocimientos adquiridos con la realidad nacional.

X. OBJETIVOS GENERALES

- Conocer los fundamentos elementales de las redes telefónicas digitales, así como los servicios de nueva generación que se prestan sobre estas redes, permitiendo al estudiante aplicarlos adecuadamente es su formación como futuro Ingeniero en Telecomunicaciones.

- Aplicar los conocimientos, métodos y técnicas adquiridas en la ejecución del Trabajo de curso propuesto en esta materia; donde el estudiante demostrara su capacidad de dar respuesta a una problemática específica en el área de las telecomunicaciones.

- Hacer laboratorios con el uso de software de simulación y modelaje de diseño de redes telefónicas digitales, ejercitándose en el uso de los mimos, para aplicarlos adecuadamente en el diseño de los mismos en el ámbito laboral una vez que ya estén ejerciendo la profesión.

XI. PLAN TEMÁTICO

N°	UNIDADES TEMÁTICAS	FORMAS DE ORGANIZACIÓN DE LA ENSEÑANZA (F.O.E.) [8]								Total de horas
		TEORÍA	PRÁCTICA							
		C	S	C.P	LAB	G. C	T	T.C	P.C	
I	La ISDN	6						2		**8**
II	El sistema telefónico móvil	16	4	4	2			2		**28**
III	Estructura y servicios de redes de banda ancha	10	4		4			2		**20**
IV	Redes de Datos	12	4	4	2			2		**24**
V	Telefonía sobre IP	10	4					2		**16**
	Total de horas presenciales.	**54**	**16**	**8**	**8**			**10**		**96**
2da evaluación parcial, 1ra y 2da convocatoria										**6**
TOTAL										**102**

XII. UNIDADES TEMÁTICAS: NOMBRE DE LA UNIDAD, OBJETIVOS PARTICULARES, CONTENIDOS Y RECOMENDACIONES METODOLÓGICAS

UNIDAD I: LA RED DE SERVICIOS DIGITALES INTEGRADOS (ISDN)

OBJETIVOS PARTICULARES:

- Estudiar los aspectos introductorios de las redes de servicios digitales integrados (ISDN) comprendiendo sus principios y funcionamiento.

- Utilizar el conocimiento de la estructura de las ISDN, analizando si algunos de los operadores de servicios de Telecomunicaciones nacionales utilizan esta tecnología.

- Mostrar interés en las ISDN de banda ancha (B-ISDN), identificando su aplicación en las Redes Telefónicas modernas.

CONTENIDOS

1.1 Introducción a la Red de Servicio Digitales Integrados (ISDN).

1.2 Estructura de la ISDN, estructura de la trama (acceso básico y acceso primario).

[8] C (Conferencia), S (Seminario), CP (Clase Práctica), Lab (Laboratorio), GC (Gira de campo), T (Taller), TC (trabajo de curso), PC (Proyecto de Curso).

1.3 Señalización de usuario (capa 1,2 y 3); señalización entre centrales y servicios brindados en una ISDN.

1.4 B-ISDN (Red de banda ancha de Servicios Digitales Integrados)

RECOMENDACIONES METODOLÓGICAS

Para el desarrollo de esta primera unidad se hará uso tres sesiones de conferencias y una para el Trabajo de Curso. Es recomendado que el docente haga uso de medios audio-visuales tales como proyector, datashow, presentaciones de videos, etc. de manera que sea más comprensible el contenido de esta unidad (una imagen habla más que mil palabras).

En esta unidad se definirá el trabajo de curso (TC), se organizarán los equipos de trabajo (se recomiendan mínimo de tres, máximo cuatro integrantes). Se definirá la fecha de entrega y se les indicará a los estudiantes que este es la nota correspondiente a la tercera evaluación parcial. El docente deberá ir supervisando el avance del TC aclarando y/o ayudando en donde los estudiantes muestren debilidades para lograr así que todos los grupos logren el cumplimiento de los objetivos propuesto con este TC.

En el informe del TC deberá ir la captura de pantallas de todos los pasos realizados en la configuración de los parámetros usados en la simulación y/o modelado de la red Telefónica digital, junto con los resultados obtenidos (según la herramienta TIC utilizada).

Todos los pasos realizados, los parámetros de configuración introducidos a la herramienta TIC utilizada, así como los valores obtenidos, deberán ir debidamente explicados en informe en base a los fundamentados y principios estudiados en esta clase, más los elementos nuevos investigados por los alumnos para cumplir con los objetivos propuestos para este Trabajo.

UNIDAD II: EL SISTEMA TELENÓNICO MÓVIL

OBJETIVOS PARTICULARES:

- Distinguir los sistemas de Radio Comunicaciones Móviles, identificando ejemplos de estos sistemas utilizados por los operadores nacionales de Telecomunicaciones.

- Efectuar una taxonomía de los Sistemas telefónicos inalámbricos estableciendo una comparación en cuanto a capacidad de transmisor y servicios que se pueden.

- Enjuiciar sobre los diferentes sistemas de comunicaciones móviles por satélite comparando sus ventajas, desventajas y uso de cada uno de ellos.

CONTENIDOS

2.1 Introducción a los Sistemas de Radiocomunicaciones Móviles.
- 2.1.1 Sistema de radio telefonía móvil celular.
- 2.1.2 Sistemas móviles privados.
- 2.1.3 Radio búsqueda.
- 2.1.4 Comunicaciones móviles por satélites.

2.2 Sistemas de Radio Telefonía Móvil Celular
- 2.2.1 Antecedentes, clasificación de los sistemas, sistemas convencionales de radio móvil.
- 2.2.2 Sistema de telefonía celular básico: reuso de frecuencia, subdivisión celular, hand-off, roaming.
- 2.2.3 Aspectos a considerar en el diseño de un sistema de telefonía celular.

2.3 Técnicas de Acceso a Canal: TDMA y CDMA.

2.4 Generaciones Avanzada de Sistemas Telefónicos Inalámbricos.
- 2.4.1 Sistemas 2G, 3G y 3.5G (IMT-2000).
- 2.4.2 Sistema EDGE GSM.
- 2.4.3 Sistema GPRS GSM.

2.5 Sistemas de Comunicaciones Móviles por Satélite.
- 2.5.1 INMARSAT.
- 2.5.2 IRIDIUN.
- 2.5.3 GLOBALSTAR.

RECOMENDACIONES METODOLÓGICAS

Esta segunda unidad, se harán uso de ocho conferencias teóricas, dos de clase práctica, dos para seminario y una de laboratorios. El docente puede abordar el inciso 2,1 y 2.2.1 a un nivel más profundo en aspectos ingenieriles ya que son temas que se abordaron en la clase **Comunicaciones Inalámbrica**. Los incisos 2.2.2 y 2.2.3 se podrá reforzar con ejercicios de reuso de frecuencia, cálculos de diseño de una pequeña red celular (subdivisión celular, hand-off, roaming) mediante las dos sesiones de Clase Práctica y el laboratorio destinado para esta unidad. Para la sesión de laboratorio el docente deberá de suministrar la guía de laboratorio, se recomienda que la práctica sea sobre el modelaje de una pequeña red celular haciendo unos de la o las herramientas de diseño y/ o modelaje con que se cuenten en el laboratorio[9].

[9] ICS de Telecom tiene una versión trial que puede ser utilizado para tal propósito. En Internet se encuentran tutoriales de esta herramienta y en YouTube hay suficientes videos de ejemplo de uso de la misma

Los acápites 2.4 y 2.5 queda a discreción del docente si él los abordará o los deja como temas de investigación y explosión, haciendo uso tanto de las sesiones de clases teóricas como de los seminarios; esto en base a lo indicado en el párrafo anterior. El docente intervendrá en las explosiones o participaciones de los estudiantes en los seminarios cuando él considere necesario reforzar un tema que no fuese abortado en contenido, a fin que se garantice el cumplimiento de los objetivos de esta unidad. Estas explosiones y el seminario será parte de la nota sistemática a acumular por el estudiante.

Para la sesión del TC destinada en esta unidad, el docente ira monitoreando el avance de los estudiantes, verificando que los temas estudiados en esta unidad sean considerados por los estudiantes en dicho TC. Así mismo el docente irá dándole la orientación necesaria en caso que lo ameriten, al igual que las recomendaciones y sugerencias para un buen desarrollo del mismo, con el objeto del correcto cumplimiento de los objetivos de dicho TC.

UNIDAD III: ESTRECTURAS Y SERVICIOS DE REDES DE BANDA ANCHA

OBJETIVOS PARTICULARES:

- Comprender las aplicaciones y servicios que se brindan en una red de datos, analizando la importancia de cada uno de estos elementos.

- Examinar los diferentes tipos de conexión de Línea de Abonado Digital haciendo una comparación entre ellos.

- Interesarse en los servicios que se puede brindar en las redes de banda ancha comparándolos con los servicios que brindan los operadores nacionales de Telecomunicaciones.

CONTENIDOS

3.1 Aplicaciones y servicios en las Redes de Datos.

3.2 xDLS (Los diferentes tipos de conexión de Línea de Abonado Digital: DLS).

3.2.1 ADSL (Línea de Abonado Digital Asimétrica)

3.2.2 HDSL (Línea de Abonado Digital Veloz).

3.2.3 VDSL (Línea de Abonado Digital de muy alta tasa de transferencia).

3.2.4 DSL inalámbrico (Línea de Abonado Digital inalámbrico).

3.3 Servicios de Redes de Banda Ancha: FRAME RELAY, SMDS, ATM.

3.3.1 Definición, Estándares.

3.3.2 Acceso, red y equipos.

3.3.3 Protocolo y estructura de la celda.

3.3.4 Costos, ventajas y desventajas.

3.3.5 Aplicaciones.

RECOMENDACIONES METODOLÓGICAS

El contenido de esta unidad se desarrollará en cinco sesiones teóricas, dos de seminarios, y dos de laboratorios. Para los ítems 3.1 y 3.2 se sugiere hacer uso de presentaciones en PowerPoint a fin de hacerla más dinámica a la vez que se economiza tiempo con esta forma de docencia y se puede así, instar a los alumnos a participar con ejemplos que ellos conozcan de la realidad nacional o que ellos indaguen sobre lo que se utiliza actualmente en otros países referente a los diferentes tipos de conexiones DSL estudiados en esta unidad.

Para el tema 3.3 se recomienda que el estudiantado lo desarrolle con exposiciones utilizando algunas horas de las sesiones teóricas, así como de los seminarios ya que es un tema visto en las clases de **Redes de Computadora I y II**. Esta será parte de la nota sistemática a acumularse.

Para la sesión de laboratorio el docente deberá de suministrar la guía de laboratorio. Los Reporte de los laboratorios serán parte de la nota sistemática acumular. Se puede hacer ejercicios de conexión de DSL haciendo uso de la herramienta Packet Tracer.

El docente en las sesiones del TC, deberá ir monitoreando el correcto avance del mismo y comprobar que el estudiante este aplicando adecuadamente conocimientos adquiridos en las conferencias.

UNIDAD IV: REDES DE DATOS

OBJETIVOS PARTICULARES:

- Distinguir los aspectos que involucra la Transmisión Digital en un canal analógico aplicándolos en la discusión de los seminarios de esta unidad.

- Desarrollar un cuadro comparativo de los servicios que demandan la Conmutación de Circuitos o Conmutación de paquetes discutiendo este tema inmerso su ubicación en el modelo OSI.

- Valorar la importancia del estudio del MPLS (Conmutación Multi-Protocolo mediante Etiquetas), enfocándose que fue diseñado para unificar el servicio de transporte de datos para las redes basadas en conmutación de circuitos y paquetes.

CONTENIDOS

4.1 Transmisión Binaria.
- 4.1.1 Transmisión Asíncrona y Síncrona.
- 4.1.2 La interface de Datos (La capa física).
- 4.1.3 TIA/EIA-644 Señal Diferencial de bajo voltaje (LVDS).

4.2 Transmisión Digital en un canal analógico.

4.3 Modem (Modulación–Demodulación).

4.4 Conmutación de Circuitos y Conmutación de paquetes.
- 4.4.1 Redes de conmutación de circuitos.
- 4.4.2 Red de conmutación de paquetes (X.25).

4 5 Los protocolos TCP/IP.
- 4.5.1 El protocolo IP.
- 4.5.2 El protocolo TCP.
- 4.5.3 IPv6.

4.6 MPLS (Conmutación Multi-Protocolo mediante Etiquetas).
- 4.6.1 Acrónimo y Definición.
- 4.6.2 MPLS Descripción.
- 4.6.3 (VPN) Red Privada Virtual.

RECOMENDACIONES METODOLÓGICAS

Los ítems 4.1, 4.2 4.3 se recomiendan abordarlos a un nivel de reforzamiento ya que fueron temas de estudio de clases anteriores, pero involucra mucha matemática y proceso estocástico y es saludable un reforzamiento de estos temas. Las dos sesiones de clase práctica serán destinadas a reforzar estos temas.

Los ítems 4.4 y 4.5 por ser temas abordados en las clases de redes queda a discreción del docente ser destinados como temas de exposición haciéndose uso de las horas de seminario.

El tema 4.6 deberá ser abortado bajo la primicia que este estándar fue diseñado para poder brindar calidad de servicios en las redes de hoy en día (que transportan diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP) ya que MPLS fue diseñado para opera entre la capa de enlace de datos y la capa de red del modelo OSI; unificando el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes, donde es vital garantizar el trato adecuado al tráfico que es sensible en el tiempo.

La práctica de laboratorio puede realizarse con Packet Tracer sobre ejercicios de telefonía IP. El docente deberá de suministrar la guía de laboratorio.

Durante la sesión del TC, el docente deberá ir monitoreando el correcto avance del mismo y comprobar que el estudiante este aplicando adecuadamente conocimientos abordados en esta unidad.

UNIDAD V: TELEFONIA SOBRE IP

OBJETIVOS PARTICULARES:

- Definir los beneficios y aplicaciones de la voip comparándola con la telefonía convencional.

- Elaborar una comparación entre los protocolos de tiempo real y de reserva de recursos mencionando ejemplos de servicios que demanden estos protocolos.

- Manifestar interés en la obtención de Calidad de Servicio en la telefonía IP comparando el tratamiento especial que este servicio merece vs paquetes de datos.

CONTENIDOS

5.1 Beneficios y aplicaciones de la Telefonía sobre Internet.

5.2 Voz sobre IP (voip).

5.2.1 Arquitectura de red del estándar H.323.

5.2.2 Requerimientos del estándar H.323

5.2.3 Codificación y decodificación de Audio (CODEC).

5.2.3.1 Estándar G.711.

5.2.3.2 Estándar G.722.

5.2.3.3 Estándar G.723.

5.2.3.4 Estándar G.728.

5.2.3.5 Estándar G.729.

5.2.4 Eco, pérdida de paquetes y detección de actividad.

5.3 Protocolo de Transporte (RTP Y RSVP).

5.3.1 Protocolo de Transporte en Tiempo Real (RTP).

5.3.2 Protocolo de Transporte con reserva de recursos (RSVP).

5.4 Calidad de servicio en la Telefonía sobre IP.

RECOMENDACIONES METODOLÓGICAS

Para el desarrollo de esta unidad se hará uso de cinco sesiones teóricas, dos sesiones de seminario y una para TC. En las sesiones se recomienda el uso de presentaciones en PowerPoint por lo extenso y nivel teórico de los mismos. Se recomienda que los seminarios se realicen al finalizar la unidad para reforzar el conocimiento adquirido.

La sesión del TC se destinará a revisar los aspectos finales del reporte y hacer las ultimas sugerencias y/o recomendaciones de mejoras al mismo.

XIII. EVALUACIÓN DEL APRENDIZAJE: [10]

EVALUACIONES ORDINARIAS [11]		
I Evaluación Parcial	Evaluaciones Sistemáticas[12]	15%
	Examen	20%
II Evaluación Parcial	Evaluaciones Sistemáticas	15%
	Examen	20%

[10] UNI (2006): Reglamento de Régimen Académico de la Universidad Nacional de Ingeniería. Aprobado por el Consejo Universitario el 27 de octubre del 2006. Managua.
[11] Adecuar de conformidad con la naturaleza de cada programa de asignatura (Arto. 24 del Reglamento de Régimen Académico).
12 Preguntas de control, seminarios, clases prácticas, laboratorios, giras de campo, talleres, trabajos extra-clase, pruebas cortas. (Arto. 27 del Reglamento de Régimen Académico).

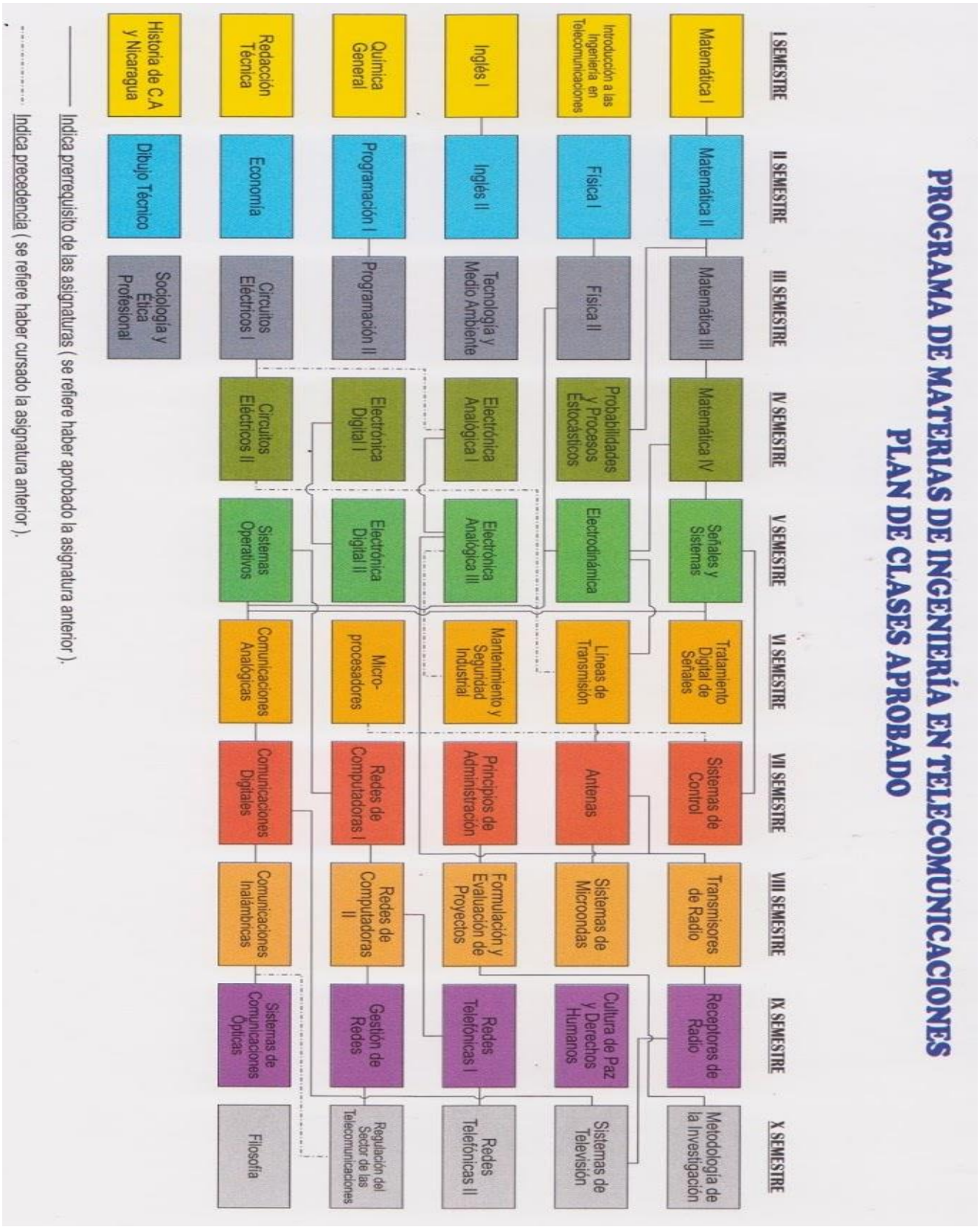
III Evaluación Parcial	Trabajo de Curso	30%
Total		100%
EVALUACIONES EXTRAORDINARIAS		
Convocatoria	Examen	70%
	Trabajo de Curso	30%
Total		100%

XIV. BIBLIOGRAFÍA:

14.1. Textos Básico:

- Bellamy, John C. (2000). *Digital Telephony*. USA. Wiley Interscience. 3ra Edicion.
- Caballero, José M. (1998). *Redes de Banda Ancha*. España. Editorial: Marcombo.
- Freeman, Roger L. (2004). *Telecommunication System Engineering*. USA. Editorial Editorial: Wiley Interscience. 4ta Edición.
- Freeman, Roger L. (2013). *Fundamentals of Telecommunications.* USA. Editorial Editorial: Wiley Interscience. 2da Edición.
- Stallings, William. (1999). *ISDN and Broadband ISDN with Frame Relay and ATM*. USA. Editorial: Prentice Hall. 4ta Edicion.

Pensum de Ingenieria en Telecomunicaciones



GUIA DE LABORATORIO 1: RESUELTA

Configuración de OSPF de área única para el intercambio de información de ruteo entre una empresa y sus sucursales.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Aplicar y reforzar conocimientos del protocolo de enrutamiento dinámico OSPF (Open Shortest Path First).
- Observar la manera que se intercambian la información de ruteo entre una empresa y sus sucursales.

INTRODUCCION

En la siguiente guía de laboratorio, se dará a conocer cómo funciona el protocolo de enrutamiento de dinámico OSPF. Mediante un ejemplo en el cual se evidencia como una empresa intercambia tablas de ruteo con sus sucursales de manera dinámica.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

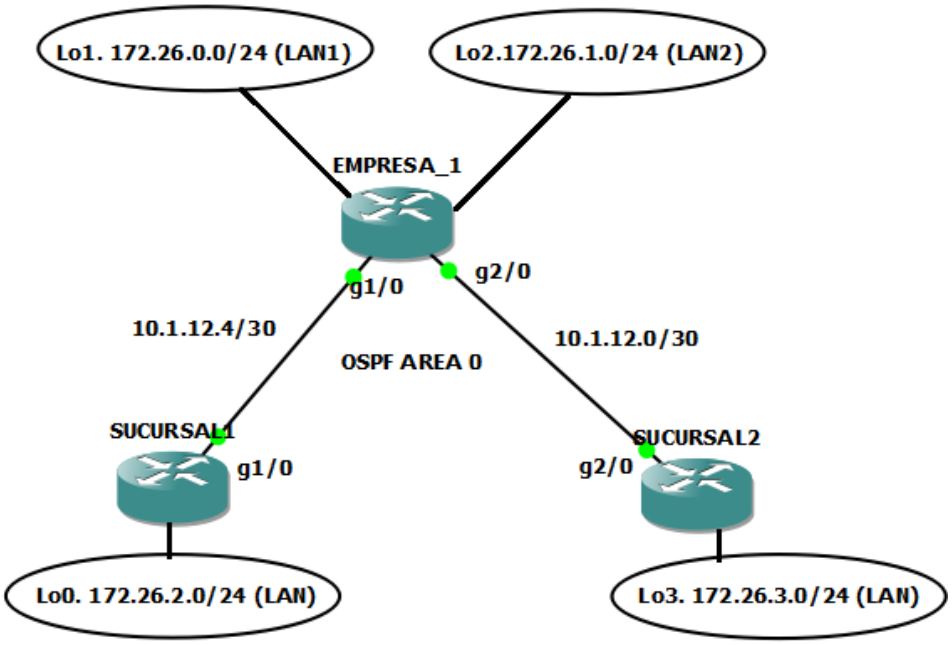


Tabla de direccionamiento

Equipo	Interfaz	Dirección IP	Mascara
EMPRESA_1	GigabitEthernet1/0	10.1.12.5	255.255.255.252
	GigabitEthernet2/0	10.1.12.1	255.255.255.252
	Loopback1 (LAN1)	172.26.0.1	255.255.255.0
	Loopback2 (LAN2)	172.26.1.1	255.255.255.0
SUCURSAL1	GigabitEthernet1/0	10.1.12.6	255.255.255.252
	Loopback0 (LAN)	172.26.2.1	255.255.255.0
SUCURSAL2	GigabitEthernet2/0	10.1.12.2	255.255.255.252
	Loopback3 (LAN)	172.26.3.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

Usando el direccionamiento propuesto en el diagrama anterior, crearemos interfaces loopback y aplicaremos el direccionamiento IPV4 para estas, así como la configuración de las interfaces gigabitEthernet asociadas a la empresa y sus sucursales. Las loopbacks configuradas en los routers simulan segmentos de redes reales utilizados por la empresa y sus sucursales para garantizar la conexión entre ellas.

EMPRESA_1(config)# interface Lo1
EMPRESA_1(config-if)# ip add 172.26.0.1 255.255.255.0
EMPRESA_1(config-if)#no shutdown
EMPRESA_1(config-if)#exit

EMPRESA_1(config)# interface Lo2
EMPRESA_1(config-if)# ip add 172.26.1.1 255.255.255.0

EMPRESA_1(config-if)#no shutdown

EMPRESA_1(config-if)#exit

EMPRESA_1(config)#int gigabitEthernet 1/0

EMPRESA_1(config-if)# description SUCURSAL1_Gi1/0

EMPRESA_1(config-if)# ip address 10.1.12.5 255.255.255.252

EMPRESA_1(config-if)#no shutdown

EMPRESA_1(config)#int gigabitEthernet 2/0

EMPRESA_1(config-if)# description SUCURSAL2_Gi2/0

EMPRESA_1(config-if)# ip address 10.1.12.1 255.255.255.252

EMPRESA_1(config-if)#no shutdown

SUCURSAL1(config)#int loopback 0

SUCURSAL1(config-if)# ip address 172.26.2.1 255.255.255.0

SUCURSAL1(config-if)#no shutdown

SUCURSAL1(config)#int gigabitEthernet 1/0

SUCURSAL1(config-if)# description EMPRESA1_Gi1/0

SUCURSAL1(config-if)# ip address 10.1.12.6 255.255.255.252

SUCURSAL1(config-if)#no shutdown

SUCURSAL2(config)#int loopback 3

SUCURSAL2(config-if)# ip address 172.26.3.1 255.255.255.0

SUCURSAL2(config-if)# no shutdown

SUCURSAL2(config)#int gigabitEthernet 2/0

SUCURSAL2(config-if)# description EMPRESA1_Gi2/0

SUCURSAL2(config-if)# ip address 10.1.12.2 255.255.255.252

SUCURSAL2(config-if)# no shutdown

Usar el comando ping para probar la conectividad entre los routers directamente conectados.

EMPRESA_1#ping 10.1.12.6

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.12.6, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/50/52 ms

EMPRESA_1#ping 10.1.12.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 44/49/52 ms

SUCURSAL1#ping 10.1.12.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.12.5, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/60 ms

SUCURSAL2#ping 10.1.12.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.12.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/48/56 ms

Paso 2.- Configurar OSPF en los routers.

Crear proceso OSPF 1 y defina OSPF router-id en los tres routers (*EMPRESA_1 = 1.1.1.1; SUCURSAL2 = 2.2.2.2; SUCURSAL1= 3.3.3.3).* Usando los comandos de

redes, configurar las subredes en las interfaces eléctricas entre los routers antes mecionados para agregarlos en el proceso ospf área 0. Así como enrutar las redes LAN simuladas en las interfaces loopback.

EMPRESA_1(config)#router ospf 1
EMPRESA_1(config-router)# router-id 1.1.1.1
EMPRESA_1(config-router)# network 10.1.12.0 0.0.0.3 area 0
EMPRESA_1(config-router)# network 10.1.12.4 0.0.0.3 area 0
EMPRESA_1(config-router)# network 172.26.0.0 0.0.0.255 area 0
EMPRESA_1(config-router)# network 172.26.1.0 0.0.0.255 area 0

EMPRESA_1(config)#interface GigabitEthernet1/0
EMPRESA_1(config-if)# ip ospf 1 area 0

EMPRESA_1(config)#interface GigabitEthernet2/0
EMPRESA_1(config-if)# ip ospf 1 area 0

El comando **show ip ospf** es utilizado para verificar el OSPF router ID. Si el router ID está utilizando valores de 32-bit, otro que no haya sido especificado por el comando Router-id. Se puede aplicar un reset router ID, mediante la utilización del comando clear ip ospf *pid* process y verificar nuevamente.

EMPRESA_1#sh ip ospf
Routing Process "ospf 1" with ID 172.26.1.1
Start time: 01:06:17.080, Time elapsed: 00:34:57.180
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msecs

Minimum hold time between two consecutive SPFs 10000 msecs

Maximum wait time between two consecutive SPFs 10000 msecs

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msecs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Number of areas transit capable is 0

External flood list length 0

IETF NSF helper support enabled

Cisco NSF helper support enabled

Reference bandwidth unit is 100 mbps

Area BACKBONE(0) (Inactive)

Number of interfaces in this area is 4 (2 loopback)

Area has no authentication

SPF algorithm last executed 00:00:02.404 ago

SPF algorithm executed 1 times

Area ranges are

Number of LSA 1. Checksum Sum 0x0009A9

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

EMPRESA_1#clear ip ospf process

Reset ALL OSPF processes? [no]: yes

EMPRESA_1#sh ip ospf

Routing Process "ospf 1" with ID 1.1.1.1

Start time: 01:06:17.080, Time elapsed: 00:37:51.260

Supports only single TOS(TOS0) routes

Supports opaque LSA

Supports Link-local Signaling (LLS)

Supports area transit capability

Supports NSSA (compatible with RFC 3101)

Event-log enabled, Maximum number of events: 1000, Mode: cyclic

Router is not originating router-LSAs with maximum metric

Initial SPF schedule delay 5000 msecs

Minimum hold time between two consecutive SPFs 10000 msecs

Maximum wait time between two consecutive SPFs 10000 msecs

Incremental-SPF disabled

Minimum LSA interval 5 secs

Minimum LSA arrival 1000 msecs

LSA group pacing timer 240 secs

Interface flood pacing timer 33 msecs

Retransmission pacing timer 66 msecs

Number of external LSA 0. Checksum Sum 0x000000

Number of opaque AS LSA 0. Checksum Sum 0x000000

Number of DCbitless external and opaque AS LSA 0

Number of DoNotAge external and opaque AS LSA 0

Number of areas in this router is 1. 1 normal 0 stub 0 nssa

Number of areas transit capable is 0

External flood list length 0

IETF NSF helper support enabled

Cisco NSF helper support enabled

Reference bandwidth unit is 100 mbps

Area BACKBONE(0) (Inactive)

Number of interfaces in this area is 4 (2 loopback)

Area has no authentication

SPF algorithm last executed 00:00:14.128 ago

SPF algorithm executed 1 times

Area ranges are

Number of LSA 1. Checksum Sum 0x00BF7C

Number of opaque link LSA 0. Checksum Sum 0x000000

Number of DCbitless LSA 0

Number of indication LSA 0

Number of DoNotAge LSA 0

Flood list length 0

SUCURSAL2(config)#router ospf 1
SUCURSAL2(config-router)# router-id 2.2.2.2
SUCURSAL2(config-router)# network 10.1.12.0 0.0.0.3 area 0
SUCURSAL2(config-router)# network 172.26.3.0 0.0.0.255 area 0

SUCURSAL2(config)#interface GigabitEthernet2/0
SUCURSAL2(config-if)# ip ospf 1 area 0

SUCURSAL1(config)#router ospf 1
SUCURSAL1(config-router)# router-id 3.3.3.3
SUCURSAL1(config-router)#network 10.1.12.4 0.0.0.3 area 0
SUCURSAL1(config-router)#network 172.26.2.0 0.0.0.255 area 0

SUCURSAL1(config)#interface GigabitEthernet1/0
SUCURSAL1(config-if)# ip ospf 1 area 0

Nuevamente, el comando **show ip ospf** debe ser usado para verificar el OSPF router id. Que este sea igual al especificado por el comando router-id. En caso de que este no coincida se deberá aplicar reset al proceso OSPF en ambos routers R2 y R3. Mediante el comando **clear ip ospf process.** Luego verificar nuevamente.

Verificar que se observe los vecinos ospf, por medio del comando **show ip ospf neighbors** en la salida de los routers. Así como garantizar los routers puedan aprender las loopbacks declaradas entre ellos. Con el comando **show ip route.**

EMPRESA_1#sh ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*
3.3.3.3	*1*	*FULL/DR*	*00:00:35*	*10.1.12.6*	*GigabitEthernet1/0*
2.2.2.2	*1*	*FULL/DR*	*00:00:31*	*10.1.12.2*	*GigabitEthernet2/0*

CUESTIONARIO

¿Cuál son los ID de los vecinos con quien el equipo EMPRESA_1 con que el equipo hablaba OSPF?

R/ El equipo tiene de vecino a los siguientes ID 2.2.2.2 Y 3.3.3.3. Por las interfaces Gi1/0 y Gi2/0. Recordemos que si no se configura el Router-id dentro del OSPF. Mostrará como vecinos las direcciones IP ocupadas para garantizar la conectividad punto a punto. Lo que ocasionaría problemas a la hora de elegir DR/BDR.

EMPRESA_1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.12.0/30 is directly connected, GigabitEthernet2/0
L 10.1.12.1/32 is directly connected, GigabitEthernet2/0
C 10.1.12.4/30 is directly connected, GigabitEthernet1/0
L 10.1.12.5/32 is directly connected, GigabitEthernet1/0
172.26.0.0/16 is variably subnetted, 6 subnets, 2 masks
C 172.26.0.0/24 is directly connected, Loopback1
L 172.26.0.1/32 is directly connected, Loopback1
C 172.26.1.0/24 is directly connected, Loopback2
L 172.26.1.1/32 is directly connected, Loopback2
O 172.26.2.0/24 [110/2] via 10.1.12.6, 00:09:56, GigabitEthernet1/0
O 172.26.3.0/24 [110/2] via 10.1.12.2, 00:09:56, GigabitEthernet2/0

¿Cuantos prefijos son aprendidos mediante el protocolo dinámico OSPF en el equipo EMPRESA_1?

R/ Este aprende dos segmentos ip, los cuales serán fáciles de identificar en la tabla de rutas debido a que se les antepone la letra O. los cuales son 172.26.2.0/24 y 172.26.3.0/24

SUCURSAL1# sh ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*
1.1.1.1	*1*	*FULL/BDR*	*00:00:34*	*10.1.12.5*	*GigabitEthernet1/0*

¿Cuál es el ID del vecino para el Router SUCURSAL_1?

R/ El router tiene como vecino al ID 1.1.1.1.

SUCURSAL1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.1.12.0/30 [110/2] via 10.1.12.5, 00:13:48, GigabitEthernet1/0
C 10.1.12.4/30 is directly connected, GigabitEthernet1/0
L 10.1.12.6/32 is directly connected, GigabitEthernet1/0
172.26.0.0/16 is variably subnetted, 5 subnets, 2 masks
O 172.26.0.0/24 [110/2] via 10.1.12.5, 00:13:48, GigabitEthernet1/0
O 172.26.1.0/24 [110/2] via 10.1.12.5, 00:13:48, GigabitEthernet1/0
C 172.26.2.0/24 is directly connected, Loopback0
L 172.26.2.1/32 is directly connected, Loopback0
O 172.26.3.0/24 [110/3] via 10.1.12.5, 00:13:38, GigabitEthernet1/0

¿Qué segmentos de red debe de aprender el equipo SUCURSAL_1? ¿Por qué?

R/ Este equipo debe aprender los segmentos que se encuentren distribuidos dentro del proceso OSPF de los equipos EMPRESA_1 y SUCURSAL_2. Los cuales son:

10.1.12.0/30
172.26.0.0/24
172.26.1.0/24
172.26.3.0/24

SUCURSAL2#sh ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 FULL/BDR 00:00:33 10.1.12.1 GigabitEthernet2/0

¿Cuál es el ID del vecino para el Router SUCURSAL_1?

R/ El router tiene como vecino al ID 1.1.1.1.

SUCURSAL2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C 10.1.12.0/30 is directly connected, GigabitEthernet2/0
L 10.1.12.2/32 is directly connected, GigabitEthernet2/0
O 10.1.12.4/30 [110/2] via 10.1.12.1, 00:14:23, GigabitEthernet2/0
172.26.0.0/16 is variably subnetted, 5 subnets, 2 masks
O 172.26.0.0/24 [110/2] via 10.1.12.1, 00:14:23, GigabitEthernet2/0
O 172.26.1.0/24 [110/2] via 10.1.12.1, 00:14:23, GigabitEthernet2/0
O 172.26.2.0/24 [110/3] via 10.1.12.1, 00:14:23, GigabitEthernet2/0
C 172.26.3.0/24 is directly connected, Loopback3
L 172.26.3.1/32 is directly connected, Loopback3

¿Qué segmentos de red debe de aprender el equipo SUCURSAL_2? ¿Por qué?

R/ Este equipo debe aprender los segmentos que se encuentren distribuidos dentro del proceso OSPF de los equipos EMPRESA_1 y SUCURSAL_1. Los cuales son:

10.1.12.4/30
172.26.0.0/24
172.26.1.0/24
172.26.2.0/24

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

GUIA DE LABORATORIO 2: RESUELTA

Configuración de OSPF Multi-Área y su compartimiento con la redistribución de rutas estáticas.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Aplicar y reforzar conocimientos del protocolo de enrutamiento dinámico OSPF (Open Shortest Path First).
- Configure OSPFv2 de áreas múltiples para IPv4
- Verificar el comportamiento de múltiples áreas.
- Observar la manera que se intercambian la información de ruteo entre diferentes áreas.

INTRODUCCION

En la siguiente guía de laboratorio, se realizará la configuración de OSPFv2 de áreas múltiples para IPv4. Y su comportamiento redistribuyendo rutas estáticas en el proceso OSPF.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

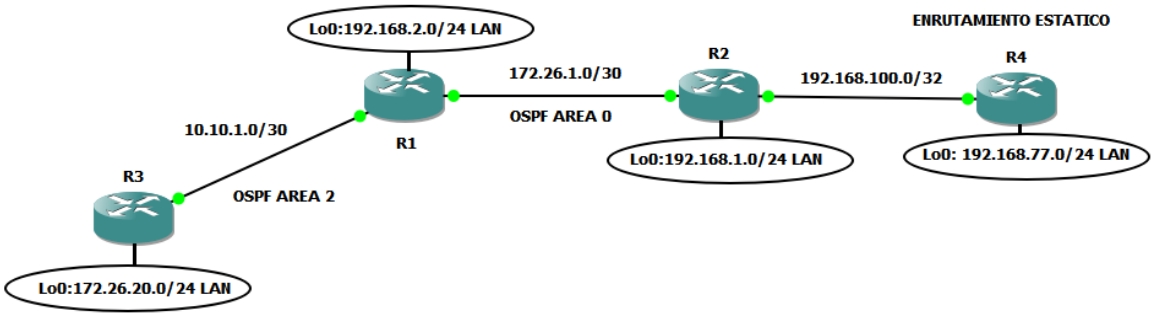


Tabla de direccionamiento

Equipo	Interfaz	Direccionamiento IP	Mascara
R1	GigabitEthernet1/0	172.26.1.1	255.255.255.252
	GigabitEthernet2/0	10.10.1.1	255.255.255.252
	Loopback1(LAN)	192.168.2.1	255.255.255.0
R2	GigabitEthernet1/0	172.26.1.2	255.255.255.252
	GigabitEthernet2/0	192.168.100.1	255.255.255.252
	Loopback1(LAN)	192.168.1.1	255.255.255.0
R3	GigabitEthernet2/0	10.10.1.2	255.255.255.252
	Loopback1(LAN)	172.26.20.1	255.255.255.0
R4	GigabitEthernet2/0	192.168.100.2	255.255.255.252
	Loopback1(LAN)	192.168.77.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

En este laboratorio, se configurara una red OSFPv2 Multi-area para IPV4. El área 2 se configurará como un área normal de OSPF, un área de código auxiliar y usando el direccionamiento propuesto en el diagrama anterior, aplicaremos el direccionamiento IPV4 para las interfaces gigabit Ethernet e interfaces virtuales. Las loopbacks configuradas en los routers simulan segmentos de redes reales.

R1(config)#interface GigabitEthernet1/0
R1(config-if)#ip address 172.26.1.1 255.255.255.252
R1(config-if)#no shutdown

R1(config)#interface GigabitEthernet2/0
R1(config-if)#description R3_GI2/0

R1(config-if)#ip address 10.10.1.1 255.255.255.252

R1(config-if)#no shutdown

R1(config)#interface Loopback1

R1(config-if)#description LAN_1

R1(config-if)#ip address 192.168.2.1 255.255.255.0

R1(config-if)#no shutdown

R2(config)#interface GigabitEthernet1/0

R2(config-if)#description R1_GI1/0

R2(config-if)#ip address 172.26.1.2 255.255.255.252

R2(config-if)#no shutdown

R2(config)#interface GigabitEthernet2/0

R2(config-if)#description R4_GI2/0

R2(config-if)#ip address 192.168.100.1 255.255.255.252

R2(config-if)#no shutdown

R2(config)#interface Loopback1

R2(config-if)#description LAN_1

R2(config-if)#ip address 192.168.1.1 255.255.255.0

R2(config-if)#no shutdown

R3(config)#interface GigabitEthernet2/0

R3(config-if)#description R1_GI2/0

R3(config-if)#ip address 10.10.1.2 255.255.255.252

R3(config-if)#no shutdown

R3(config)#interface Loopback1

R3(config-if)#description LAN_1

R3(config-if)#ip address 172.26.20.1 255.255.255.0

R3(config-if)#no shutdown

R4(config)#interface GigabitEthernet2/0
R4(config-if)#description R2_GI2/0
R4(config-if)#ip address 192.168.100.2 255.255.255.252
R4(config-if)#no shutdown

R4(config)#interface Loopback1
R4(config-if)#description LAN_1
R4(config-if)#ip address 192.168.77.1 255.255.255.0
R4(config-if)#no shutdown

Realizar pruebas de conectividad a nivel L3, mediante Ping.

R1#ping 172.26.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.26.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/70/76 ms

R1#ping 10.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/50/52 ms

R2#ping 172.26.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.26.1.1, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/56 ms

R2#ping 192.168.100.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/48/52 ms

R3#ping 10.10.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/46/52 ms

R4#ping 192.168.100.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/60 ms

Paso 2.- Configurar OSPF en los routers.

Crea proceso OSPFv2 1 en los router R1, R2 y proceso 120 en el router R3. Configurar el OSPF Router ID en cada uno de ellos. Habilitar redes directamente conectadas en el proceso OSPF utilizando **ip ospf *process-id* área *área-id*** (R1=1.1.1.1; R2=2.2.2.2; R3=3.3.3.3).

El comando **show ip ospf** es utilizado para verificar el OSPF router ID. Si el router ID está utilizando valores de 32-bit, otro que no haya sido especificado por el comando Router-id. Se puede aplicar un reset router ID, mediante la utilización del comando **clear ip ospf *pid* process** y verificar nuevamente.

Configurar R2 con router OSPFv2 en área 0

R2(config)#router ospf 1
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 192.168.1.0 0.0.0.255 area 0

R2(config)#interface GigabitEthernet1/0
R2(config-if)# ip ospf 1 area 0

Configurar R1, como router ABR para el área o y área 2. Interfaz Gi1/0 en el área 0 y la interfaz Gi2/0 en el área 2.

R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0

R1(config)#interface GigabitEthernet1/0
R1(config-if)# ip ospf 1 area 0

R1(config)#interface GigabitEthernet2/0
R1(config-if)# ip ospf 1 area 2

Paso 3.- Configurar R3 como router OSPFv2 interno en el área 2.

R3(config)#router ospf 120
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 172.26.20.0 0.0.0.255 area 2

R3(config)#int gigabitEthernet 2/0
R3(config-if)#ip ospf 120 area 2

Verificar que los routers tengan vecinos OSPFv2. Utilizando el comando show ip ospf neighbors. A continuación se muestra el router R1

R1#sh ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*
2.2.2.2	*1*	*FULL/DR*	*00:00:32*	*172.26.1.2*	*GigabitEthernet1/0*
3.3.3.3	*1*	*FULL/BDR*	*00:00:34*	*10.10.1.2*	*GigabitEthernet2/0*

Verificar que el router R2 pueda ver todas las redes IPv4 en la tabla de enrutamiento OSPFv2 usando el comando show ip route.

R2#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 192.168.100.2 to network 0.0.0.0

O IA 10.10.1.0 [110/2] via 172.26.1.1, 00:03:27, GigabitEthernet1/0
172.26.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.26.1.0/30 is directly connected, GigabitEthernet1/0
L 172.26.1.2/32 is directly connected, GigabitEthernet1/0
O IA 172.26.20.1/32 [110/3] via 172.26.1.1, 00:03:27, GigabitEthernet1/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Loopback1
L 192.168.1.1/32 is directly connected, Loopback1

192.168.2.0/32 is subnetted, 1 subnets

O 192.168.2.1 [110/2] via 172.26.1.1, 00:03:27, GigabitEthernet1/0

C 192.168.100.0/30 is directly connected, GigabitEthernet2/0

L 192.168.100.1/32 is directly connected, GigabitEthernet2/0

Ejecutar el comando sh ip route en el router R1

R1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

*ia - IS-IS inter area, * - candidate default, U - per-user static route*

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

+ - replicated route, % - next hop override

Gateway of last resort is 172.26.1.2 to network 0.0.0.0

C 10.10.1.0/30 is directly connected, GigabitEthernet2/0

L 10.10.1.1/32 is directly connected, GigabitEthernet2/0

172.26.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.26.1.0/30 is directly connected, GigabitEthernet1/0

L 172.26.1.1/32 is directly connected, GigabitEthernet1/0

O 172.26.20.1/32 [110/2] via 10.10.1.2, 00:16:59, GigabitEthernet2/0

192.168.1.0/32 is subnetted, 1 subnets

O 192.168.1.1 [110/2] via 172.26.1.2, 00:16:59, GigabitEthernet1/0

192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.2.0/24 is directly connected, Loopback1

L 192.168.2.1/32 is directly connected, Loopback1

Paso 4.- Configura una ruta estática IPV4 por defecto en el router ASBR R2 para reenviar tráfico para el router R4. Y propagar la ruta estática por defecto en el OSPFv2.

R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.2
R2(config)#router ospf 1
R2(config-router)# default-information originate

Para el router R4 se deberá crear una ruta estatica por defecto para que pueda alcanzar todas rutas anunciados por los procesos OSPF multiarea.

R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.100.1

Ejecute el comando show ip route static en el R2, para verificar la ruta estática la tabla de enrutamiento IPV4.

R2#sh ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 192.168.100.2 to network 0.0.0.0

S 0.0.0.0/0 [1/0] via 192.168.100.2*

Se requiere la configuración de una ruta estática en el router ASBR, La cual simule un cliente que se encuentre fuera del proceso de enrutamiento dinámico. R2 para la

red 192.168.77.0/24 del R4. Redistribuye la ruta estática en el proceso OSPFv2 usando el comando **redistribute static subnets**. El parámetro de subredes se usa para incluir subredes y no solo direcciones de red con clase.

R2(config)#ip route 192.168.77.0 255.255.255.0 192.168.100.2
R2(config)#router ospf 1
R2(config-router)# redistribute static subnets

Utiliza el comando show ip route ospf en el R3, para verificar que la ruta predeterminada y la ruta estática redistribuida se anuncian en el proceso OSPFv2.

R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.10.1.1 to network 0.0.0.0

*O*E2 0.0.0.0/0 [110/1] via 10.10.1.1, 01:21:11, GigabitEthernet2/0*
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.1.0/30 is directly connected, GigabitEthernet2/0
L 10.10.1.2/32 is directly connected, GigabitEthernet2/0
172.26.0.0/16 is variably subnetted, 3 subnets, 3 masks
O IA 172.26.1.0/30 [110/2] via 10.10.1.1, 01:21:11, GigabitEthernet2/0
C 172.26.20.0/24 is directly connected, Loopback1
L 172.26.20.1/32 is directly connected, Loopback1
192.168.1.0/32 is subnetted, 1 subnets
O IA 192.168.1.1 [110/3] via 10.10.1.1, 01:21:11, GigabitEthernet2/0

192.168.2.0/32 is subnetted, 1 subnets

O IA 192.168.2.1 [110/2] via 10.10.1.1, 01:21:11, GigabitEthernet2/0

O E2 192.168.77.0/24 [110/20] via 10.10.1.1, 01:21:11, GigabitEthernet2/0

CUESTIONARIO

¿Qué significa el "E2" para la ruta predeterminada y la ruta externa redistribuida?

R/ Significa que es una ruta externa de OSPF tipo 2.

¿Por qué en el router R1 no tiene rutas inter-area en su tabla de enrutamiento?

R/ No tiene rutas inter-area debido a que él es el rouer ASBR. Y se encuentra entre las 2 áreas 0 y 2.

¿Cuantas rutas OSPFv2 intra-area hay en el router R2 dentro su tabla de enrutamiento IPV4? ¿Cuántas rutas inter-area hay en su tabla de enrutamiento?

R/ Para el Router R2 se tiene 1 ruta intra-area (son rutas que se originan y aprenden en la misma área OSPF). Y 2 rutas inter-area (se originaron en algún otro área OSPF y se anuncian en su área OSPF).

¿Qué direccionamiento en el R2 es utilizado para establecer adyacencia de vecindad con el R1?

R/ Utiliza la dirección IP 172.26.1.2

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

GUIA DE LABORATORIO 3: RESUELTA

Configuración de BGP para el intercambio de información de ruteo entre dos ISP y un cliente.

OBJETIVOS

- Aprender a utilizar el programa GNS3
- Aplicar y reforzar conocimientos del protocolo de enrutamiento de Gateway exterior (BGP)
- Observar la manera que se intercambian la información de ruteo entre los ISP y un cliente que tiene distintos sistemas autónomos (AS)
- Aprender a configurar EBGP

INTRODUCCION

En la siguiente guía de laboratorio, se dará a conocer cómo funciona el protocolo de enrutamiento de dinámico de Gateway exterior BGP. Mediante un ejemplo en el que se evidencie como 3 empresas de proveedoras de servicios intercambian tablas de ruteo entre ellas.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt.

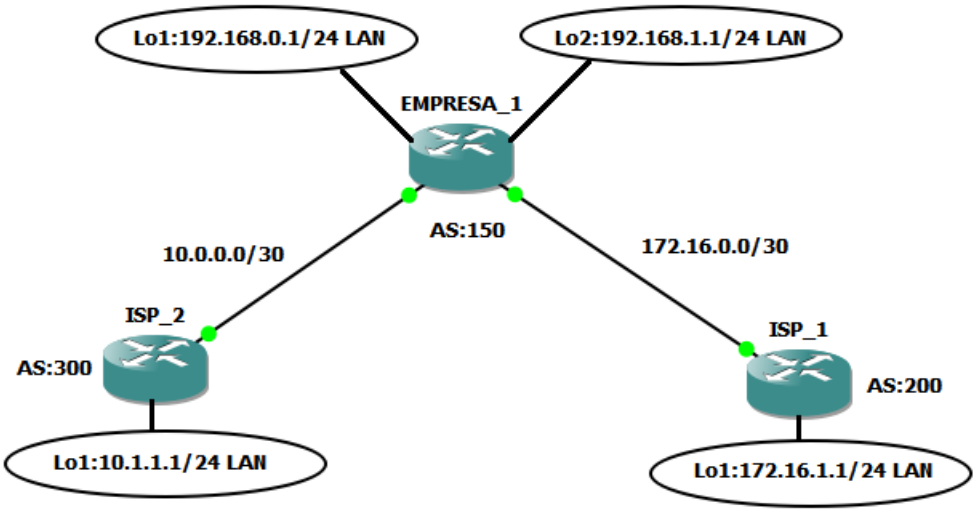


Tabla de direccionamiento

Equipo	Interfaz	Direccionamiento IP	Mascara
ENPRESA_1	GigabitEthernet1/0	10.0.0.1	255.255.255.252
	GigabitEthernet2/0	172.16.0.1	255.255.255.252
	Loopback0 (LAN)	192.168.0.1	255.255.255.0
	Loopback1 (LAN)	192.168.1.1	255.255.255.0
ISP_1	GigabitEthernet2/0	172.16.0.2	255.255.255.252
	Loopback0 (LAN)	172.16.1.1	255.255.255.0
ISP_2	GigabitEthernet1/0	10.0.0.2	255.255.255.252
	Loopback0 (LAN)	10.1.1.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

Usando el direccionamiento propuesto en el diagrama anterior, crearemos interfaces loopback y aplicaremos el direccionamiento IPV4 para estas, así como en las interfaces gigabitEthernet asociadas a ISP_1, ISP_2 y EMPRESA_1. Las loopbacks configuradas en los routers ISP simulan redes reales que pueden ser alcanzadas a través de los ISP.

```
ISP_2(config)# interface Lo0
ISP_2 (config-if)# ip add 10.1.1.1 255.255.255.0
ISP_2(config-if)#no shutdown
ISP_2(config-if)#exit


ISP_2(config)#int gigabitEthernet 1/0
ISP_2(config-if)# description EMPRESA_1_GI0/1
ISP_2(config-if)# ip address 10.0.0.2 255.255.255.252
ISP_2(config-if)#no shutdown

EMPRESA_1(config)#int loopback 0
EMPRESA_1(config-if)# ip address 192.168.0.1 255.255.255.0
EMPRESA_1(config-if)#no shutdown

EMPRESA_1(config)#int loopback 1
EMPRESA_1(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
EMPRESA_1(config-if)#no shutdown

EMPRESA_1(config)#int gigabitEthernet 1/0
EMPRESA_1(config-if)# description ISP_2_G1/0
EMPRESA_1(config-if)# ip address 10.0.0.1 255.255.255.252
EMPRESA_1(config-if)#no shutdown

EMPRESA_1(config)#int gigabitEthernet 2/0
EMPRESA_1(config-if)#description ISP_1_GI2/0
EMPRESA_1(config-if)# ip address 172.16.0.1 255.255.255.252
EMPRESA_1(config-if)#no shutdown

ISP_1(config)#int loopback 0
ISP_1(config-if)# ip address 172.16.1.1 255.255.255.0
ISP_1(config-if)# no shutdown

ISP_1(config)#int gigabitEthernet 2/0
ISP_1(config-if)# description EMPRESA_1_GI2/0
ISP_1(config-if)# ip address 172.16.0.2 255.255.255.252
ISP_1(config-if)# no shutdown
```

Usar ping para probar la conectividad entre los routers directamente conectados. **Nota:** no se logra alcanzar las IP entre los router ISP_1 y ISP_2.

```
ISP_2#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/72/76 ms

EMPRESA_1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/53/60 ms

EMPRESA_1#ping 172.16.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/48/56 ms

ISP_1#ping 172.16.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/47/60 ms
```

Paso 2.- Configurar BGP en los routers ISP (ISP_1, ISP_2)

En los routers ISP_1 y ISP_2. Configure BGP punto a punto con el router borde (EMPRESA_1) y anuncie las redes loopback de los ISP. Configure los AS según topología.

```
ISP_2(config)#router bgp 300
ISP_2(config-router)# bgp log-neighbor-changes
ISP_2(config-router)# neighbor 10.0.0.1 remote-as 150
ISP_2(config-router)# network 10.1.1.0 mask 255.255.255.0

ISP_1(config)#router bgp 200
ISP_1(config-router)# bgp log-neighbor-changes
ISP_1(config-router)# neighbor 172.16.0.1 remote-as 150
ISP_1(config-router)# network 172.16.1.0 mask 255.255.255.0
```

Paso 3.- Configurar BGP en el router borde EMPRESA_1.

Configurar el router EMPRESA_1 para que corra el protocolo BGP con los proveedores de servicio. Configure los AS según topología.

```
EMPRESA_1(config)#router bgp 150
EMPRESA_1(config)# bgp log-neighbor-changes
EMPRESA_1(config-router)# neighbor 10.0.0.2 remote-as 300
EMPRESA_1(config-router)# neighbor 172.16.0.2 remote-as 200
EMPRESA_1(config-router)# network 192.168.0.0
EMPRESA_1(config-router)# network 192.168.1.0
```

Para verificar que la configuración se encuentra aplicada correctamente. Se debe verificar la tabla de enrutamiento con el comando sh ip route.

```
EMPRESA_1# sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        10.0.0.0/30 is directly connected, GigabitEthernet1/0
L        10.0.0.1/32 is directly connected, GigabitEthernet1/0
B        10.1.1.0/24 [20/0] via 10.0.0.2, 01:04:43
     172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
```

```
C       172.16.0.0/30 is directly connected, GigabitEthernet2/0
L       172.16.0.1/32 is directly connected, GigabitEthernet2/0
B       172.16.1.0/24 [20/0] via 172.16.0.2, 01:35:14
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, Loopback0
L       192.168.0.1/32 is directly connected, Loopback0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback1
L       192.168.1.1/32 is directly connected, Loopback1
```

Pasó 3.- Verificar BGP en los routers

Para verificar la operatividad de BGP en el router EMPRESA_1, se utiliza el siguiente comando show ip bgp.

```
EMPRESA_1#sh ip bgp
BGP table version is 5, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.1.1.0/24     10.0.0.2                 0             0 300 i
 *>  172.16.1.0/24    172.16.0.2               0             0 200 i
 *>  192.168.0.0      0.0.0.0                  0         32768 i
 *>  192.168.1.0      0.0.0.0                  0         32768 i
```

En EMPRESA_1. Usa el comando **show ip bgp neighbors**. Visualice los AS y id, versión de BGP.

```
EMPRESA_1#        sh ip bgp neighbors
BGP neighbor is 10.0.0.2, remote AS 300, external link
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 03:36:38
  Last read 00:00:35, last write 00:00:49, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
```

```
                Sent       Rcvd
  Opens:           1          1
  Notifications:   0          0
  Updates:         6          4
  Keepalives:    237        240
  Route Refresh:   0          0
  Total:         244        245
Default minimum time between advertisement runs is 30 seconds
```

CUESTIONARIO

¿Cuál es el ID del router local? Demuestre con comandos

R/ 192.168.1.1

¿Cuál es la versión de tabla mostrada?

R/ BGP table version is 5

(*) A la par de la ruta indica que es válida. (>) Indica que la ruta hacia seleccionada como la mejor ruta.
Para verificar la operación en el router Cotel, usando el comando show ip bgp.

```
ISP_2#sh ip bgp
BGP table version is 5, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>  10.1.1.0/24     0.0.0.0                  0         32768 i
 *>  172.16.1.0/24   10.0.0.1                               0 150 200 i
 *>  192.168.0.0     10.0.0.1                 0            0 150 i
 *>  192.168.1.0     10.0.0.1                 0            0 150 i
```

¿Cuál es la versión de tabla y es esta la misma versión de tabla bgp que la del router EMPRESA_1? Explique su respuesta

R/ BGP table version is 5, y si es la misma. Son las mismas versiones porque la información de tablas de intercambian entres los routers

Para ISP_2, ¿Cuál es la ruta de la red 172.16.1.0/24?

R/ La ruta es conocida por la ip 10.0.0.1, por protocolo bgp en el router EMPRESA_1, ya que esa red pertenece al isp de claro.

En el router ISP_2. Aplique el comando shutdown en la interfaz lo0, y después valide las rutas bgp en el EMPRESA_1.

ISP_2(config)#int loopback 0
ISP_2(config-if)#shutdown
ISP_2(config-if)#exit

EMPRESA_1#sh ip bgp
BGP table version is 6, local router ID is 192.168.1.1
*Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,*
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

	Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
*>	*172.16.1.0/24*	*172.16.0.2*	*0*		*0*	*200 i*
*>	*192.168.0.0*	*0.0.0.0*	*0*		*32768*	*i*
*>	*192.168.1.0*	*0.0.0.0*	*0*		*32768*	*i*

¿Cuál es la versión de la tabla mostrada? ¿Por qué?

R/ BGP table version is 6, y este se incrementó debido a que surgió un cambio en la tabla de enrutamiento.

¿Qué paso con la ruta para la red 10.1.1.0/24?

R/ La ruta dejo de distribuirse por bgp debido a que se apagó la interfaz lo0.

En el router ISP_2, realizar Roll back en la interfaz int lo0 con el comando no shutdown

ISP_2l(config)#int loopback 0
ISP_2(config-if)#no shutdown
ISP_2(config-if)#exit

¿Cuál es el estado del bgp entre este router EMPRESA_1 y el ISP_2?

R/ BGP state = Established.

¿Cuánto tiempo tiene de estar esta conexión activa?

R/ up for 03:45:51

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.

GUIA DE LABORATORIO 4: RESUELTA

Configuración de MPLS L3, VPN-MPLS para cliente EMPRESA_1.

OBJETIVOS

- Aprender a utilizar el programa GNS3.
- Configurar OSPFv2 de área única IPv4.
- Configurar el protocolo de etiqueta MPLS LDP.
- Configurar el protocolo dinámico BGP.
- Configuración de VRF para servicios de clientes. Haciendo uso de la tecnología MPLS L3 VPN.

INTRODUCCION

En la siguiente guía de laboratorio, se realizarán las configuraciones de una red MPLS-VPN donde se configura la casa matriz junto con sus sucursales del cliente EMPRESA_1 para que posean conectividad utilizando la infraestructura del proveedor. Igualmente se configura un anillo MPLS con redundancia, este simula una red WAN de un ISP.

REQUERIMIENTOS

- Computadora Procesador i3, 4GB RAM
- Programa GNS3.
- Programa SecureCrt

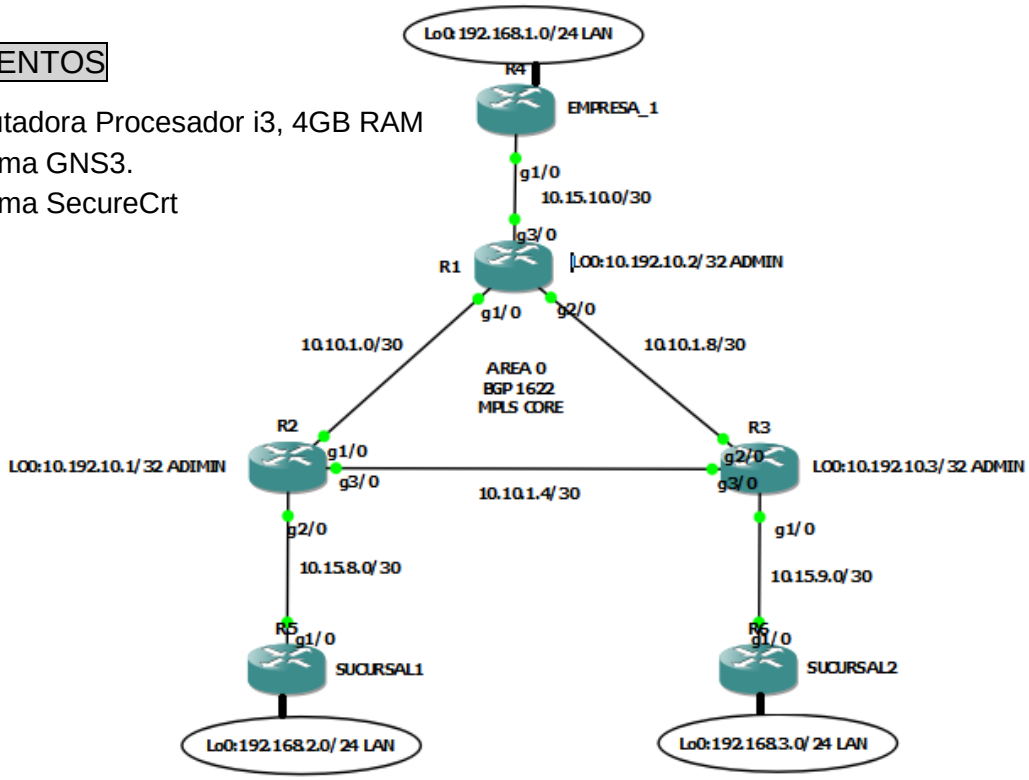


Tabla de direccionamiento

Equipo	Interfaz	Dirección IP	Mascara
R1	Loopback0 (Admin)	10.192.10.1	255.255.255.255
	GigabitEthernet1/0	10.10.1.1	255.255.255.252
	GigabitEthernet2/0	10.10.1.9	255.255.255.252
	GigabitEthernet3/0	10.15.10.1	255.255.255.252
R2	Loopback0(Admin)	10.192.10.2	255.255.255.255
	GigabitEthernet1/0	10.10.1.2	255.255.255.252
	GigabitEthernet3/0	10.10.1.5	255.255.255.252
	GigabitEthernet2/0	10.15.8.1	255.255.255.252
R3	Loopback0(Admin)	10.192.10.3	255.255.255.255
	GigabitEthernet2/0	10.10.1.10	255.255.255.252
	GigabitEthernet3/0	10.10.1.6	255.255.255.252
	GigabitEthernet1/0	10.15.9.1	255.255.255.252
R4	GigabitEthernet1/0	10.15.10.2	255.255.255.252
	Loopback0 (LAN)	192.168.1.1	255.255.255.0
R5	GigabitEthernet1/0	10.15.8.2	255.255.255.252
	Loopback0 (LAN)	192.168.2.1	255.255.255.0
R6	GigabitEthernet1/0	10.15.9.2	255.255.255.252
	Loopback0 (LAN)	192.168.3.1	255.255.255.0

PROCEDIMIENTO

Paso 1.- Configuración de las direcciones IP en las interfaces físicas y virtuales.

En este laboratorio, se configurara una red OSFPv2 multi-área para IPV4. El área 2 se configurará como un área normal de OSPF, un área de código auxiliar y usando el direccionamiento propuesto en el diagrama anterior, aplicaremos el

direccionamiento IPV4 para las interfaces gigabit Ethernet e interfaces virtuales. Las loopbacks configuradas en los routers simulan segmentos de redes reales.

PE1(config)#interface GigabitEthernet1/0
PE1(config-if)# description PE2_GI1/0
PE1(config-if)# ip address 10.10.1.1 255.255.255.252
PE1(config-if)#no shut

PE1(config)#interface GigabitEthernet2/0
PE1(config-if)# description PE3_GI2/0
PE1(config-if)# ip address 10.10.1.9 255.255.255.252
PE1(config-if)#no shut

PE1(config)#interface Loopback0
PE1(config-if)# description ADMIN
PE1(config-if)# ip address 10.192.10.1 255.255.255.255
PE1(config-if)#no shut

PE2(config)#interface GigabitEthernet1/0
PE2(config-if)# description PE1_GI1/0
PE2(config-if)#ip address 10.10.1.2 255.255.255.252
PE2(config-if)#no shut

PE2(config)#interface GigabitEthernet3/0
PE2(config-if)# description PE3_GI3/0
PE2(config-if)#ip address 10.10.1.5 255.255.255.252
PE2(config-if)#no shut

PE2(config)#interface Loopback0
PE2(config-if)# description ADMIN
PE2(config-if)# ip address 10.192.10.2 255.255.255.255

PE2(config-if)#no shut

PE3(config)#interface GigabitEthernet2/0
PE3(config-if)# description PE1_GI2/0
PE3(config-if)#ip address 10.10.1.10 255.255.255.252
PE3(config-if)#no shut

PE3(config)#interface GigabitEthernet3/0
PE3(config-if)# description PE2_GI3/0
PE3(config-if)# ip address 10.10.1.6 255.255.255.252
PE3(config-if)#no shut

PE3(config)#interface Loopback0
PE3(config-if)# description ADMIN
PE3(config-if)# ip address 10.192.10.3 255.255.255.255
PE3(config-if)#no shut

Realizar pruebas de conectividad a nivel L3, mediante ping.

PE1#ping 10.10.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/56 ms

PE1#ping 10.10.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/51/52 ms

PE2#ping 10.10.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/60 ms

PE2#ping 10.10.1.6

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.6, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/56 ms

PE3#ping 10.10.1.9

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.9, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/60 ms

PE3#ping 10.10.1.5

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.1.5, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 40/47/56 ms

Paso 2.- Configurar OSPF en los routers.

Crea proceso (1) OSPFv2 en los router PE1, PE2 y PE3. Configurar el OSPF Router ID en cada uno de ellos (*PE1=10.192.10.1, PE2=10.192.10.2, PE3=10.192.10.3*). Habilitar redes directamente conectadas en el proceso OSPF utilizando **ip ospf *process-id* área *área-id***. En este caso se utilizara como ***router-id*** la Lo0 de admin.

Configurar router OSPFv2 en área 0 para los equipos PE

PE1(config)#router ospf 1
PE1(config-router)# router-id 10.192.10.1
PE1(config-router)# redistribute connected
PE1(config-router)# redistribute static subnets

PE2(config)#router ospf 1
PE2(config-router)# router-id 10.192.10.2
PE2(config-router)# redistribute connected
PE2(config-router)# redistribute static subnets
.
PE3(config)#router ospf 1
PE3(config-router)# router-id 10.192.10.3
PE3(config-router)# redistribute connected
PE3(config-router)# redistribute static subnets

Nota: se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro del proceso OSPF 1 para que este redistribuya las rutas estáticas y las conectadas directamente al equipo.

Se procederá a configurar las interfaces físicas y lógicas que participaran el protocolo de enrutamiento dinámico OSPFv2. (proceso 1 área 0)

PE1(config)#interface GigabitEthernet1/0
PE1(config-if)# ip ospf 1 area 0

PE1(config)#interface GigabitEthernet2/0
PE1(config-if)# ip ospf 1 area 0

PE1(config)#interface Loopback0
PE1(config-if)#ip ospf 1 area 0

PE2(config)#interface GigabitEthernet1/0
PE2(config-if)# ip ospf 1 area 0

PE2(config)#interface GigabitEthernet3/0
PE2(config-if)# ip ospf 1 area 0

PE2(config)#interface Loopback0
PE2(config-if)#ip ospf 1 area 0

PE3(config)#interface GigabitEthernet2/0
PE3(config-if)# ip ospf 1 area 0

PE3(config)#interface GigabitEthernet3/0
PE3(config-if)# ip ospf 1 area 0

PE3(config)#interface Loopback0
PE3(config-if)#ip ospf 1 area 0

Verificar que los routers tengan vecinos OSPFv2. Utilizando el **comando show ip ospf neighbors**.

PE1#sh ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*
10.192.10.3	*1*	*FULL/DR*	*00:00:37*	*10.10.1.10*	*GigabitEthernet2/0*
10.192.10.2	*1*	*FULL/DR*	*00:00:34*	*10.10.1.2*	*GigabitEthernet1/0*

PE2#sh ip ospf neighbor

Neighbor ID	*Pri*	*State*	*Dead Time*	*Address*	*Interface*

10.192.10.3 1 FULL/DR 00:00:36 10.10.1.6 GigabitEthernet3/0
10.192.10.1 1 FULL/BDR 00:00:37 10.10.1.1 GigabitEthernet1/0

PE3#sh ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
10.192.10.2 1 FULL/BDR 00:00:33 10.10.1.5 GigabitEthernet3/0
10.192.10.1 1 FULL/BDR 00:00:38 10.10.1.9 GigabitEthernet2/0

Verificar que el router R1 pueda ver todas las redes IPv4 en la tabla de enrutamiento OSPFv2 usando el comando **show ip route**.

PE1#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
*ia - IS-IS inter area, * - candidate default, U - per-user static route*
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C 10.10.1.0/30 is directly connected, GigabitEthernet1/0
L 10.10.1.1/32 is directly connected, GigabitEthernet1/0
O 10.10.1.4/30 [110/2] via 10.10.1.10, 01:47:34, GigabitEthernet2/0
[110/2] via 10.10.1.2, 01:47:34, GigabitEthernet1/0
C 10.10.1.8/30 is directly connected, GigabitEthernet2/0
L 10.10.1.9/32 is directly connected, GigabitEthernet2/0

C 10.192.10.1/32 is directly connected, Loopback0

O 10.192.10.2/32 [110/2] via 10.10.1.2, 01:47:34, GigabitEthernet1/0

10.192.10.3/32 [110/2] via 10.10.1.10, 01:47:34, GigabitEthernet2/

Paso 3.- Habilitar el protocolo MPLS LDP en los Router PE.

Se procederá a habilitar MPLS en los equipos PE1, PE2 y PE3. Antes de comenzar con dichas configuraciones se debe de aplicar el comando ***ip cef***. Luego se deberá activar el protocolo LDP con el comando ***mpls label protocol ldp*** dentro del modo de configuración, seguido del comando ***mpls ldp router-id Loopback0*** en el cual se le indica al router que recibirá actualizaciones por medio de la Lo0. Esto se realiza para evitar que el router tenga conflictos por elección de IP, y que pueda quedar desactualizado por esta razón.

PE1(config)#ip cef
PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id Loopback0

PE2(config)#ip cef
PE2(config)#mpls label protocol ldp
PE2(config)#mpls ldp router-id Loopback0

PE3(config)#ip cef
PE3(config)#mpls label protocol ldp
PE3(config)#mpls ldp router-id Loopback0

Luego se debe definir y configurar las interfaces que van a participar dentro del protocolo MPLS, con el siguiente comando ***mpls ip*** dentro de la interfaz en cuestión. Esto habilitara el protocolo y permitirá agregar un encabezado a la trama IP que servirá como etiqueta. Con la facilidad que se permita intercambiar paquetes entres

los equipos PE (CORE) e identificar el destino de cada paquete sin tener que analizar toda la trama. Lo que evita que el equipo sature su CPU.

PE1(config)#interface GigabitEthernet1/0
PE1(config-if)# mpls ip

PE1(config)#interface GigabitEthernet2/0
PE1(config-if)# mpls ip

PE2(config)#interface GigabitEthernet1/0
PE2(config-if)# mpls ip

PE2(config)#interface GigabitEthernet3/0
PE2(config-if)# mpls ip

PE3(config)#interface GigabitEthernet2/0
PE3(config-if)# mpls ip

PE3(config)#interface GigabitEthernet3/0
PE3(config-if)# mpls ip

Deberá agregarse dentro el proceso OSPF 1 el comando ***mpls ldp sync*** para que MPLS tenga sincronía a través del protocolo de enrutamiento dinámico. Y el comando ***mpls ldp autoconfig*** lo que hace referencia que tendrá una configuración automática con sus demás adyacencias.

PE1(config)#router ospf 1
PE1(config-router)#mpls ldp sync
PE1(config-router)# mpls ldp autoconfig

PE2(config)#router ospf 1

PE2(config-router)#mpls ldp sync

PE2(config-router)#mpls ldp autoconfig

PE3(config)#router ospf 1

PE3(config-router)#mpls ldp sync

PE3(config-router)#mpls ldp autoconfig

Procederemos a verificar las vecindades de MPLS en el equipo PE1

PE1#sh mpls ldp neighbor

Peer LDP Ident: 10.192.10.3:0; Local LDP Ident 10.192.10.1:0

TCP connection: 10.192.10.3.39975 - 10.192.10.1.646

State: Oper; Msgs sent/rcvd: 208/202; Downstream

Up time: 02:54:09

LDP discovery sources:

GigabitEthernet2/0, Src IP addr: 10.10.1.10

Addresses bound to peer LDP Ident:

10.10.1.10 10.192.10.3 10.10.1.6

Peer LDP Ident: 10.192.10.2:0; Local LDP Ident 10.192.10.1:0

TCP connection: 10.192.10.2.52377 - 10.192.10.1.646

State: Oper; Msgs sent/rcvd: 207/208; Downstream

Up time: 02:54:08

LDP discovery sources:

GigabitEthernet1/0, Src IP addr: 10.10.1.2

Addresses bound to peer LDP Ident:

10.10.1.2 10.192.10.2 10.10.1.5

Paso 4. -Se habilitara protocolo de Gateway Exterior BGP.

Dentro de los equipos PE se habilitara el proceso BGP con el AS de 1622. Utilizando el comando ***router bgp*** dentro del modo de configuración. Seguido del comando ***bgp***

log-neighbor-changes el que permite que el equipo reciba actualizaciones de base de datos de rutas aprendidas por sus vecinos. Sus peer de vecinos serán configurados mediante el comando **neighbor x.x.x.x remote-as xxxx** y recibirán actualizaciones de cambio por la interfaz **lo0**. Utilizando el comando **neighbor x.x.x.x update-source lo0**.

Luego se debe ingresar al modo de configuración **address-family ipv4**, habilita el intercambio de información con un peer BGP, posteriormente se define las redes vecinas con sus máscaras con el comando **network *x.x.x.x*** (Red) **mask *x.x.x.x*** (Mascara). Despues se procederá a definir a los peers vecinos en modo activo usando el comando **neighbor *x.x.x.x*** (Lo0 vecinos) **active.** Utilice **exit-address-family** para salir de ese modo de configuración.

Habilitar en los routers PE en el modo de configuración de BGP el comando **address-family vpnv4**, el cual habilita secciones de enrutamiento para prefijos de direcciones VPNv4. Se declara nuevamente los peers vecinos en modo activo y luego de cada peer vecino se utiliza el comando **neighbor *x.x.x.x*** (Lo0 vecinos) **send-community extended**, el cual especifica las comunidades que deben ser enviadas a un peer BGP vecino.

PE1(config)#router bgp 1622
PE1(config-router)# bgp log-neighbor-changes
PE1(config-router)# neighbor 10.192.10.2 remote-as 1622
PE1(config-router)# neighbor 10.192.10.2 update-source Loopback0
PE1(config-router)# neighbor 10.192.10.3 remote-as 1622
PE1(config-router)# neighbor 10.192.10.3 update-source Loopback0

PE1(config-router)# address-family ipv4
PE1(config-router-af)# network 10.10.1.0 mask 255.255.255.252
PE1(config-router-af)# network 10.10.1.8 mask 255.255.255.252
PE1(config-router-af)# redistribute connected

PE1(config-router-af)# redistribute static

PE1(config-router-af)# neighbor 10.192.10.2 activate

PE1(config-router-af)# neighbor 10.192.10.3 activate

PE1(config-router-af)# exit-address-family

PE1(config-router)# address-family vpnv4

PE1(config-router-af)# neighbor 10.192.10.2 activate

PE1(config-router-af)# neighbor 10.192.10.2 send-community extended

PE1(config-router-af)# neighbor 10.192.10.3 activate

PE1(config-router-af)# neighbor 10.192.10.3 send-community extended

PE1(config-router-af)# exit-address-family

PE2(config)#router bgp 1622

PE2(config-router)# bgp log-neighbor-changes

PE2(config-router)# neighbor 10.192.10.1 remote-as 1622

PE2(config-router)# neighbor 10.192.10.1 update-source Loopback0

PE2(config-router)# neighbor 10.192.10.3 remote-as 1622

PE2(config-router)# neighbor 10.192.10.3 update-source Loopback0

PE2(config-router)# address-family ipv4

PE2(config-router-af)# network 10.10.1.0 mask 255.255.255.252

PE2(config-router-af)# network 10.10.1.4 mask 255.255.255.252

PE2(config-router-af)# redistribute connected

PE2(config-router-af)# redistribute static

PE2(config-router-af)# neighbor 10.192.10.1 activate

PE2(config-router-af)# neighbor 10.192.10.3 activate

PE2(config-router-af)# exit-address-family

PE2(config-router)# address-family vpnv4

PE2(config-router-af)# neighbor 10.192.10.1 activate

PE2(config-router-af)# neighbor 10.192.10.1 send-community extended

PE2(config-router-af)# neighbor 10.192.10.3 activate
PE2(config-router-af)# neighbor 10.192.10.3 send-community extended
PE2(config-router-af)# exit-address-family

PE3(config)#router bgp 1622
PE3(config-router)# bgp log-neighbor-changes
PE3(config-router)# neighbor 10.192.10.1 remote-as 1622
PE3(config-router)# neighbor 10.192.10.1 update-source Loopback0
PE3(config-router)# neighbor 10.192.10.2 remote-as 1622
PE3(config-router)# neighbor 10.192.10.2 update-source Loopback0

PE3(config-router)# address-family ipv4
PE3(config-router-af)# network 10.10.1.4 mask 255.255.255.252
PE3(config-router-af)# network 10.10.1.8 mask 255.255.255.252
PE3(config-router-af)# redistribute connected
PE3(config-router-af)# redistribute static
PE3(config-router-af)# neighbor 10.192.10.1 activate
PE3(config-router-af)# neighbor 10.192.10.2 activate
PE3(config-router-af)# exit-address-family

PE3(config-router)# address-family vpnv4
PE3(config-router-af)# neighbor 10.192.10.1 activate
PE3(config-router-af)# neighbor 10.192.10.1 send-community extended
PE3(config-router-af)# neighbor 10.192.10.2 activate
PE3(config-router-af)# neighbor 10.192.10.2 send-community extended
PE3(config-router-af)# exit-address-family

Nota: se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro del modo de configuracion family-addess para que este redistribuya las rutas estáticas y las conectadas directamente al equipo

Una vez configurado los peer vecinos para intercambio de rutas a nivel BGP. Se deberá confirmar las tablas de IP BGP en cada PE de la topología. Para identificar las vecindades, el sistema autónomo al que pertenecen, el tipo de tabla y la versión que está utilizando. Para esto se usarán los comandos **show ip bgp summary, show ip bgp**

PE1#sh ip bgp summary

BGP router identifier 10.192.10.1, local AS number 1622
BGP table version is 7, main routing table version 7
6 network entries using 864 bytes of memory
9 path entries using 720 bytes of memory
4/4 BGP path/bestpath attribute entries using 544 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2152 total bytes of memory
BGP activity 12/0 prefixes, 15/0 paths, scan interval 60 secs

Neighbor	*V*	*AS*	*MsgRcvd*	*MsgSent*	*TblVer*	*InQ*	*OutQ*	*Up/Down*	*State/PfxRcd*
10.192.10.2	*4*	*1622*	*15*	*16*	*7*	*0*	*0*	*00:08:48*	*3*
10.192.10.3	*4*	*1622*	*16*	*16*	*7*	*0*	*0*	*00:09:00*	*3*

PE2#sh ip bgp summary

BGP router identifier 10.192.10.2, local AS number 1622
BGP table version is 8, main routing table version 8
6 network entries using 864 bytes of memory
9 path entries using 720 bytes of memory
4/4 BGP path/bestpath attribute entries using 544 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2152 total bytes of memory
BGP activity 12/0 prefixes, 15/0 paths, scan interval 60 secs

Neighbor	*V*	*AS*	*MsgRcvd*	*MsgSent*	*TblVer*	*InQ*	*OutQ*	*Up/Down*	*State/PfxRcd*
10.192.10.1	*4*	*1622*	*16*	*15*	*8*	*0*	*0*	*00:08:03*	*3*
10.192.10.3	*4*	*1622*	*16*	*15*	*8*	*0*	*0*	*00:08:10*	*3*

PE3#sh ip bgp summary

BGP router identifier 10.192.10.3, local AS number 1622

BGP table version is 8, main routing table version 8

6 network entries using 864 bytes of memory

9 path entries using 720 bytes of memory

4/4 BGP path/bestpath attribute entries using 544 bytes of memory

1 BGP extended community entries using 24 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

BGP using 2152 total bytes of memory

BGP activity 12/0 prefixes, 15/0 paths, scan interval 60 secs

Neighbor	*V*	*AS*	*MsgRcvd*	*MsgSent*	*TblVer*	*InQ*	*OutQ*	*Up/Down*	*State/PfxRcd*
10.192.10.1	*4*	*1622*	*17*	*17*	*8*	*0*	*0*	*00:10:04*	*3*
10.192.10.2	*4*	*1622*	*16*	*17*	*8*	*0*	*0*	*00:09:59*	*3*

Seguido de esto se deberá revisar las tablas de rutas bgp para cada PE

PE1# sh ip bgp

BGP table version is 7, local router ID is 10.192.10.1

*Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,*

r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,

x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

Network	*Next Hop*	*Metric*	*LocPrf*	*Weight*	*Path*
** i 10.10.1.0/30*	*10.192.10.2*	*0*	*100*	*0*	*i*

**> 0.0.0.0 0 32768 i*
r>i 10.10.1.4/30 10.192.10.2 0 100 0 i
r i 10.192.10.3 0 100 0 i
** i 10.10.1.8/30 10.192.10.3 0 100 0 i*
**> 0.0.0.0 0 32768 i*
**> 10.192.10.1/32 0.0.0.0 0 32768 ?*
r>i 10.192.10.2/32 10.192.10.2 0 100 0 ?
r>i 10.192.10.3/32 10.192.10.3 0 100 0 ?

PE2# show ip bgp

BGP table version is 8, local router ID is 10.192.10.2
*Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,*
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
** i 10.10.1.0/30 10.192.10.1 0 100 0 i*
**> 0.0.0.0 0 32768 i*
** i 10.10.1.4/30 10.192.10.3 0 100 0 i*
**> 0.0.0.0 0 32768 i*
r>i 10.10.1.8/30 10.192.10.1 0 100 0 i
r i 10.192.10.3 0 100 0 i
r>i 10.192.10.1/32 10.192.10.1 0 100 0 ?
**> 10.192.10.2/32 0.0.0.0 0 32768 ?*
r>i 10.192.10.3/32 10.192.10.3 0 100 0 ?

PE3#sh ip bgp

BGP table version is 8, local router ID is 10.192.10.3
*Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,*
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

```
    Network          Next Hop            Metric LocPrf Weight Path
r>i 10.10.1.0/30     10.192.10.1              0    100      0 i
r i                  10.192.10.2              0    100      0 i
* i 10.10.1.4/30     10.192.10.2              0    100      0 i
*>                   0.0.0.0                  0         32768 i
* i 10.10.1.8/30     10.192.10.1              0    100      0 i
*>                   0.0.0.0                  0         32768 i
r>i 10.192.10.1/32   10.192.10.1              0    100      0 ?
r>i 10.192.10.2/32   10.192.10.2              0    100      0 ?
*>  10.192.10.3/32   0.0.0.0                  0         32768 ?
```

Paso 5. –Configuración de MPLS-VPN.

Una vez configurado los enrutamientos dinámicos en cada PE, se procederá con las configuraciones de MPLS L3 VPN. Donde se configurará las VRF o virtual route forward con el comando **vrf definition** *NombredelaVRFdelCliente* (EMPRESA_1) y se definirá el route-distinguisher con el comando **rd** (16:22). Utilizando el comando **address-family** indicaremos que este cliente intercambiara rutas en IPv4. Usar los comandos **route-target export** y **route-targe import** para indicar al address-family por cual RD se importará y exportaran las direcciones IPv4. Utilice **exit-address-family** para salir de ese modo de configuración. Las VRF tienen la ventaja de crear múltiples redes virtuales independientes dentro de un mismo equipo. Lo que permite alojar y transportar tráfico de distintos clientes de manera segura sobre una arquitectura ISP sin que estos se conozcan o intercambien prefijos entre sí, debido a que estos se comportan como enlaces punto a punto en el caso que no sea requerido importar y exportar prefijos hacia otras VRF.

```
PE1(config)#vrf definition EMPRESA_1
PE1(config-vrf)# rd 16:22
PE1(config-vrf)# address-family ipv4
```

PE1(config-vrf-af)# route-target export 16:22
PE1(config-vrf-af)# route-target import 16:22
PE1(config-vrf-af)# exit-address-family

PE2(config)#vrf definition EMPRESA_1
PE2(config-vrf)# rd 16:22
PE2(config-vrf)# address-family ipv4
PE2(config-vrf-af)# route-target export 16:22
PE2(config-vrf-af)# route-target import 16:22
PE2(config-vrf-af)# exit-address-family

PE3(config)#vrf definition EMPRESA_1
PE3(config-vrf)# rd 16:22
PE3(config-vrf)# address-family ipv4
PE3(config-vrf-af)# route-target export 16:22
PE3(config-vrf-af)# route-target import 16:22
PE3(config-vrf-af)# exit-address-family

Nota: El sistema autónomo (AS) de BGP es 1622 y el RD (route-distinguisher) del cliente es 16:22, estos no tienen relación y pueden ser distintos números, pero por casualidad son los mismo en esta topología. El RD dentro de la VRF es el ID único de cada cliente para identificarlos en la red MPLS.

Después de que se definió el nombre de la VRF y su RD (route-distinguisher). Se debe configurar las rutas que se van a importar y exportar IPv4 dentro del proceso BGP 1622. Para esto se utilizan los comandos **address-family** *familiaIP* **vrf** *NombredelaVRFdelCliente*. Para luego ser aprendidas por los PE vecinos. Se aplican los comandos ***redistribute connected*** y ***redistribute static subnets*** dentro de la address-family asociada vrf del cliente en proceso BGP, para que este redistribuya las rutas estáticas y las conectadas directamente al equipo

PE1(config)#router bgp 1622
PE1(config-router)# address-family ipv4 vrf EMPRESA_1
PE1(config-router-af)# redistribute connected
PE1(config-router-af)# redistribute static
PE1(config-router-af)# exit-address-family

PE2(config)#router bgp 1622
PE2(config-router)#address-family ipv4 vrf EMPRESA_1
PE2(config-router-af)# redistribute connected
PE2(config-router-af)# redistribute static
PE2(config-router-af)# exit-address-family

PE3(config)#router bgp 1622
PE3(config-router)# address-family ipv4 vrf EMPRESA_1
PE3(config-router-af)# redistribute connected
PE3(config-router-af)# redistribute static
PE3(config-router-af)# exit-address-family

Luego de distribuir la VRF para el cliente EMPRESA_1 dentro del BGP 1622. Donde se tomará en cuenta las rutas estáticas y directamente conectadas para crear conectividad entre las 2 sucursales y la casa matriz haciendo uso de la infraestructura de un proveedor. Se deberá definir interfaces WAN y direccionamiento a utilizar entre el PE y el CPE, según tabla de direccionamiento y topología. Dentro de las interfaces físicas se debe configurar el **comando vrf forwarding** *NombredelaVRFdelCliente, con esto se asocia la interfaz física a la vrf del cliente.*

PE1(config)#interface GigabitEthernet3/0
PE1(config-if)# description EMPRESA_1
PE1(config-if)# vrf forwarding EMPRESA_1
PE1(config-if)# ip address 10.15.10.1 255.255.255.252

PE1(config-if)# negotiation auto

PE1(config-if)# no shut

PE2(config)#interface GigabitEthernet2/0

PE2(config-if)# description SUCURSAL1

PE2(config-if)# vrf forwarding EMPRESA_1

PE2(config-if)# ip address 10.15.8.1 255.255.255.252

PE2(config-if)# negotiation auto

PE2(config-if)# no shut

PE3(config)#interface GigabitEthernet1/0

PE3(config-if)# description SUCURSAL2

PE3(config-if)# vrf forwarding EMPRESA_1

PE3(config-if)# ip address 10.15.9.1 255.255.255.252

PE3(config-if)# negotiation auto

PE3(config-if)# no shut

Se deberá crear una ruta estática asociada a la IP WAN del CPE del cliente para lograr enrutar el segmento LAN interno del cliente. Mediante el comando **ip route vrf** *NombredelaVRFdelCliente* ***x.x.x.x*** *(LAN)* ***x.x.x.x*** *(Mask)* ***x.x.x.x*** *(WAN CPE)* **name** *Descripcion,* dentro del modo de configuración de los routers core MPLS. Use tabla de direccionamiento y topología.

PE1(config)#ip route vrf EMPRESA_1 192.168.1.0 255.255.255.0 10.15.10.2 name EMPRESA_1

PE2(config)#ip route vrf EMPRESA_1 192.168.2.0 255.255.255.0 10.15.8.2 name SUCURSAL1

PE3(config)#ip route vrf EMPRESA_1 192.168.3.0 255.255.255.0 10.15.9.2 name SUCURSAL2

Se debe configurar las interfaces físicas y virtuales en los CPE del cliente, utilice tabla de direccionamiento y topología. Luego configure una ruta estatica por defecto en cada CPE con el comando **ip route 0.0.0.0 0.0.0.0 *x.x.x.x*** (Gateway).

EMPRESA_1(config)#interface Loopback0
EMPRESA_1(config-if)# description LAN_EMPRESA_1
EMPRESA_1(config-if)# ip address 192.168.1.1 255.255.255.0

EMPRESA_1(config)#interface GigabitEthernet1/0
EMPRESA_1(config-if)# description PE1
EMPRESA_1(config-if)# ip address 10.15.10.2 255.255.255.252
EMPRESA_1(config-if)# negotiation auto
EMPRESA_1(config-if)# no shut

EMPRESA_1(config)#ip route 0.0.0.0 0.0.0.0 10.15.10.1

SUCURSAL1(config)#interface Loopback0
SUCURSAL1(config-if)# description LAN_SUCURSAL1
SUCURSAL1(config-if)# ip address 192.168.2.1 255.255.255.0

SUCURSAL1(config)#interface GigabitEthernet1/0
SUCURSAL1(config-if)# description PE2
SUCURSAL1(config-if)# ip address 10.15.8.2 255.255.255.252
SUCURSAL1(config-if)# negotiation auto
SUCURSAL1(config-if)#no shut

SUCURSAL1(config)#ip route 0.0.0.0 0.0.0.0 10.15.8.1

SUCURSAL2(config)#interface Loopback0
SUCURSAL2(config-if)# description LAN
SUCURSAL2(config-if)# ip address 192.168.3.1 255.255.255.0

SUCURSAL2(config)#interface GigabitEthernet1/0
SUCURSAL2(config-if)# description WAN
SUCURSAL2(config-if)# ip address 10.15.9.2 255.255.255.252
SUCURSAL2(config-if)# negotiation auto
SUCURSAL2(config-if)# no shut

*SUCURSAL2(config)#ip route 0.0.0.0 0.0.0.0 10.15.9.*1

Una vez detallada la configuración de cada CPE del cliente. Observamos que no presenta mayor complejidad, más que una interfaz como enlace WAN hacia el proveedor, la creación de una lo0 para simular la LAN del cliente, por último, pero no menos importante una ruta por defecto apuntando hacia el siguiente salto, que permita que todas las redes sean alcanzadas desde cualquier sucursal o casa Matriz. Realizar pruebas de conectividad de entre los equipos de la casa matriz y sus sucursales.

Como practica final se deberá habilitar los comandos ***debug ip ospf adj, debug ip bgp events y debug mpls ldp bindings*** en el R1, seguido del apagado la interfaz GI2/0 en el R3. Se deberán observar los cambios de estados de los protocolos OSPF, BGP y MPLS.

PE3#sh int gigabitEthernet 2/0 description

Interface	Status	Protocol	Description
Gi2/0	admin down	down	PE1_GI2/0

PE1#

*Nov 30 15:29:11.939: LIB: prefix recurs walk start: 10.192.10.3/32, tableid: 0

*Nov 30 15:29:11.943: ldpx_fwdg: path change upcall event from fwdg

*Nov 30 15:29:11.943: LIB: get path labels for route 10.192.10.3/32

*Nov 30 15:29:11.943: LIB: get path labels: 10.192.10.3/32(0), nh ctx_id: 0, Gi1/0, nh 10.10.1.2

*Nov 30 15:29:11.947: LDP LLAF: 10.192.10.3 accepted, absence of filtering config

*Nov 30 15:29:11.947: tib: Assign 10.192.10.3/32 nh 10.10.1.2 real label

*Nov 30 15:29:11.951: LIB: add a route info for 10.192.10.3/32(0, 10.10.1.2, Gi1/0), remote label Unknown

*Nov 30 15:29:11.951: LIB: update remote label for route info 10.192.10.3/32(0, 10.10.1.2, Gi1/0) remote label 16 from 10.192.10.2:0

*Nov 30 15:29:11.955: lcon: announce labels for: 10.192.10.3/32; nh 10.10.1.2, Gi1/0, inlabel 22, outlabel 16 (from 10.192.10.2:0), fwdg upcall or intf event

*Nov 30 15:29:11.959: LIB: announced out label 16 for 10.192.10.3/32 (via 10.10.1.2)

*Nov 30 15:29:11.959: LIB: prefix w

PE1#alking remove route info for 10.192.10.3/32(0, 10.10.1.10, Gi2/0), remote label imp-null from 10.192.10.3:0

*Nov 30 15:29:11.963: LIB: Deleting route info: 10.192.10.3/32(0) nh:10.10.1.10

*Nov 30 15:29:11.975: LIB: prefix recurs walk start: 10.10.1.4/30, tableid: 0

*Nov 30 15:29:11.975: ldpx_fwdg: path change upcall event from fwdg

*Nov 30 15:29:11.979: LIB: get path labels for route 10.10.1.4/30

*Nov 30 15:29:11.979: LIB: get path labels: 10.10.1.4/30(0), nh ctx_id: 0, Gi1/0, nh 10.10.1.2

*Nov 30 15:29:11.983: LDP LLAF: 10.10.1.4 accepted, absence of filtering config

*Nov 30 15:29:11.983: tib: Assign 10.10.1.4/30 nh 10.10.1.2 real label

*Nov 30 15:29:11.987: LIB: found route info for 10.10.1.4/30(0, 10.10.1.2, Gi1/0), remote label imp-null from 10.192.10.2:0

*Nov 30 15:29:11.987: lcon: announce labels for: 10.10.1.4/30; nh 10.10.1.2, Gi1/0, inlabel 21, outlabel imp-null (from 10.192.10.2:0), fwdg upcall or intf event

*Nov 30 15:29:11.991: LIB: announced out label 3 for 10

PE1#.10.1.4/30 (via 10.10.1.2)

*Nov 30 15:29:11.995: LIB: prefix walking remove route info for 10.10.1.4/30(0, 10.10.1.10, Gi2/0), remote label imp-null from 10.192.10.3:0

*Nov 30 15:29:11.995: LIB: Deleting route info: 10.10.1.4/30(0) nh:10.10.1.10

*Nov 30 15:29:12.031: LIB: prefix deleted: 192.168.3.0/24(1); no context

*Nov 30 15:29:12.035: LIB: prefix deleted: 10.15.9.0/30(1); no context

*Nov 30 15:29:12.035: BGP: topo global:IPv4 Unicast:base Scanning routing tables

*Nov 30 15:29:12.039: BGP: topo global:VPNv4 Unicast:base Scanning routing tables

*Nov 30 15:29:12.043: BGP: topo EMPRESA_1:VPNv4 Unicast:base Scanning routing tables

*Nov 30 15:29:12.047: BGP: topo global:IPv4 Multicast:base Scanning routing tables

*Nov 30 15:29:12.047: BGP: topo global:MVPNv4 Unicast:base Scanning routing tables

*Nov 30 15:29:12.051: BGP: topo EMPRESA_1:MVPNv4 Unicast:base Scanning routing tables

PE1#

*Nov 30 15:29:14.979: OSPF-1 ADJ Gi2/0: Nbr 10.192.10.3: Clean-up dbase exchange

PE1#

*Nov 30 15:29:16.395: OSPF-1 ADJ Gi2/0: Rcv int status from LDP: 1 0 1 0

PE1#

*Nov 30 15:29:16.403: %LDP-5-NBRCHG: LDP Neighbor 10.192.10.3:0 (1) is DOWN (TCP connection closed by peer)

PE1#

*Nov 30 15:29:24.451: lcon: tibent(10.10.1.0/30): label 24 from 10.192.10.3:0 removed

*Nov 30 15:29:24.455: lcon: tibent(10.10.1.4/30): label imp-null from 10.192.10.3:0 removed

*Nov 30 15:29:24.459: lcon: tibent(10.10.1.8/30): label imp-null from 10.192.10.3:0 removed

*Nov 30 15:29:24.459: lcon: tibent(10.192.10.1/32): label 22 from 10.192.10.3:0 removed

*Nov 30 15:29:24.463: lcon: tibent(10.192.10.2/32): label 21 from 10.192.10.3:0 removed

*Nov 30 15:29:24.467: lcon: tibent(10.192.10.3/32): label imp-null from 10.192.10.3:0 removed

*Nov 30 15:29:24.471: lcon: (default) Deassign peer id; 10.192.10.3:0: id 0

PE1#

*Nov 30 15:29:39.959: OSPF-1 ADJ Gi2/0: 10.192.10.3 address 10.10.1.10 is dead

*Nov 30 15:29:39.959: OSPF-1 ADJ Gi2/0: 10.192.10.3 address 10.10.1.10 is dead, state DOWN

*Nov 30 15:29:39.963: %OSPF-5-ADJCHG: Process 1, Nbr 10.192.10.3 on GigabitEthernet2/0 from FULL to DOWN, Neighbor Down: Dead timer expired

PE1#

*Nov 30 15:29:39.963: OSPF-1 ADJ Gi2/0: Neighbor change event

*Nov 30 15:29:39.967: OSPF-1 ADJ Gi2/0: DR/BDR election

*Nov 30 15:29:39.967: OSPF-1 ADJ Gi2/0: Elect BDR 0.0.0.0

*Nov 30 15:29:39.971: OSPF-1 ADJ Gi2/0: Elect DR 10.192.10.1

*Nov 30 15:29:39.971: OSPF-1 ADJ Gi2/0: DR: 10.192.10.1 (Id) BDR: none

PE1#

*Nov 30 15:30:12.763: BGP: topo global:IPv4 Unicast:base Scanning routing tables

*Nov 30 15:30:12.767: BGP: topo global:VPNv4 Unicast:base Scanning routing tables

*Nov 30 15:30:12.767: BGP: topo EMPRESA_1:VPNv4 Unicast:base Scanning routing tables

*Nov 30 15:30:12.771: BGP: topo global:IPv4 Multicast:base Scanning routing tables

*Nov 30 15:30:12.775: BGP: topo global:MVPNv4 Unicast:base Scanning routing tables

*Nov 30 15:30:12.775: BGP: topo EMPRESA_1:MVPNv4 Unicast:base Scanning routing tables

CUESTIONARIO

Si se pregunta por la red 192.168.3.1 configurada como puerta de enlace para la LAN de la sucursal SUCURSAL2 en el PE1 sobre la vrf EMPRESA_1 ¿Qué resultado obtenemos como respuesta?

R/ Que esta se aprende via bgp 1622, por el equipo con la IP de gestión 10.192.10.3, la cual pertenece al PE3. Donde se deberá realizar la misma pregunta, para posterior encontrar la WAN asignada al servicio y su última milla a como representa con los siguientes comandos.

PE1#sh ip route vrf EMPRESA_1 192.168.3.1

Routing Table: EMPRESA_1

Routing entry for 192.168.3.0/24

Known via "bgp 1622", distance 200, metric 0, type internal

Last update from 10.192.10.3 00:59:42 ago

Routing Descriptor Blocks:

** 10.192.10.3 (default), from 10.192.10.3, 00:59:42 ago*

Route metric is 0, traffic share count is 1

AS Hops 0

MPLS label: 20

MPLS Flags: MPLS Required

PE3#sh ip route vrf EMPRESA_1 192.168.3.1

Routing Table: EMPRESA_1

Routing entry for 192.168.3.0/24

Known via "static", distance 1, metric 0

Redistributing via bgp 1622

Advertised by bgp 1622

Routing Descriptor Blocks:

** 10.15.9.2*

Route metric is 0, traffic share count is 1

PE3#sh ip route vrf EMPRESA_1 10.15.9.2

Routing Table: EMPRESA_1

Routing entry for 10.15.9.0/30

Known via "connected", distance 0, metric 0 (connected, via interface)

Redistributing via bgp 1622

Advertised by bgp 1622

Routing Descriptor Blocks:

** directly connected, via GigabitEthernet1/0*

Route metric is 0, traffic share count is 1

¿Debería de haber conexión vía ping entre las sucursales y la EMPRESA_1? ¿Por qué?

Si debería, porque cada PE tiene configurada una VRF llamada EMPRESA_1 la cual importa y exporta prefijos mediante BGP a nivel de arquitectura del ISP. Lo que permite crear una conexión punto a punto entre las LAN asociadas al cliente. Se detalla lo siguiente.

EMPRESA_1#ping 192.168.2.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/75/88 ms

EMPRESA_1#ping 192.168.3.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/102/116 ms

¿Cuantas rutas OSPFv2 intra-area hay en el router PE1 dentro su tabla de enrutamiento IPV4?

R/ Para el Router PE1 se tiene 3 rutas intra-area, las cuales son rutas que se originan y aprenden en la misma área OSPF.

¿Por qué el Router PE3 se encuentra en estado FULL/BDR?

R/ Porque es el router designado de reserva

¿Qué direccionamiento en el PE2 es utilizado para establecer adyacencia de vecindad con el PE1?

R/ Utiliza la dirección IP 10.10.1.2

¿Qué direccionamiento en el PE3 es utilizado para establecer adyacencia de vecindad con el PE1?

R/ Utiliza la dirección IP 10.10.1.9

¿Qué comportamiento se observa en el PE1 para los protocolos OSPF, BGP Y MPLS cuando se realiza el apagado del puerto GI2/0? Explique cada uno.

R/ Como se observa en la captura en tiempo de real del router R1. Al caer el link entre R1 y R3. Los protocolos OSPF y MPLS están en estado DOWN en ese enlace, mientras el protocolo BGP se encuentra activo por que el PE1 está aprendiendo al peer PE3 a través de un enlace redundante.

TRABAJO PREVIO:

Realice todas las configuraciones solicitadas en la guía y simúlelos en el laboratorio, realice las correcciones si es necesario y conteste el cuestionario. Muestre a su profesor la topología funcionando correctamente.