INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS" ZACATENCO

"PROTOCOLO DE ENRUTAMIENTO DINÁMICO BGP EN REDES DE ALTA DISPONIBILIDAD"

SEMINARIO

PARA OBTENER EL TITULO DE:

INGENIERO EN COMUNICACIONES Y ELECTRONICA

PRESENTA:

ARMANDO MUÑOZ MARTÍNEZ

ASESORES:

ING. ARTURO A. HIT ESPINOSA
ING. GUILLERMO MANUEL ESCÁRCEGA CARRERA

CDMX, Mayo 2019

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

REPORTE TÉCNICO

PARA OBTENER EL TÍTULO DE: **INGENIERO EN COMUNICACIONES Y ELECTRÓNICA**
PARA LA OPCIÓN DE TITULACIÓN SEMINARIO REG. DES/ESIMEZAC/06.2017.06.2019/451/31/19
DEBERA(N) DE DESARROLLAR **C. ARMANDO MUÑOZ MARTÍNEZ**

"PROTOCOLO DE ENRUTAMIENTO DINÁMICO BGP EN REDES DE ALTA DISPONIBILIDAD"

OBJETIVO: IMPLEMENTAR EL PROTOCOLO DE ENRUTAMIENTO DINÁMICO BGP COMO PROTOCOLO GATEWAY EXTERIOR ENTRE REDES EMPRESARIALES IPv4 CON ALTA DISPONIBILIDAD Y EL ISP QUE BRINDA EL SERVICIO DE CONECTIVIDAD.

CIUDAD DE MÉXICO, A 11 DE MAYO DE 2019

ASESORES

ING. ARTURO A. HIT ESPINOSA

ING. GUILLERMO M. ESCARCEGA CARRERA

ING. GABRIEL VEGA REYES
JEFE DEL DEPARTAMENTO DE INGENIERÍA
EN COMUNICACIONES Y ELECTRÓNICA

Autorización de uso de obra

Instituto Politécnico Nacional
Presente

Bajo protesta de decir verdad el que suscribe **Armando Muñoz Martínez**, manifiesto ser autor y titular de los derechos morales y patrimoniales de la obra titulada **"PROTOCOLO DE ENRUTAMIENTO DINÁMICO BGP EN REDES DE ALTA DISPONIBILIDAD"**, en adelante **"La Tesis"** y de la cual se adjunta copia en 2 CDs, por lo que por medio del presente y con fundamento en el artículo 27 fracción II, inciso b) de la Ley Federal de Derecho de Autor otorgo a el **Instituto Politécnico Nacional** en adelante **"El IPN"**, autorización no exclusiva para comunicar y exhibir públicamente total o parcialmente en medios digitales para que se ocupe como una guía de apoyo y estudio en futuros trabajos relacionados con el tema de **"La Tesis"** por un periodo de 1 año contando a partir de la fecha de la presente autorización, dicho periodo se renovara automáticamente en caso de no dar aviso expreso a **"El IPN"** de su terminación.

En virtud de lo anterior, **"El IPN"** deberá reconocer en todo momento mi calidad de autor de **"La Tesis"**.

Adicionalmente y en mi calidad de autor y titular de los derechos morales y patrimoniales de **"La Tesis"**, manifiesto que la misma es original y que la presente autorización no contraviene ninguna otorgada por el suscrito respecto de **"La Tesis"**, por lo que deslindo de toda responsabilidad a **"El IPN"** en caso de que el contenido de **"La Tesis"** o la autorización concedida afecte o viole derechos autorales, industriales, secretos industriales, convenios o contratos de confidencialidad o en general cualquier derecho de propiedad intelectual de terceros y asumo las consecuencias legales y económicas de cualquier demanda o reclamación que puedan derivarse del caso.

México, Ciudad de México, a 25 de junio de 2019

Atentamente

Armando Muñoz Martínez

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

OBJETIVO

Implementar el protocolo de enrutamiento dinámico BGP como protocolo de Gateway exterior entre redes empresariales IPv4 con alta disponibilidad y el ISP que brinda el servicio de conectividad.

JUSTIFICACIÓN

Debe existir un orden con la asignación de redes que se anuncian a internet y la manera en que se identificarán, lo que se ha implementado para este objetivo es mantener el registro del número de sistema autónomo ASN (Autonomous System Number) del ISP u organización a la que pertenece cada prefijo de red en todo internet, pero realizarlo se vuelve un problema con la mayoría de los protocolos de enrutamiento dinámico debido a que son desarrollados como protocolo de puerta de enlace interior IGP (Interior Gateway Protocol) y se requiere uno del tipo protocolo de puerta de enlace exterior EGP (Exterior Gateway Protocol).

El protocolo de puerta de enlace de frontera BGP (Border Gateway Protocol) resuelve este problema ya que funciona de ambas maneras como IGP en el modo iBGP (internal BGP) y como EGP en el modo eBGP (external BGP), siendo este último modo el que se implementará para anunciar redes públicas a internet manteniendo el registro de sistemas autónomos utilizados para su anuncio y conservando un orden en internet.

INTRODUCCIÓN

La asignación de direccionamiento IPv4 (Protocolo de Internet versión 4, por sus siglas en inglés Internet Protocol version 4) público es administrado por la Autoridad de Asignación de Números de Internet IANA (Internet Assigned Numbers Authority). IANA realiza esta asignación a través de los diferentes Registros Regionales de Internet RIR's (Regional Internet Registry) del mundo, los RIR pueden asignar direccionamiento público a sus Registros Nacionales de Internet NIR (National Internet Registry), a los diferentes Proveedores de Servicio de Internet ISP (Internet Service Provider) o Registros Locales de Internet LIR (local Internet registry), incluso un RIR puede asignar direccionamiento directamente a un usuario final. En el diagrama siguiente se muestra los flujos que se pueden seguir para la asignación de direccionamiento público.

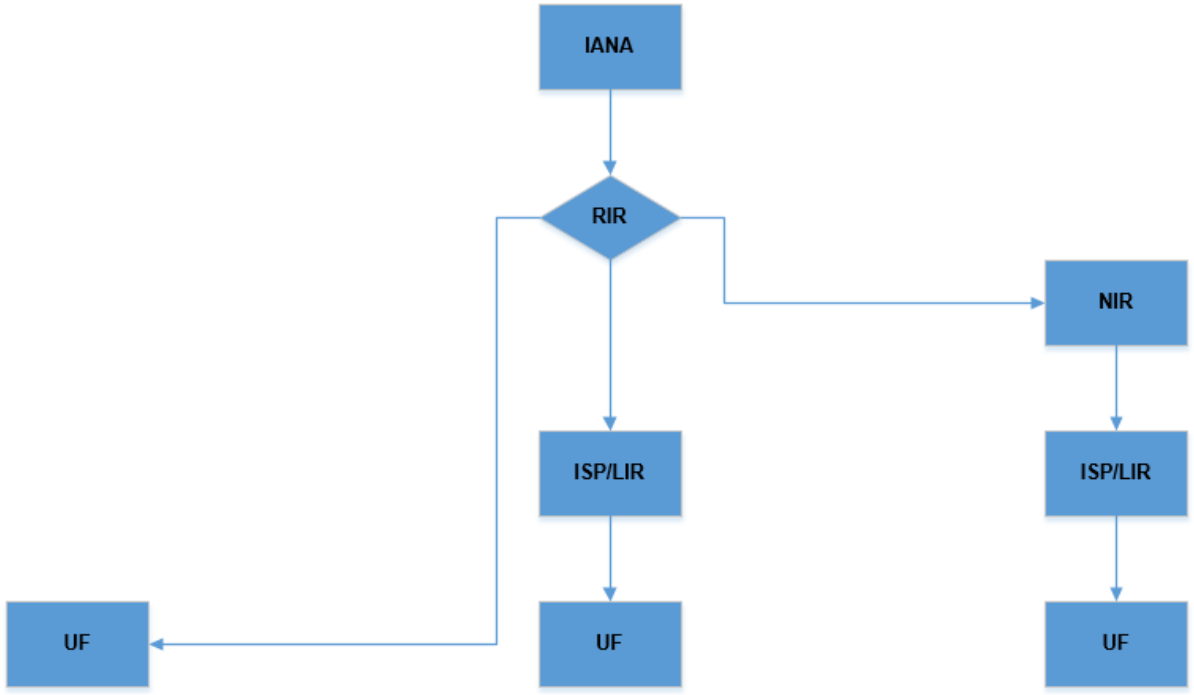

Figura 0-1. Flujos de asignación de direccionamiento público

Los diferentes RIR's existentes y la región del mundo que administran se muestran en la siguiente tabla.

RIR	Región
AFRINIC (African Network Information Centre)	África
APNIC (Asia-Pacific Network Information Centre)	Asia / Pacífico
ARIN (American Registry for Internet Numbers)	América del norte
LACNIC (Latin American and Caribbean Internet Address Registry)	Latino América / Caribe
RIPE NCC (Réseaux IP Européens Network Coordination Centre)	Europa, medio oriente y Asia central

Tabla 0.1. RIR's del mundo y región que administran

Solamente algunos RIR's tienen NIR's en algún país dentro de la región que administran LACNIC tiene NIRs en México (a través de la página www.iar.mx), Brasil (a través de la página www.registro.br).

A los diferentes ISP se les asigna un rango de direccionamiento IPv4 homologado exclusivo e irrepetible en internet, estos a su vez lo segmentan y lo asignan a los clientes que compren el servicio.

Los rangos de direccionamiento homologado deben ser anunciados a internet solamente por el ISP al que se le asignó, para llevar el control de estos anuncios se hace uso del número de sistema autónomo ASN (Autonomous System Number) que también es asignado por IANA y representa el número que se utiliza para identificar y diferenciar a un sistema autónomo AS (Autonomous System) de otro o dicho en otras palabras diferenciar una red privada de otra, de esta manera cualquier organización que compre prefijos de red públicos y no cuente con la infraestructura para anunciarlos a internet puede contratar a un ISP el anuncio. El ISP deberá anunciar además de las redes del cliente el ASN al que pertenecen manteniendo así una ruta de AS (AS Path) para alcanzar el prefijo.

En el capítulo uno se revisarán los tipos de redes existentes, los modelos de referencia que nos sirven para entender el proceso de comunicación de extremo a extremo, los tipos de redundancia que se pueden brindar dependiendo del nivel de

disponibilidad que se pretenda tener, por último, se hablará de las redes privadas y la manera de realizar anuncios a internet atravesando la red de un ISP.

En el capítulo dos se revisará el enrutamiento estático y varios protocolos de enrutamiento dinámico haciendo énfasis en el funcionamiento y características de BGP, así como la diferencia entre protocolos de Gateway interior y exterior.

El capítulo tres, tratara el tema de anuncios a internet para redes IPv4, explicando el funcionamiento de los atributos de BGP que pueden utilizarse en dependiendo el escenario de conexión.

En el capítulo cuatro se implementará una red simulada donde se pueda apreciar el comportamiento de BGP en enlaces redundantes y la manera como se anuncian a internet los prefijos IPv4 en el escenario donde el ISP es dueño de los prefijos de red y el cliente contrata un servicio redundado de internet. También se hablará del simulador GNS3 y el sistema operativo CISCO IOS mismos que se utilizarán para la implementación de la simulación.

1. TIPOS DE REDES DE DATOS, MODELOS DE REFERENCIA Y ACCESO A INTERNET

Las redes de datos son la interconexión de dispositivos también llamados nodos, a través de un medio con el objetivo de intercambiar información, en ellas los nodos comparten los recursos disponibles.

Una red de datos está conformada por:

- *Medios de transmisión*, estos pueden ser fibra óptica, cobre, micro onda etc.
- *Elementos* como switch, router, hub, servidores etc.
- *Identificadores locales como dirección MAC*.
- *Identificadores globales como dirección IP*.
- *Topologías físicas y lógicas* como son bus, anillo, estrella etc.

En el proceso de intercambio de información se establecen los roles emisor y receptor que se estarán alternando dependiendo del sentido en el que se realice la transmisión de datos. El dispositivo que envía datos tendrá el rol de emisor mientras el que reciba la información tendrá el de receptor. La transmisión de datos se llevará a cabo a través de los medios por los cuales se encuentren interconectados los nodos y es necesario que los mensajes de información se conviertan a bits es decir a señales digitales codificadas en binario, antes de enviarse a sus destinos.

La comunicación entre los elementos de la red es posible gracias al medio de transmisión, los medios se clasifican como guiado o no guiado dependiendo del tipo de conexión. En una red pueden estar presentes ambos tipos de medios gracias a los protocolos que permite el envío de información de manera independiente al medio.

Las conexiones guiadas al inicio eran realizadas con cable coaxial, actualmente es obsoleto y se ha sustituido por el cable de par trenzado y la fibra óptica, las conexiones no guiadas, se refieren a conexiones inalámbricas utilizando ondas electromagnéticas,

aplicadas a tecnologías como las implementadas en los estándares 802.11 de las redes inalámbricas de área local, Bluetooth, infrarrojo y microondas.

Los servicios que se solicitan en una red de datos son muy variados, se enlistan a continuación solo algunos.

- Comercio electrónico.
- Banca en línea.
- Trámites de gobierno
- Comunicaciones personales (e-mail, chat, voz, videoconferencia).
- E-learning.
- Entretenimiento.

El diseño de una red depende muchas variables, las más comunes y minimas que se deben considerar son: La cantidad de usuarios, tipo y número de elementos, tipo de servicios que se ofrecerán en ella, y el presupuesto, este diseño se realiza de acuerdo a las diferentes topologías de red existentes.

1.1.- Topologías de red

La topología es el arreglo físico o lógico usado para la interconexión de los dispositivos sobre un medio en una red. La forma de comunicación de los nodos de una red dependerá de la topología seleccionada. La elección de una topología adecuada para una red es de suma importancia debido a que de ella dependerá, la cantidad de nodos que se conectarán, la velocidad de la red, el tipo de acceso al medio, el costo etc. una mala elección de la topología reflejará una baja eficiencia en la red.

Una red debe tener una topología física y lógica, no necesariamente deben ser la misma. La topología física se refiere al diseño físico de la red incluyendo la instalación y localización de cables, dispositivos, etc. La topología lógica es referida a la manera

de transferir la información a su paso por los nodos de la red, puede ser considerada como estructura virtual de la red.

1.1.1.- Topología de bus

Topología donde los nodos están conectados mediante un cable común permitiendo que la comunicación sea directa, pero la ruptura de este cable hace que los hosts queden desconectados. En esta topología las señales generadas por un dispositivo son recibidas por tolos los integrantes de la red, este comportamiento hace que se presenten problemas de tráfico y colisiones.

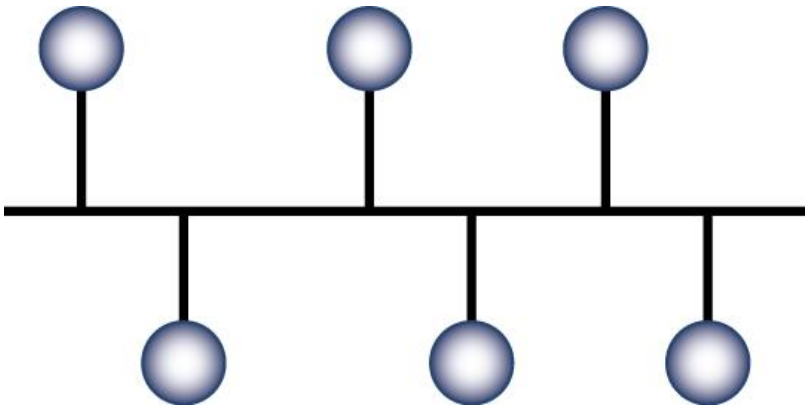

Figura 1-1: Topología de BUS

1.1.2.- Topología de Anillo

En esta topología los dispositivos se encuentran conectados solo a los dos nodos adyacentes mediante una única conexión de entrada y salida, Cada equipo tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.

Con la topología anillo, la comunicación se da mediante el paso de un token o testigo, para así evitar posibles colisiones que generen perdidas de información. Si algún dispositivo de la red falla, la comunicación en todo el anillo se pierde, además de que no es sencillo agregar un nuevo nodo y requiere de un diseño de conexión adecuado.

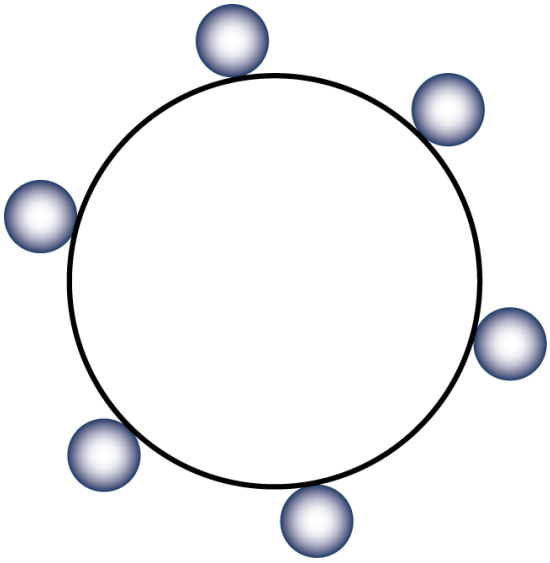

Figura 1-2: Topología de anillo

1.1.3.- Topología de anillo doble

La topología de anillo doble es igual a la de anillo, pero agrega un segundo anillo redundante. La incorporación de este segundo anillo brinda a la red mayor fiabilidad y flexibilidad donde cada dispositivo de la red se encuentra dentro de dos topologías de anillo independientes de las cuales solo se ocupa una a la vez. La mayor desventaja de esta topología es el de los altos costos comparada con la de anillo.

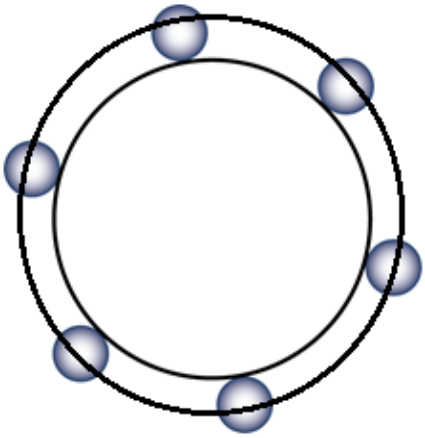

Figura 1-3: Topología de anillo doble

1.1.4.- Topología de Estrella

Es la topología donde los dispositivos se encuentran conectados de manera independiente a un centro de comunicaciones denominado nodo central pero no están conectados entre sí. El nodo central gestiona la redistribución de la información a los nodos de la red facilitando la supervisión y control de la información. Al conectar cada nodo de manera independiente, cualquier dispositivo que falle no afectará en nada la operación de la red, este esquema también facilita agregar nuevos nodos, los costos del cableado son elevados y al tener un nodo central se convierte en un único punto de falla, el aumento del número de dispositivos está limitada a la capacidad del nodo central y en caso de requerir mayor densidad que la soportada por este, los costos son muy elevados.

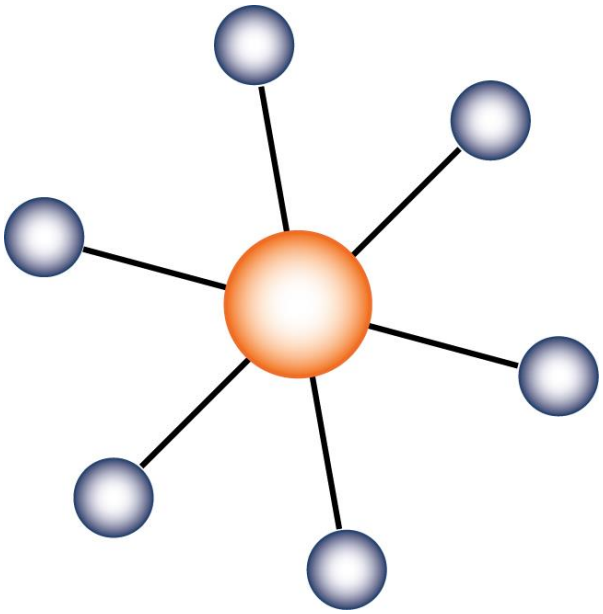

Figura 1-4: Topología de estrella

1.1.5.- Topología de Árbol

Esta topología pude verse como una serie de topologías de estrella y/o bus anidadas desde un nodo secundario a un nodo central, troncal o de backbone desde el que se conectan los demás nodos. En una red con topología de árbol, la falla de un nodo secundario interrumpe la comunicación solo de los nodos que se encuentren conectados a él, dejando comunicados los nodos que no tienen conexión con el nodo caído, pero si el nodo de backbone falla, toda la red dejará de funcionar. Esta topología permite limitar el acceso a algún servicio exclusivo para usuarios de alguna rama específica.

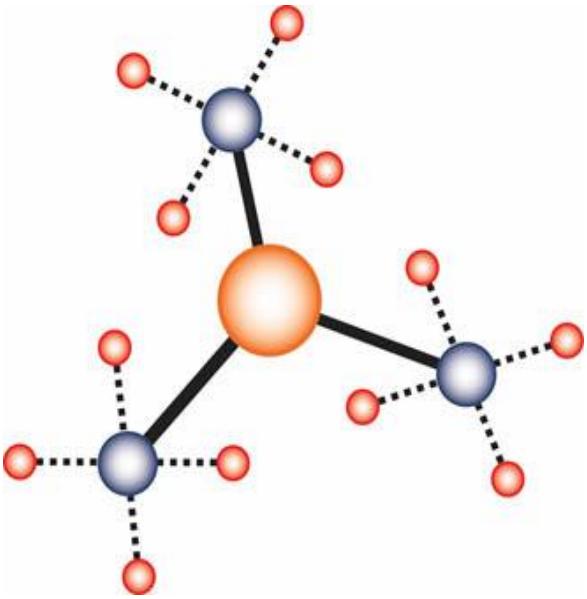

Figura 1-5: Topología de árbol

1.1.6.- Topología en Malla

En una red con topología malla todos los dispositivos se encuentran conectados entre sí permitiendo tener múltiples caminos para enviar información entre ellos. Como la malla está diseñada para que cada dispositivo tenga una conexión directa con cualquier otro nodo de la red, la interrupción de un enlace no afecta el servicio de los nodos debido a que existirán caminos alternos para el envío de información. Una red en malla es sumamente cara debido a la cantidad de cableado y conexiones que

demanda, considerando este último punto, aunque es la topología que garantiza el mejor desempeño de la red, su implementación no es muy común.

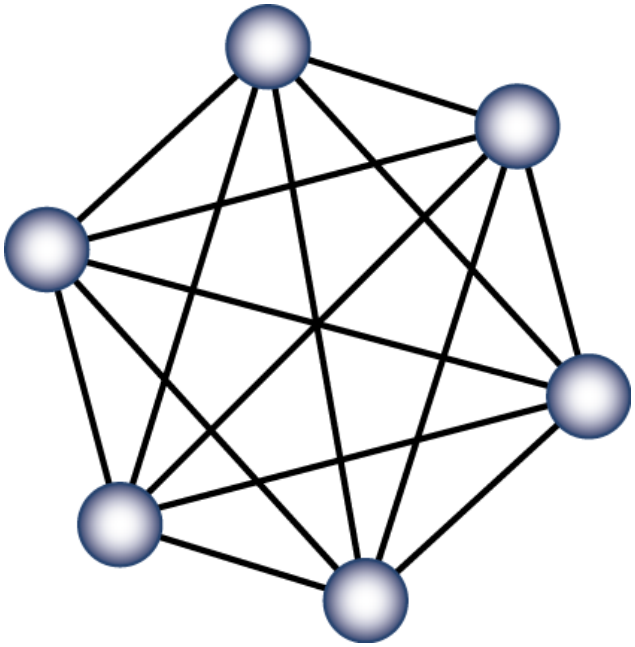

Figura 1-6: Topología de Malla

1.2.- Tipos de redes

Las redes de datos por lo general se clasifican en base a su alcance, pueden ser redes dentro de un departamento u oficina, redes que brinden servicio a un campus como lo son escuelas, hospitales, etc, o redes que geográficamente abarquen ciudades o el mundo entero. La clasificación de las redes basada en este aspecto refleja su volumen de datos. En este sentido, puede hablarse los siguientes tipos de redes:

- Red de área local LAN (Local Area Network).
- Red de área de campus CAN (Campus Area Network).
- Red de área metropolitana MAN (Metropolitan Area Network).
- Red de área amplia WAN (Wide Area Network).

1.2.1.- Rede de área local LAN

Son redes que abarcan sitios específicos de poco alcance, como una casa, una oficina, a lo sumo algunos pisos dentro de un edificio. Son usuales en negocios, escuelas, empresas, etc. El principal objetivo de este tipo de redes es brindar conectividad a todos los nodos de una red en un solo lugar geográfico.

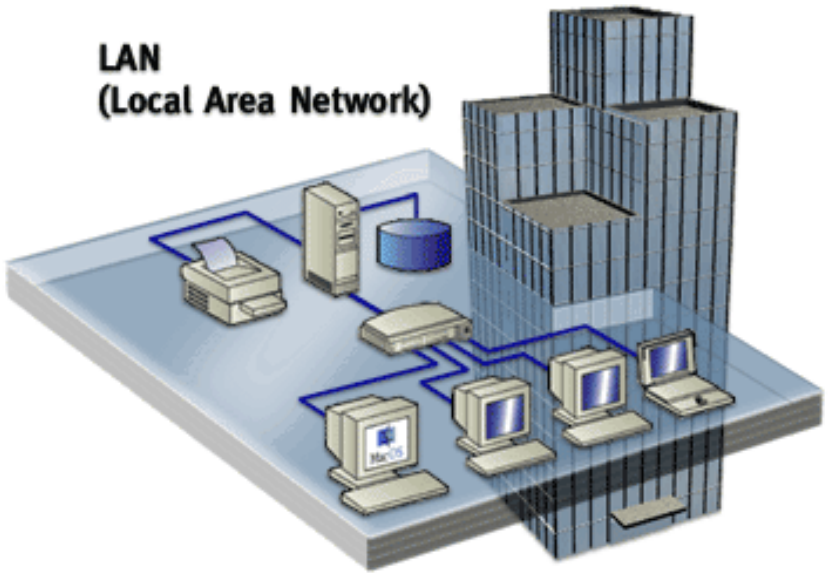

Figura 1-7: Red LAN

1.2.2.- Rede de área de campus CAN

En estas redes se implementan dispositivos de altas velocidades para unir redes LAN en un área geográfica limitada como un campus universitario, un hospital, una base militar, etc.

Figura 1-8: Red CAN

1.2.3.- Rede de área metropolitana MAN

Las redes MAN son implementadas con equipos de altas velocidades y soportando grandes capacidades de tráfico para brindar cobertura a sedes ubicadas en diferentes puntos de una ciudad, su alcance es mayor que el de una red de campus, pero menor al de una red de área amplia.

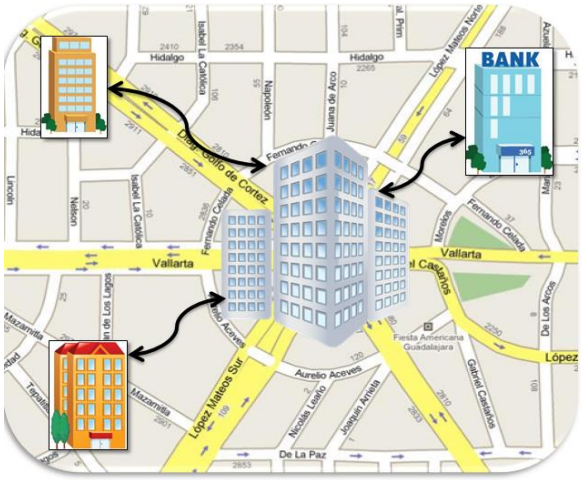

Figura 1-9: Red MAN

1.2.4.- Rede de área amplia WAN

Las redes WAN geográficamente se extienden sobre un área extensa empleando medios de comunicación poco habituales, como satélites, cables interoceánicos, fibra óptica, etc. Su alcance es mundial.

Figura 1-10: Red WAN

1.3.- Modelos de referencia

Son elementos fundamentales para la comprensión de los procesos involucrados en la transmisión de datos entre elementos de red. Los modelos están formados por capas o niveles creando pilas de protocolos o de normas. Cada nivel se comunica con la capa superior e inferior de la misma pila a través de interfaces de programación o API (Application Programming Interface), que representan protocolos específicos, y/o con capas análogas de otras pilas. Los niveles más bajos son los más próximos al equipo físico (hardware), mientras que las capas superiores, que manejan protocolos de más alto nivel, son las más cercanas al usuario.

1.3.1.- Modelo de referencia OSI

En la década de los ochenta se realizó una reunión entre los fabricantes informáticos más importantes de la época con el objetivo de unificar diferencias y recopilar la mayor información posible acerca de cómo poder integrar sus productos hasta el momento incompatibles entre sí. Gracias al acuerdo resultado de esta reunión, la Organización Internacional para la Normalización ISO (International Organization for Standarization) desarrolló el modelo de referencia llamado interconexión de sistemas abiertos OSI (Open System Interconnection) y lo publicó en 1984, el modelo sigue los parámetros comunes de hardware y software haciendo posible la integración multifabricante.

El modelo OSI divide la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin necesidad de depender de otras áreas. Un programador crea una aplicación determinada sin importarle cuáles serán los medios por los que se propagarán los datos, inversamente un técnico de comunicaciones proveerá comunicación sin importarle que datos transporta.

En su conjunto, el modelo OSI se compone de 7 capas bien definidas que son: Aplicación, presentación, sesión, transporte, red, enlace de datos y física. Cada una de estas capas presta servicio a la capa inmediatamente superior, la capa de aplicación al ser la última capa, su servicio está relacionado con el usuario. Cada una de estas siete capas del host origen se comunican con su similar en el host destino. Las cuatro capas inferiores se denominan capas de medios mientras que las 3 superioras, capas de host o de aplicación.

#	Nombre
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Tabla 1.1: Capas del modelo OSI

Las principales características del modelo de referencia OSI se pueden resumir en los siguientes puntos:

- Divide las operaciones complejas de la red en capas específicas más fácilmente administrables.
- Es la referencia para crear e implementar estándares de red, dispositivos y esquemas de interconexiones de red.
- Separa la compleja operación de una red en elementos más simples.
- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares ocupándose cada uno de la parte específica que les corresponde.
- Proporciona la posibilidad de definir interfaces estándar para compatibilidad plug-and-play e integración multifabricante.
- Permite elaborar especificaciones que ayudan al progreso de la industria.
- Permite introducir cambios parciales en una capa sin requerir cambios en la totalidad.
- Facilita la resolución de fallas en la red.

1.3.2.- Capa 1 Física

En la capa física se definen el medio, el conector y el tipo de señalización. Se especifican los requisitos necesarios para la transmisión de datos, los bits son transformados según el medio en el que se propaguen en pulsos eléctricos, luz o radiofrecuencia para ser enviados. Se establecen las características eléctricas, mecánicas y funcionales para activar, mantener y desactivar la conexión física entre sistemas finales. También especifica características como niveles de voltaje, tasa de transferencia de datos, distancias máximas de transmisión y conectores, cada medio de red posee a su vez su propio ancho de banda y unidad máxima de transmisión MTU (Maximum Transmission Unit).

Los medios físicos y conectores usados para conectar dispositivos al medio vienen definidos por estándares de la capa física.

Los conectores y dispositivos de esta capa pueden ser transceivers, repetidores y hubs, ninguno de ellos manipula los datos transmitidos, sino que solo se encarga de transportarlos y propagarlos por la red.

Los repetidores se encargan de retransmitir y retemporizar los pulsos eléctricos cuando la extensión del cableado supera las medidas especificadas.

Los hubs son repetidores multipuerto. Al recibir una trama inundan todos sus puertos obligando a todos los dispositivos conectados a él a leer dichas tramas.

Los transceivers son adaptadores de un medio a otro.

La unidad de datos del protocolo PDU (Protocol Data Unit) de esta capa es el bit. Algunos protocolos de esta capa son RJ45, RJ11, UTP, BNC, fibra óptica, etc.

1.3.3.- Capa 2 Enlace de datos

La finalidad de esta capa es proporcionar comunicación entre los puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico del host de la red se realiza en esta capa para facilitar a los

dispositivos de red la determinación de si deben subir o no un mensaje a la pila de protocolos.

La capa de enlace de datos tiene conocimiento de la topología a la que está conectada y donde se desempeña la tarjeta de red NIC (Network Interface Card).

Esta capa se encuentra dividida en dos subcapas, la capa de control de enlace lógico LLC (Logical Link Control, 802.2) responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulamiento posterior de los mismos para ser transmitidos a través de la red, y la subcapa de control de acceso al medio MAC (Media Access Control 802.3), responsable del acceso al medio, el direccionamiento físico, topología de la red, notificación de errores, distribución ordenada de tramas y control óptimo de flujo. Las direcciones físicas de origen destino son representadas como direcciones de capa MAC.

Los dispositivos de capa 2 son los puentes, los switch (se considera un puente multipuerto) y la NIC, estos dispositivos dividen a la red en segmentos (cada puerto es un segmento) generando un dominio de colisión por cada segmento. Un dominio de colisión es un segmento físico de una red donde es posible que exista colisión de tramas generadas por diferentes dispositivos dentro del mismo segmento.

Los switch almacenan en una memoria de contenido direccionable CAM (Content-Addressable Memory) las direcciones físicas de los dispositivos asociados a un segmento de red conectado directamente a un puerto determinado. De esta manera identificará porque puerto enviar la trama. Si el dispositivo de destino está en el mismo segmento que el origen, el switch bloquea el paso de la trama a otro segmento, este proceso se conoce como filtrado. Si el dispositivo de destino se encuentra en otro segmento, el switch envía la trama únicamente al segmento apropiado, a este proceso se le conoce como conmutación de capa 2. Si el dispositivo destino es desconocida para el switch este reenviara la trama a todos los segmentos excepto a aquel por donde recibió la información. La NIC de cada dispositivo almacena en su propia ROM la direcciona MAC que le pertenece.

La PDU de esta capa es la trama. Algunos protocolos de esta capa son Ethernet, 802.2, 802.3, HDLC, PPP, Frame Relay, ATM, MPLS, etc

1.3.4.- Capa 3 Red

La capa de red define como transportar los datos entre dispositivos que no están conectados en el mismo dominio de difusión o de broadcast, es decir que pertenecen a diferentes redes. Para conseguir esta comunicación es necesario conocer las direcciones lógicas asociadas a cada puesto de origen y destino y una ruta bien definida a través de la red para alcanzar el destino deseado. La capa de red es independiente de la de enlace de datos por lo que puede ser utilizada para conectividad con medios físicos diferentes. Las direcciones lógicas son jerárquicas, primero definen las redes y luego al dispositivo o nodo perteneciente a esa red.

Una dirección lógica cuenta con dos partes bien definidas, una que identifica de forma única a la red dentro de un conjunto en la internetwork y otra parte que representa al host dentro de esta red. La suma de ambas partes brinda un identificador único para cada dispositivo. Un router identifica dentro de la dirección lógica la porción perteneciente a la red con el fin de identificar el segmento de red a donde debe enviar los paquetes. A estos identificadores se les llama dirección de protocolo de internet IP (Internet Protocol) pueden ser versión 4 IPv4 o versión 6 IPv6.

En IPv4 existen dos conceptos llamados IP pública e IP privada, hacen referencia al anuncio en internet, es decir una IP pública será anunciada en internet permitiendo que cualquier equipo conectado a internet pueda tener comunicación con el dispositivo dueño de esta IP, las IPs privadas no son publicadas a internet por lo que solamente dispositivos dentro de la misma red podrán tener acceso al host dueño de la IP.

Las redes IPv4 privadas son:

1) 10.0.0.0 /8
2) 172.16.0.0 /12
3) 192.168.0.0 /16

El dispositivo de esta capa se llama router, este elemento de red separa los segmentos en dominios de colisión y difusión únicos. Los routers cumplen dos funciones básicas que son enrutar y conmutar los paquetes, para lograrlo registran en tablas de enrutamiento los datos necesarios para esta función.

Una IPv4 se caracteriza por:

- Una dirección de 32 bits, dividida en 4 octetos. Este direccionamiento identifica una porción perteneciente a la red y otra al host.
- A cada dirección IP le corresponde una máscara de red de 32 bits dividida en 4 octetos. El router determina las porciones de red y de host por medio de la máscara de red.
- Las direcciones IP se representan generalmente en formato decimal para hacerlas más comprensibles. Esta forma se conoce como decimal punteado o notación decimal punteado.

  Ejemplo:

  Dirección IP 172.16.1.3

  Máscara de red 255.255.0.0

172	16	1	3
10101100	00010000	00000001	00000011

255	255	0	0
11111111	11111111	00000000	00000000

Tabla 1.2: Dirección IP y Máscara

En la tabla anterior, los octetos resaltados en color azul pertenecen a la porción de red y los campos resaltados en rosa son los pertenecientes a la porción de host.

Los routers identifican las porciones de red comparando las direcciones IP con sus respectivas máscaras efectuando la operación booleana AND. Los routers ignoran el campo de host para identificar la red destino a la que este pertenece.

Para hacer la operación AND el router compara bit a bit la dirección IP y la máscara utilizando el siguiente razonamiento:

1x1=1

1x0=0

0x1=0

0x0=0

Ejemplo:

En binario

Dirección de host 10101100.00010000.00000001.00000011

Máscara de red 11111111.11111111.00000000.00000000

Dirección de red 10101100.00010000.00000000.00000000

En decimales:

Dirección IP 172. 16. 1. 3

Máscara de red 255.255. 0. 0

Dirección de red 172. 16. 0. 0

La PDU de esta capa es el paquete. Algunos protocolos de esta capa son IPv4, IPv6, ARP, RARP, ICMP.

1.3.5.- Capa 4 Transporte

La capa de transporte establece las reglas necesarias para concretar una conexión entre dos dispositivos remostos, permite que las estaciones finales ensamblen y reensamblen múltiples segmentos del mismo flujo de datos, esto se hace por medio de identificadores llamados número de puerto. La capa cuatro permite además que las aplicaciones soliciten transporte fiable entre los sistemas, asegura que los segmentos distribuidos serán confirmados al remitente, proporciona la

retransmisión de cualquier segmento que no sea confirmado, coloca los segmentos en el orden correcto en el receptor y proporciona control de flujo regulando el tráfico de datos.

En la capa de transporte los datos pueden ser transmitidos de forma fiable o no fiable. El protocolo de control de transmisión TCP (Transmission Control Protocol) es fiable orientado a la conexión con un saludo previo de tres vías, mientras que el protocolo de datagramas de usuario UDP (User Datagram Protocol) es no fiable siendo no orientado a la conexión.

La PDU de esta capa es el segmento. Algunos protocolos de esta capa son TCP, UDP.

1.3.6.- Capa 5 Sesión

Se encarga del control de los diálogos entre distintos nodos. Un diálogo es una conversación formal en la que dos nodos acuerdan un intercambio de datos. Establece (negocia parámetros), mantiene y libera la conexión.

La PDU de esta capa son los datos. Algunos protocolos de esta capa son SQL, NFC, SCP.

1.3.7.- Capa 6 Presentación

Garantiza que la información que es enviada desde la capa de aplicación del origen, sea legible por la capa de aplicación del equipo destino, lo hace dando formato a los datos dependiendo de la aplicación que se esté manejando.

La PDU de esta capa son los datos. Algunos protocolos de la capa de presentación son TIFF, JPEG, MPEG, MP3, ASCII.

1.3.8.- Capa 7 Aplicación

Provee servicios de red a los procesos de aplicaciones de usuario que residen en el equipo terminal.

La PDU de esta capa son los datos. Algunos protocolos de la capa de aplicación son HTTP, SNMP, FTP, Telnet, SSH.

1.4.- Modelo de referencia TCP/IP

El departamento de defensa de Estados Unidos (DoD) creo el modelo de referencia TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia. La creación de este modelo ayudo a resolver la problemática de transmitir datos independientes del estado de un nodo particular de la red, desde entonces TCP/IP se ha convertido en la base de internet.

El modelo TCP/IP original consta de cuatro capas que son la capa de aplicación, la capa de transporte, la capa de internet y la capa de acceso a la red, posteriormente en una actualización del modelo, la capa de acceso a la red se dividió en dos subcapas la física y la de enlace de datos.

TCP/IP Original	TCP/IP Actualizado
Aplicación	Aplicación
Transporte	Transporte
Internet	Internet
Acceso a la red	Enlace de datos
	Física

Tabla 1.3: Tabla comparativa modelo TCP/IP original y actualizado

A continuación, se muestra una tabla comparativa entre el modelo OSI y el modelo TCP/IP original, así como algunos protocolos que se ocupan en cada una de las capas.

MODELO OSI	MODELO TCP/IP	Protocolo
Aplicación	Aplicación	Telnet, SSH, FTP, SNMP, TFPT, SMTP, HTTP.
Presentación		
Sesión		
Transporte	Transporte	TCP, UDP.
Red	Internet	ICMP, ARP, RARP, IP.
Enlace de datos	Acceso a la red	MPLS, RJ45, ATM, Ethernet.
Física		

Tabla 1.4: Comparación modelo OSI vs modelo TCP/IP

1.5.- Redes redundantes

Los conceptos de redundancia y de alta disponibilidad enfocados a las redes, comprenden la capacidad de un sistema de comunicaciones para detectar un fallo en la red de la manera más rápida posible y que a la vez, sea capaz de recuperarse del problema de forma eficiente y efectiva, afectando lo menos posible al servicio. La redundancia hace referencia a nodos completos que están replicados o componentes de éstos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que haya una caída del sistema. Ligado a esto, la alta disponibilidad consiste en la capacidad del sistema para ofrecer un servicio activo durante un tanto por ciento de un tiempo determinado o a la capacidad de recuperación del mismo en caso de producirse un fallo en la red. Cuando se habla de “caída del sistema” puede hacer referencia tanto a un equipo que ha dejado de funcionar, como un cable que ha sido cortado o desconectado; u otras situaciones que impliquen que la red deje de operar.

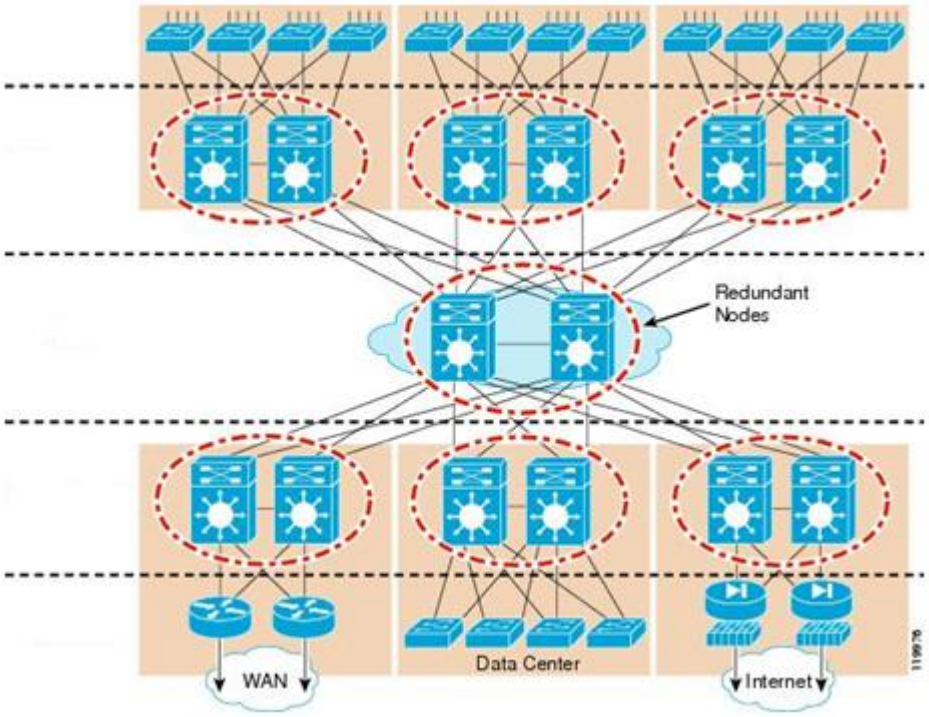

Figura 1-11: Redes redundantes basas en un modelo jerárquico

1.5.1.- Modelo Jerárquico

Los modelos Jerárquicos se utilizan con el fin de simplificar el diseño, implementación y administración de la red. Un modelo jerárquico acelera la convergencia, mantiene posibles problemas aislados por capas y reduce la sobrecarga en los dispositivos.

El modelo se compone de tres capas o niveles que son de acceso, de distribución y de núcleo o core.

La capa de acceso es el punto en el que cada usuario se conecta a la red. Los usuarios, así como los dispositivos a los que necesitan acceder con más frecuencia están disponibles a nivel local.

En algunos casos no es posible proporcionar a los usuarios un acceso a todos los servicios como archivos de bases de datos, almacenamiento centralizado o acceso telefónico a la web, en estos casos el tráfico se desvía a la siguiente capa del modelo, la capa de distribución.

Algunas de las funciones de la capa de acceso son:

- Interconexión de los grupos de trabajo hacia la capa de distribución.
- Segmentación en múltiples dominios de colisión.
- Implementación de redes de área local virtual VLAN (Virtual Local Area Network)

La capa de distribución es el punto medio entre la capa de acceso y los servicios principales de la red, las funciones principales de esta capa es la de realizar enrutamiento, filtrado y acceso a WAN.

Esta capa brinda conectividad basa en políticas determinadas, dado que determina cuando y como los paquetes pueden acceder a los servicios principales de la red. La capa de distribución selecciona la forma más rápida para que la petición de un usuario pueda ser remitida al servidor, una vez que la ruta es elegida, envía la petición a la capa de núcleo para que esta pueda transportar la petición al servidor apropiado.

La capa de núcleo se encarga de desviar el tráfico lo más rápido posible hacia los servicios apropiados. Los servicios existentes en la capa de núcleo generalmente son comunes para todos los usuarios de la red y son conocidos como servicios globales o corporativos.

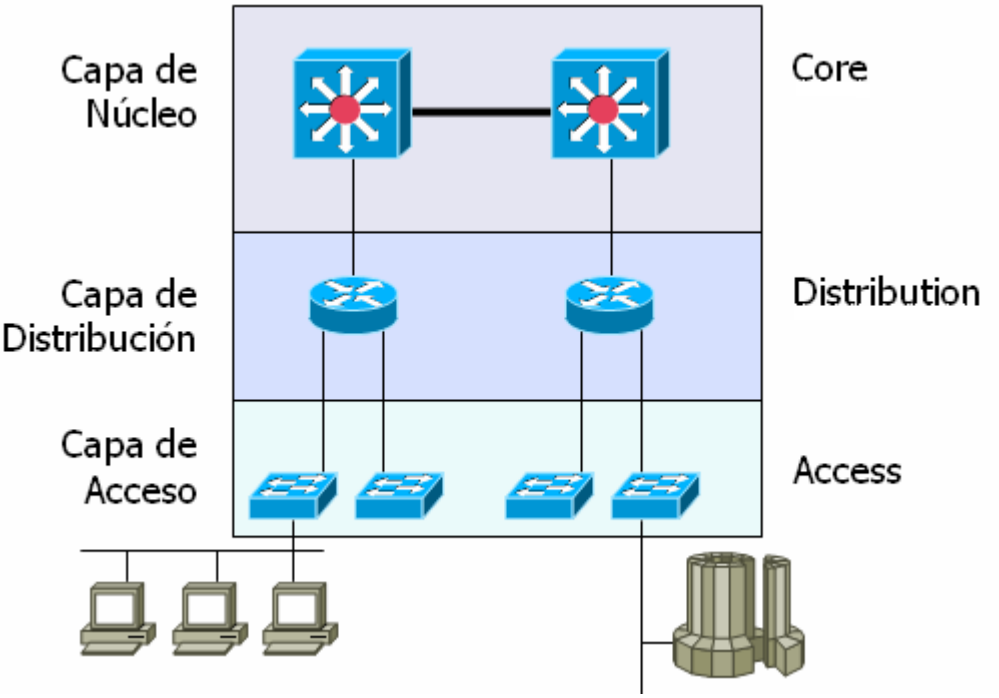

Figura 1-12: Modelo jerárquico de red

1.5.2.- Redes LAN redundantes

En un modelo Jerárquico las redundancias generalmente se realizan en las capas de distribución y de núcleo a través de hardware adicional y rutas alternas entre dicho hardware. Pero también se puede realizar la redundancia entre elementos de la capa de acceso es decir entre switch que brindan la comunicación entre usuarios de una misma red y tienen comunicación hacia la capa de distribución, este será el escenario de redundancia en el que se basará el tema 1.5.2.

Las redes LAN empresariales actuales requieren una alta resistencia a fallos que permitan asegurar una disponibilidad de servicios de red lo más cercana posible al 100% del tiempo.

Dado que no existe equipamiento que pueda asegurar una disponibilidad del 100%, este objetivo se cubre implementando redundancia. Hay diferentes niveles de redundancia que se implementan en una red, uno de ellos es la redundancia de enlaces o de rutas a nivel de capa de enlace de datos. Redundancia en este nivel

implica multiplicidad de rutas o caminos para llegar de un origen a un destino posible. La redundancia brinda ventajas de gran importancia a las redes LAN conmutadas como son:

- Confiabilidad que se traduce en un mayor tiempo de disponibilidad de la red
- Eliminación de un único punto de falla.

Pero la existencia de bucles o caminos redundantes a nivel de capa 2 en la red, también provoca inconvenientes como pueden ser:

- Tormentas de broadcast. Son el problema más habitual o conocido. Las tormentas de broadcast son un verdadero problema en capa 2 ya que en el encabezado de la trama no existe un campo de tiempo de vida que asegure el descarte de la trama, por lo que una trama podría circular indefinidamente en un bucle. En consecuencia, una red conmutada no puede tener loops o bucles en capa 2.
- Inestabilidad en las tablas de direcciones MAC. La tabla de direcciones MAC de los switches permite que una dirección MAC esté asociada al mismo tiempo solamente a un puerto. Por este motivo, cuando un switch recibe copias de una misma trama por diferentes puertos, la tabla de direcciones MAC comienza a ser permanentemente recalculada.
- Copias múltiples de una misma trama. Al generarse múltiples caminos hacia un mismo destino es posible que los dispositivos dupliquen la trama original y que como consecuencia el destino reciba múltiples copias de una misma trama. Generalmente los protocolos de capa superior no tienen mecanismos que les permitan manejar la duplicación de tramas.

En consecuencia, la implementación de redes LAN con caminos redundantes a nivel de capa 2 requiere necesariamente de un protocolo que permita administrar esa redundancia y evitar los bucles de capa de enlace. Ese protocolo es el protocolo de árbol de expansión STP (Spanning Tree Protocol).

1.5.3.- Spanning Tree Protocol

Spanning Tree Protocol STP, es un protocolo de capa dos publicado en la especificación del estándar IEEE 802.1d.

El objetivo de STP es mantener una red libre de bucles. Un camino libre de bucles se consigue cuando un dispositivo es capaz de reconocer un bucle en la topología y bloquear uno a mas puertos redundantes.

STP explora constantemente la red, de forma que cualquier fallo o adición en un enlace, switch o bridge es detectado al instante.

Cuando cambia la topología de red, el algoritmo STP reconfigura los puertos del switch o bridge para evitar una pérdida total de la conectividad.

Los switch intercambian información multicas a través de las unidades de datos de protocolo del puente BPDU (Bridge Protocol Data Units) cada dos segundos, si detecta una anomalía en algún puerto, STP cambiará de estado dicho puerto utilizando algún camino redundante sin que se pierda conectividad en la red.

Cada switch envía las BPDU a través de un puerto usando la dirección MAC de ese puerto como dirección de origen, el switch no sabe de la existencia de otros switch por lo que las BPDU son enviadas a la dirección de destino múlticast 01:80:C2:00:00:00.

Existen 2 tipos de BPDU

- Configuration BPDU: utilizada para el cálculo de STP.
- Topology Change Notification TCN: utilizada para anunciar los cambios en la topología de la red.

Para administrar la redundancia, STP elabora un “árbol” que contiene a todos los switches en toda la extensión del dominio de broadcast. A partir de este árbol STP coloca algunos puertos en estado de espera (bloqueo) definiendo una topología activa libre de bucles. Si a partir de ese momento la situación de algún puerto activo de la red cambiara, STP reconfigurará la topología activa para restablecer la ruta utilizando

un enlace alternativo activando algunos de los puertos que había bloqueado previamente.

La operación de STP es transparente para las estaciones de trabajo o terminales, que por lo tanto no participan del cálculo de esa topología activa.

Para definir una red conmutada libre de bucles el protocolo completa 3 tareas:

1.- Elección de un switch raíz o root briedge. Sólo hay un puente raíz en cada dominio de broadcast, todos los puertos del switch raíz son "puertos designados" (designated ports), los puertos designados están en estado de enviando (forwarding).

La elección de un switch raíz se lleva a cabo determinando el switch que posea el menor BID (Bridge ID), este valor es un identificador de 8 bytes de longitud compuesto de 2 elementos, prioridad (2 bytes) y dirección MAC del switch (6 bytes), en otras palabras, es la suma de la prioridad por defecto (32768) y el ID del switch equivalente a la dirección MAC. El valor de prioridad de un switch puede ser configurable por un administrador para manipular la elección del switch raíz, los valores posibles deben estar en el rango de 1 a 65536. Para determinar cuál switch de la red tiene el BID más bajo se parte del hecho de que todos los switches del dominio de broadcast al arrancar inundan la red con BPDUs conteniendo su ID como bridge raíz ya que parten del supuesto que cada uno es el bridge raíz, cada switch copia todos los BPDUs recibidos y compara los BID de origen de cada BPDU con su propio BID para determinar cuál será su bridge raíz. En escenarios donde la prioridad de los switch no se ha modificado, el valor que determinará el switch raíz es la dirección MAC de cada elemento.

2.- Todos los demás switch del dominio de broadcast son llamados non root bridge, estos deben seleccionar un solo puerto raíz (root port). Selecciona como puerto raíz el puerto de menor costo hacia el switch raíz y lo pone en estado de renviando. El costo de una ruta STP es un valor acumulado de la ruta, basado en el ancho de banda de cada uno de los enlaces que atraviesa.

Costos que establece STP.

Velocidad del puerto	802.1d	802.1t	Legacy
10 Mbps	99	1999999	1999
100 Mbps	18	199999	199
1 Gbps	4	20000	20
10 Gbps	2	2000	2

Tabla 1.5: Costos de rutas en STP

3.- En cada segmento se selecciona un puerto designado. Se elige como puerto designado el que pertenece al switch con una ruta con menor costo hacia el switch raíz. El puerto designado está en estado de reenvió, los puertos no-designados quedan en estado de bloqueado. En consecuencia, existen 3 roles de puertos STP, puerto raíz, puerto designado y puerto no designado.

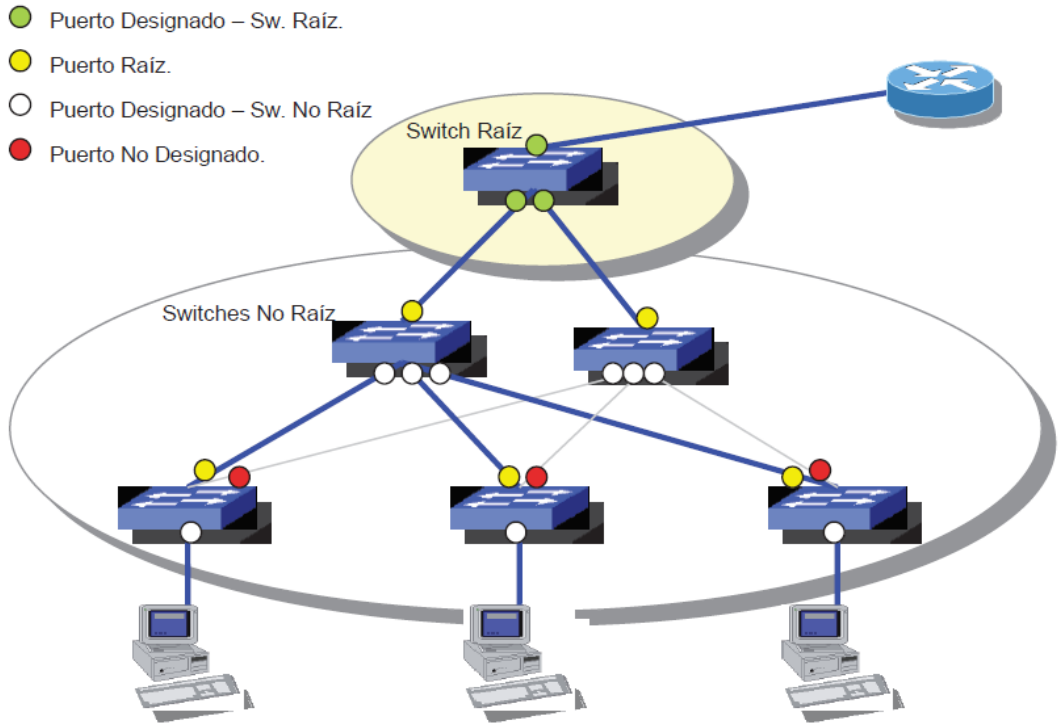

Figura 1-13: Tipos de puertos STP

En resumen, en una red LAN que implementa STP, luego de converger, los puertos de cada uno de los dispositivos de la red pueden o no formar parte de la topología activa (el árbol de rutas habilitadas para la transmisión de las tramas). Los puertos que forman parte del árbol spanning tree reciben la denominación de puertos designados y se encuentran en estado de enviando, todos los demás puertos que no forman parte del árbol, y que por lo tanto se encuentran bloqueados para evitar la formación de bucles, reciben el nombre de puertos no designados.

De acuerdo a su situación operativa respecto de la red y el árbol de Spanning Tree, los puertos de cada dispositivo pueden pasar por 5 estados diferentes que son:

1.- Bloqueado (Blocking). Es uno de los estados habituales de los puertos del switch luego de que la red ha convergido. Todos los puertos están bloqueados por defecto al momento de habilitarse para evitar los bucles. El puerto permanece en este estado mientras el switch determine que hay una ruta mejor al switch raíz (menor costo). En este estado, el puerto recibe BPDUs, pero no recibe ni envía tramas de datos.

2.- Escuchando (Listening). Es un estado transitorio del puerto, en este estado el puerto escucha BPDUs para asegurarse que no hay otra ruta mejor hacia el switch raíz antes de comenzar a enviar. Si determina que esta no es la ruta con el menor costo y hay otra mejor, el puerto regresa al estado de bloqueado. Este estado se utiliza para indicar que el puerto está en posibilidad de comenzar a transmitir, pero aún no lo hace para garantizar que no se cree un bucle.

3.- Aprendiendo (Learning). Es el siguiente estado transitorio del puerto, en este estado el switch aprende direcciones MAC a través de ese puerto, con las que construye sus tablas, pero no reenvía tramas aún. Sigue procesando BPDUs para asegurarse del estado de la red.

4.- Enviando (Forwarding). En este estado el puerto envía y recibe normalmente todas las tramas de datos que ingresan. También procesa BPDUs.

5.- Desactivado. Algunas descripciones del protocolo incluyen este quinto estado. Este en realidad no es propiamente un estado generado por el protocolo, sino que corresponde a la deshabilitación administrativa del puerto que realiza de modo manual el Administrador.

Cuando se enciende un switch, STP se encuentra activo por defecto y coloca todos los puertos en estado de blocking. A partir de este punto cada puerto debe pasar por los estados de transición (listening y learning) para luego llegar al estado de forwarding. Cuando un puerto opera con STP se estabiliza en 2 estados posibles: blocking o forwarding.

STP utiliza temporizadores para definir tanto el período de tiempo entre actualizaciones, como el período de tiempo que dura cada uno de los estados por los que pasa un puerto de una red STP, Esos temporizadores son 3:

- Hello Time. Período de tiempo entre envío de BPDUs, tiene el valor por defecto de 2 segundos.
- Forward Delay. tiempo que tarda un puerto en pasar del estado de escuchando al de aprendiendo; o del de aprendiendo al de enviando, el valor por defecto es de 15 segundos.
- Max Age. Es el tiempo por el cual el dispositivo almacena la información correspondiente a una BPDU, el valor por defecto es de 20 segundos.

En el momento en que se produce un cambio en la red, todos los dispositivos deben recalcular STP para lo cual bloquean nuevamente todos los puertos, provocando una interrupción en el tráfico de la red. Ese proceso de recalculo de la topología activa demanda 50 segundos por defecto, el escenario es el siguiente:

Al segundo 0, se recibe el último BPDU, el puerto en estado blocking permanece en el mismo hasta después de 20 segundos cuando se descarta la información correspondiente al último BPDU, y se inicia el proceso de recalculo del árbol. El puerto pasa al estado de escuchando, este estado tiene una duración por defecto de 15 segundos por lo cual al segundo 35 después de recibir el último BPDU, Finaliza

el período de escucha y el puerto comienza a aprender direcciones MAC y construir sus tablas, el puerto pasa al estado aprendiendo y permanece así otros 15 segundos, finalmente al segundo 50 el puerto cambia de estado a enviando y la red vuelve a estar disponible. Por lo tanto, STP 802.1D, requiere de 50 segundos de afectación para poder solventar una falla, este tiempo puede no ser una opción para muchas redes que demandan alta disponibilidad de su red.

1.5.4.- Tipos de STP

Existen variantes de STP que mejoran el funcionamiento y reducen el tiempo que tarda en converger la red STP una vez que se presenta una falla.

STP (802.1D). Genera una única instancia de STP para toda la red independientemente del número de VLANs existentes. En muchos casos, en redes actuales con muchas VLANs puede seleccionar rutas subóptimas para el tráfico de la red.

RSTP (Rapid Spanning Tree Protocol 802.1w). Es una evolución de 802.1D que ofrece mejores tiempos de convergencia ya que incluye la característica de Edge Port de RSTP que permite el cambio del puerto al estado enviando prácticamente de inmediato, RSTP también mantiene una única instancia de STP sin importar el número de VLANs, aún es posible que el protocolo seleccione rutas subóptimas. Dadas sus características tiene requerimientos de hardware superiores a STP.

MSTP (Multiple Spanning Tree Protocol 802.1s). Mapea múltiples VLANs a una o varias instancias de RSTP. Requiere más recursos que RSTP.

Dos inconvenientes de utilizar STP son: Tiempos de convergencia altos (aunque con RSTP y MSTP se bajan considerablemente), ancho de banda desperdiciado al no permitir el reenvío de datos por al menos un enlace de la topología de STP.

Para evitar estas problemáticas se han desarrollado soluciones como agregación de enlace (link aggregation). Esta funcionalidad implementada en la red brinda redundancia además de que mantiene todos los enlaces activos aprovechando el 100% del ancho de banda. Esto es posible debido a que se pueden unir 2 o más puertos (máximo 8 en equipos CISCO) físicos para que el dispositivo considere esta unión como un solo puerto virtual, permitiendo la transferencia de datos por todos los puertos físicos que pertenezcan al virtual. En caso de que alguno de los enlaces que lo componen falle, el tráfico se balanceará por los que se encuentren disponibles en ese momento.

En la figura siguiente se muestra un conjunto de dispositivos interconectado entre sí y haciendo uso de la agregación de enlace.

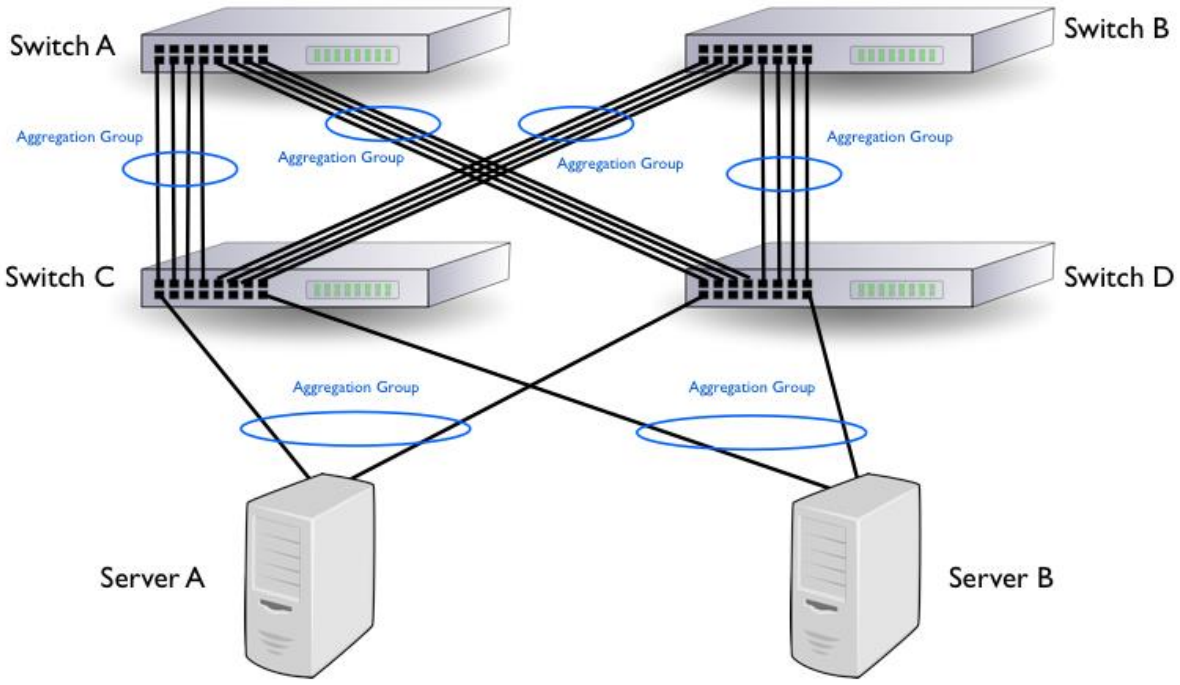

Figura 1-14: Agregación de enlace LAG (Link Agregation)

1.5.5.- Acceso de redes empresariales a la red de un ISP

Una red empresarial implementada en un edificio, se limita a comunicación LAN donde todos los servicios se encuentran disponibles en el mismo recinto para los

usuarios, pero cuando la empresa u organización es grande y cuneta con varias sedes en una ciudad, país o incluso el mundo, los más recomendable es ofrecer servicios centralizados. En este escenario, los datos de los usuarios que desean acceder a los servicios deben salir de la red LAN hacia una red WAN que los comunicará con el centro de datos donde se alojan los servidores de la empresa. La infraestructura necesaria para comunicar todas las sedes de una organización con el centro de datos puede resultar sumamente cara por lo que generalmente, las empresas contratan los servicios de algún ISP para rentar la infraestructura de este y obtener la comunicación deseada. Lo mismo sucede cuando requiere la empresa más de un acceso a internet y el servicio es dedicado.

El acceso a la red WAN en cada sede de la empresa, puede brindarse con un solo equipo que conecta el edificio del cliente con la infraestructura del ISP, a este tipo de solución se le conoce como servicio 1+0 (sin redundancia) o single homed. La figura siguiente muestra el escenario single homed.

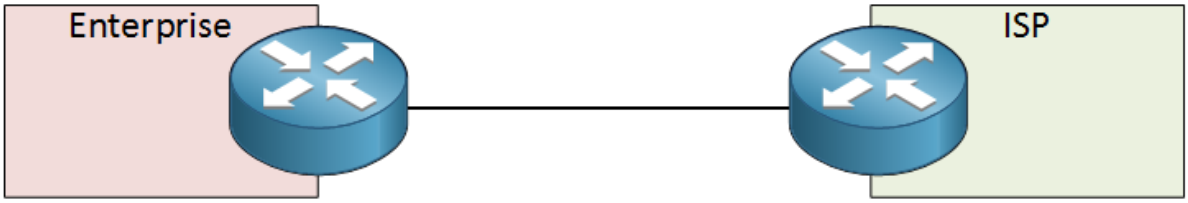

Figura 1-15: Single Homed

Un ISP puede brindar el mismo servicio a diferentes empresas (clientes) incluso si el direccionamiento IP privado es el mismo en dos o más organizaciones que requieran hacer uso de su infraestructura, sin mezclar el tráfico de cada uno. En la figura siguiente se muestra un escenario single homed en varias sedes de 3 empresas pasando por la infraestructura de un mismo ISP.

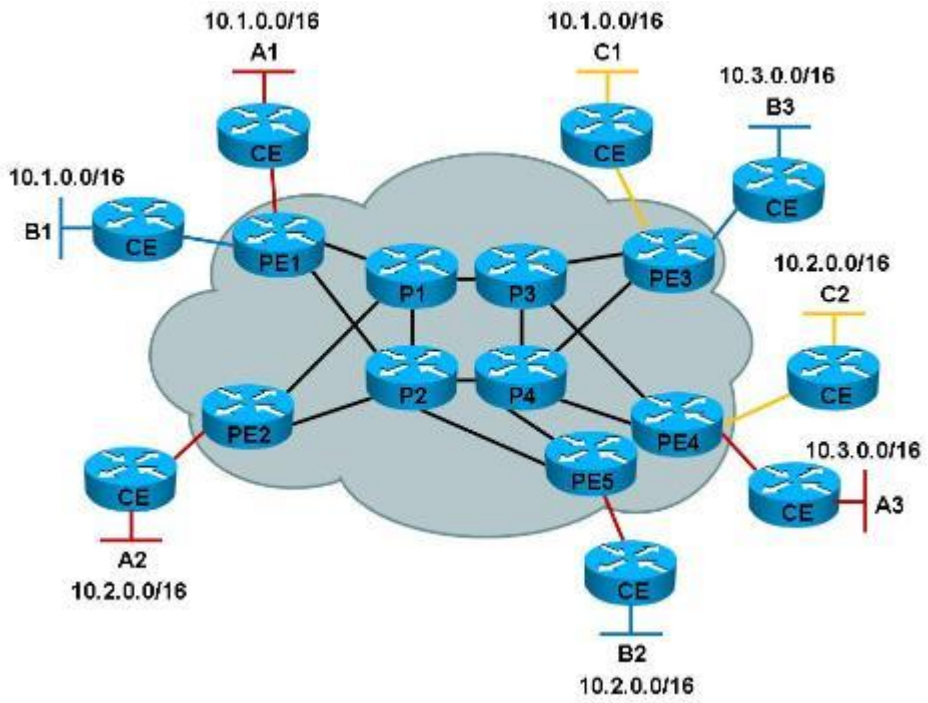

Figura 1-16 Escenario de conectividad 1+0

Los equipos CE (Customer Edge) hacen referencia a un router demarcador en la frontera de la red del cliente, mientras que los equipos PE (Provider Edge) son el equipo demarcador en la frontera de la red del ISP, Los equipos identificados como P, son equipos en los que no se conectan CEs, y se encuentran en la red de CORE de un ISP.

El problema de los servicios single homed es que la interfaz del equipo CE se vuelve el único punto de falla para acceder a la red WAN y poder alcanzar servicios fque existen fuera de la red LAN, en escenarios donde se requiera alta disponibilidad con sobrevivencia a fallas esto se vuelve un problema por lo que se deberán considerar los servicios llamados 1+1(con redundancia) o dual homed. Este tipo de servicios se puede implementar con dos equipos CE o con uno que tenga dos interfaces hacia la WAN, estos CE se conectarán a la misma red LAN. Este tipo de escenarios requiere una ingeniería de tráfico para poder determinar que paquetes se enrutan por cada equipo CE o por cada interfaz WAN en caso de que solo exista un CE, este esquema se denomina activo-activo. Cuando se configura un router como principal y el

segundo como un respaldo que solo enviará tráfico cuando el router o puerto principal falle, a este esquema se le llama activo-pasivo. Además de controlar el tráfico hacia la doble conexión WAN, también es necesario revisar cómo se conectarán los elementos de la red LAN a ambos routers para que una afectación en el equipo principal sea transparente para los usuarios finales, esto se logra con el Protocolo de redundancia de enrutador virtual VRRP (Virtual Router Redundancy Protocol) o si se maneja solo equipo CISCO se puede implementar el protocolo propietario de esta marca llamado Hot Standby Router Protocol (HSRP). En la figura siguiente se muestra el escenario Dual Homed con un solo equipo CE y un equipo del ISP

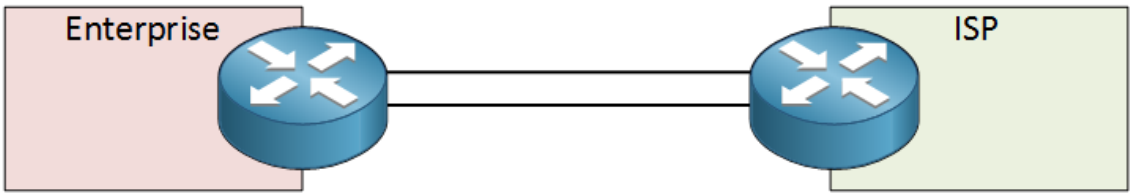

Figura 1-17: Dual Homed

A continuación, se ejemplifica el escenario Dual Homed con un solo equipo CE y dos equipos del mismo ISP

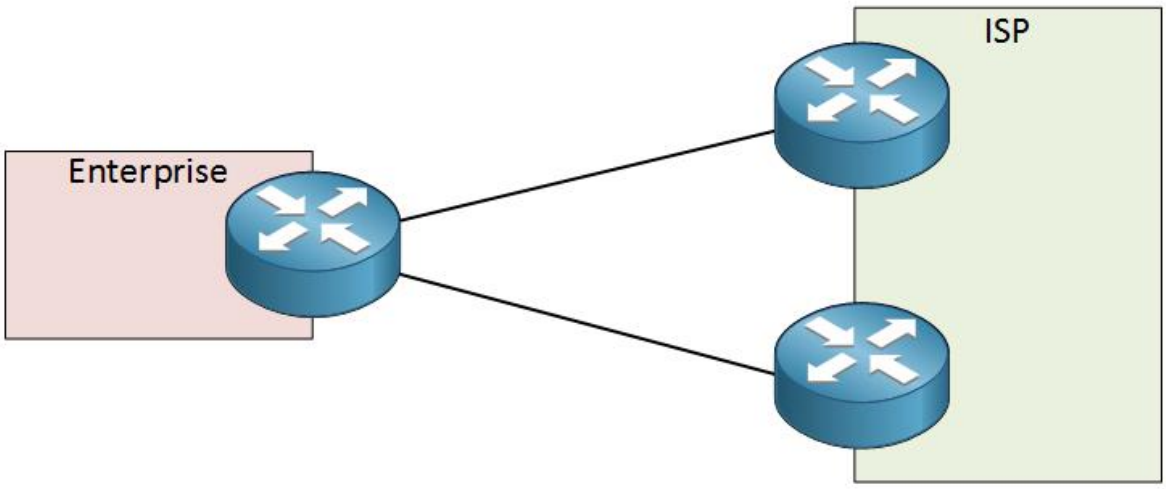

Figura 1-18: Dual Homed

La figura siguiente muestra el escenario Dual Homed con dos equipos CE y dos equipos del ISP

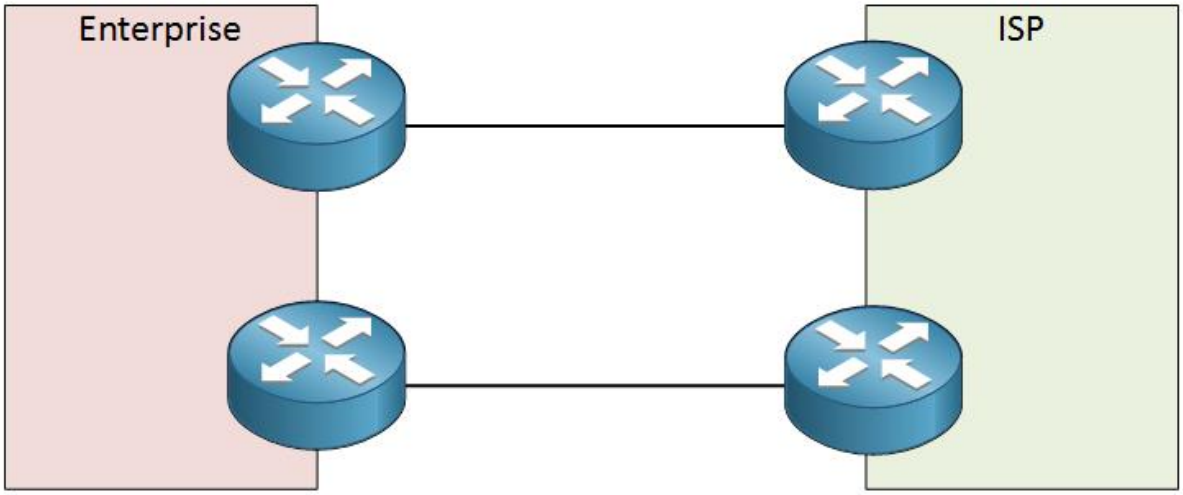

Figura 1-19: Dual Homed

Se considera la posibilidad de que las conexiones WAN sean con diferente ISP, este servicio se denomina single multihomed en caso de que exista solo una conexión a cada ISP o dual multihomed cuando se implementan al menos dos conexiones a cada ISP sin importar el número de equipos CE.

En la figura siguiente se ilustra el esquema Single Multihomed con un equipo CE

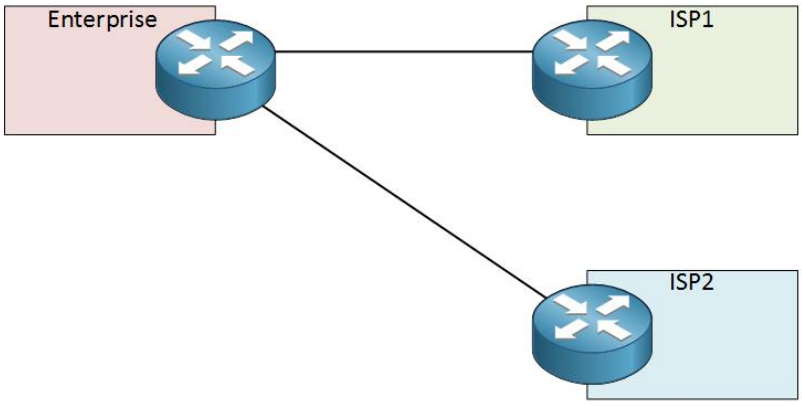

Figura 1-20: Single Multihomed

En la figura siguiente se muestra el esquema de redundancia Single Multihomed con dos equipos CE pero solo una conexión a cada ISP

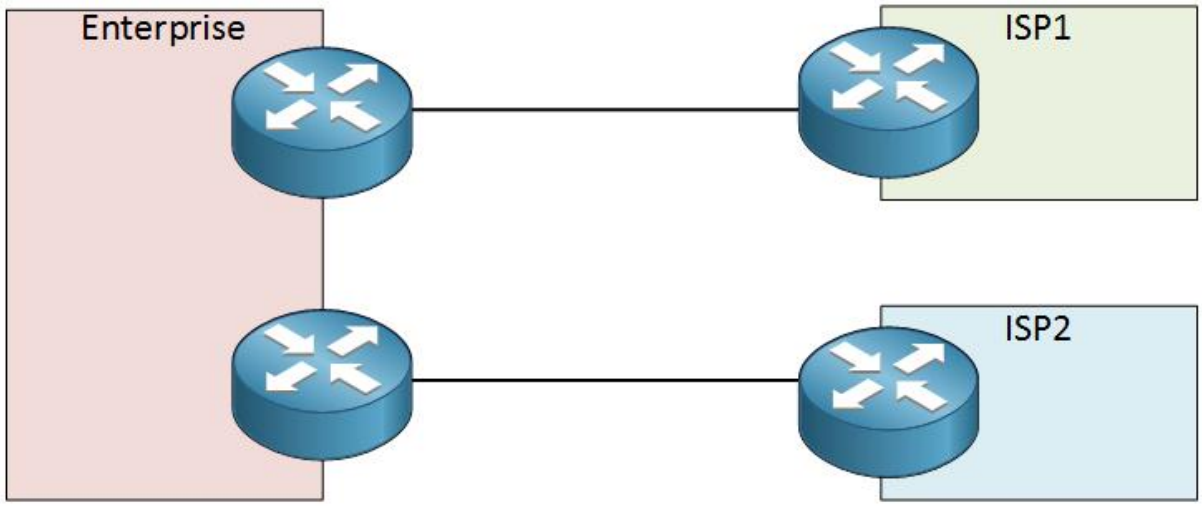

Figura 1-21: Single multihomed

La siguiente figura muestra un esquema Dual Multihomed con un solo equipo CE pero doble enlace a cada ISP.

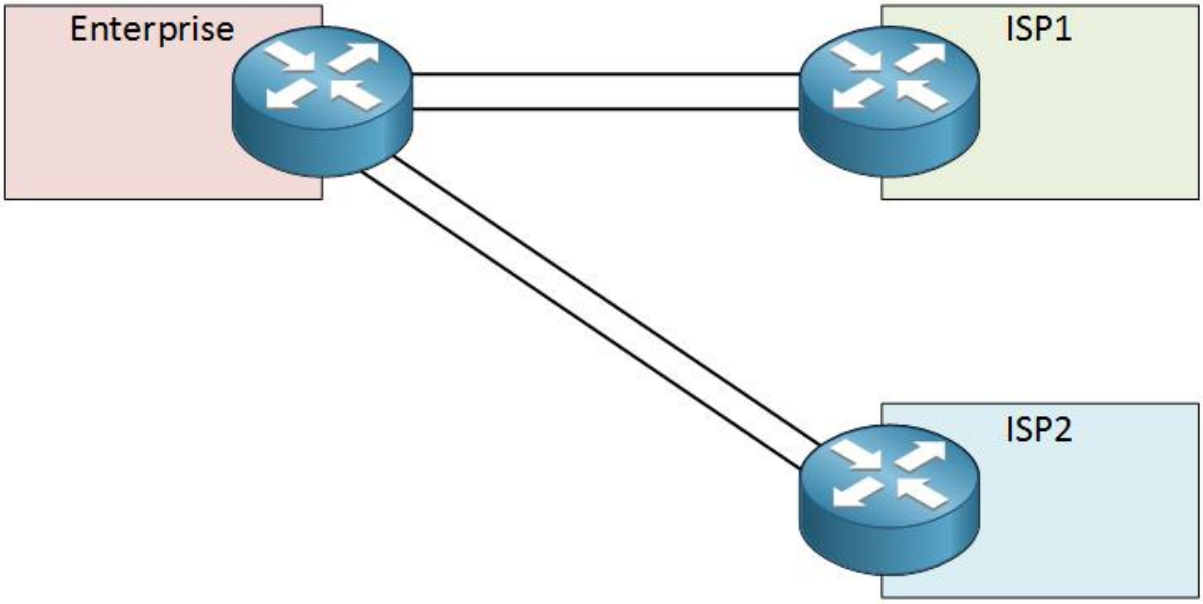

Figura 1-22: Duan Multihomed

La siguiente figura ejemplifica el esquema Dual Multihomed implementando doble equipo CE.

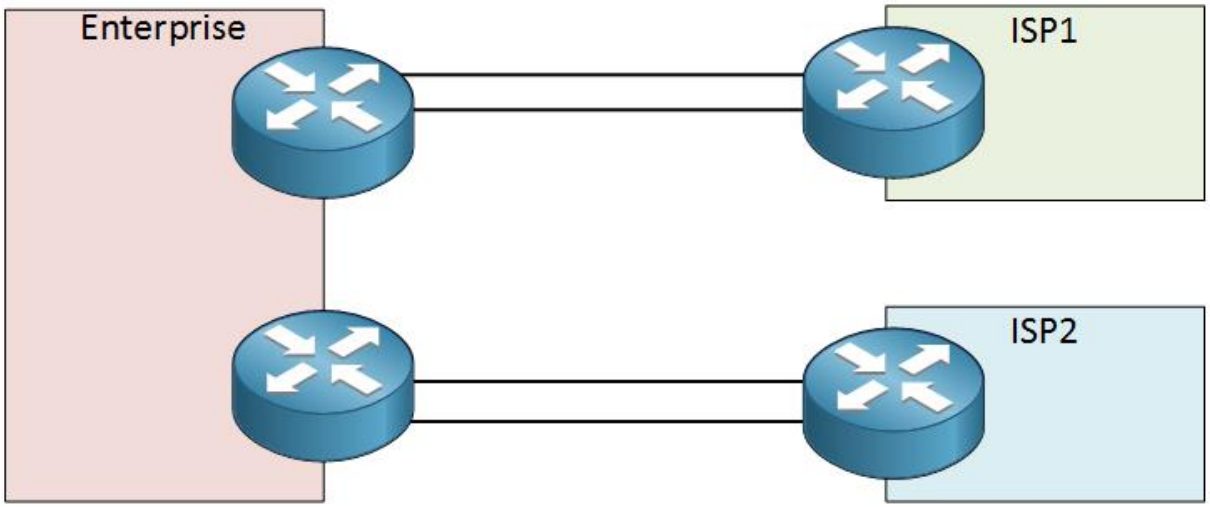

Figura 1-23: Dual Homed

El esquema de redundancia mostrado en la siguiente figura sería tal vez el que brinde mayor disponibilidad de la red debido a que cada equipo CE se encuentra con redundancia de enlace y de ISP en caso de falla.

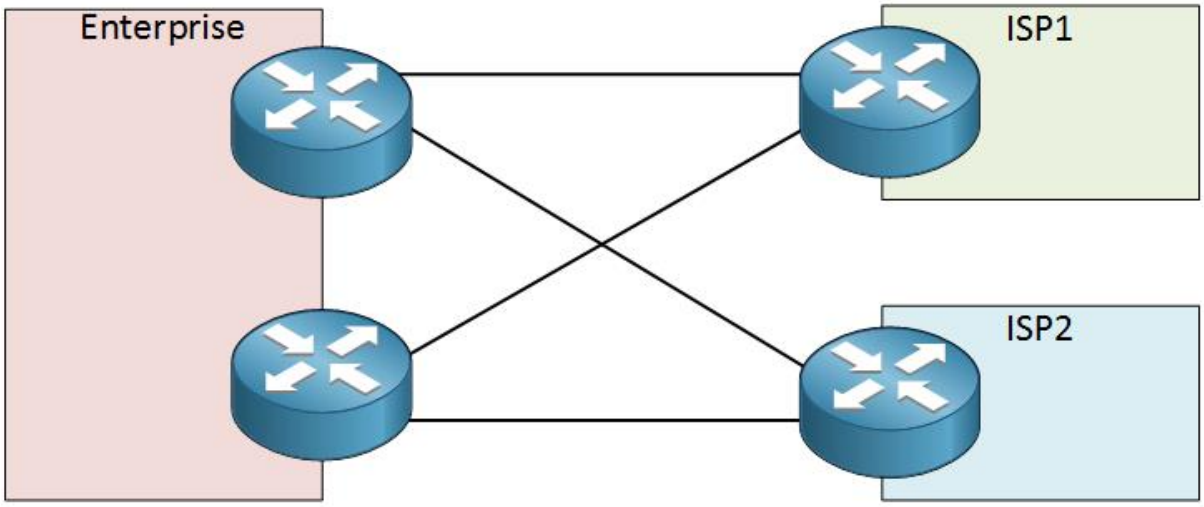

Figura 1-24: Dual Multihomed

1.5.6.- Esquema de redundancia activo-pasivo

Cuando una empresa necesita tener servidores anunciados en internet o requiere conectarse desde una o varias sedes a servicios centralizados de la misma organización, renta la infraestructura de un ISP para poder conseguirlo, partiendo de este punto, un servicio contratado por una empresa en esquema activo-pasivo trabajará de la siguiente manera:

- Existirán dos equipos CE alojados en las oficinas donde se pido el servicio o por temas de costos o diseño puede haber solo un equipo CE pero con 2 interfaces con conectividad a la infraestructura del ISP (red WAN).
- La red WAN puede pertenecer a uno o más ISP.
  a) Si ambos enlaces WAN son hacia la infraestructura de un mismo ISP, recibirá el nombre de dual homed.
  b) Si una interface WAN tiene acceso a la infraestructura de un ISP y la otra tiene acceso a la infraestructura de otro ISP, el servicio se denominará single Multihomed, esto es solo una interfaz a cada ISP sin importar si se ocupan uno o dos equipos CE. Dual multihomed se llamará el tipo de solución que tiene dos conexiones a cada ISP.
- Ambos CEs se conectarán a través de una misma red LAN mediante una interface física diferente a la WAN. En el caso de que solo exista un CE, la conexión a la red LAN será a través de un solo puerto del mismo CE pero diferente interfaz de la WAN.
- Cada CE o interfaz WAN brindará un acceso independiente a la infraestructura del ISP.
- Se configurarán políticas de salida y entrada de tráfico desde y hacia las redes LAN de tal manera que todo el tráfico salga y entre mediante el mismo equipo (principal) o interfaz WAN (en caso de que sea un solo equipo CE) y si ocurre cuna falla con este, el segundo equipo o interfaz deberá ser capaz de procesar el tráfico hasta que se solucione la falla del acceso WAN principal.

- En caso de existir doble conexión hacia la LAN, se deberá implementar VRRP o similares como HSRP para que la conmutación de salida de tráfico en caso de falla en el servicio que brinda el CE principal, sea imperceptible para los hosts de la red LAN.

1.5.7.- Esquema de redundancia activo-activo

Teniendo en cuneta las mismas necesidades de la empresa, y además se requiere ocupar el ancho de banda total de ambos accesos WAN, es necesario que se implemente el esquema activo-activo.

El modo de operación activo-activo para servicios con acceso a la red WAN redundado trabajará de la siguiente manera:

- Exitirán dos accesos a la red WAN.
- Los accesos pueden encontrarse en dos puertos independientes en un mismo equipo CE o pueden establecerse en dos equipos CE.
- Al igual que en el esquema activo-pasivo, la red WAN puede pertenecer a uno o más ISP.
  a) Si ambos enlaces WAN son hacia la infraestructura de un mismo ISP, recibirá el nombre de dual homed.
  b) Si una interface WAN tiene acceso a la infraestructura de un ISP y la otra tiene acceso a la infraestructura de otro ISP, el servicio se denominará single Multihomed, esto es solo una interfaz a cada ISP sin importar si se ocupan uno o dos equipos CE. Dual multihomed se llamará el tipo de solución que tiene dos conexiones a cada ISP.
- Se debe segmentar el tráfico LAN para que un porcentaje se mande por un acceso WAN y el resto del porcentaje se mande por la segunda interfaz WAN. En caso de falla de cualquiera de los dos accesos, el 100% del tráfico deberá ser procesado por uno solo de los accesos hasta la solución del problema. Por lo tanto, en este esquema los accesos WAN son respaldo uno del otro.

- En caso de existir doble conexión hacia la LAN, se deberá implementar VRRP o similares como HSRP para que la conmutación de salida de tráfico en caso de falla en el servicio que brinda el CE principal, sea imperceptible para los hosts de la red LAN.

1.6.- REDES PRIVADAS Y ANUNCIOS A INTERNET

Las redes privadas o intranet, no son alcanzables desde fuera de la organización como por ejemplo desde internet e incluso es posible que desde estas redes tampoco sean alcanzables nodos o servicios fuera de la misma organización. En este tipo de redes se maneja el tráfico de importancia para la organización dueña de la red como pueden ser, videos de cámaras de seguridad, telefonía IP, administración de inventarios, información financiera de la empresa, datos de clientes, etc.

El hecho de que la información que se maneja en estas redes es de ámbito privado para la empresa, permite que los dispositivos que se conectan a ella no necesariamente requieran una dirección IP pública, por lo que las redes privadas basadas en IPv4 implementan esquemas de direccionamiento privado descrito en el RFC 1918. Las redes privadas no pueden ser anunciadas en internet, por lo tanto, no es posible realizar conexiones entre redes privadas a través de internet, esto permite que diferentes organizaciones puedan ocupar el mismo direccionamiento dejando cada red aislada una de otra.

Las redes empresariales no necesariamente deben estar estructuradas como una red LAN donde todos los usuarios tienen acceso a toda la red. El número de equipos existente en la red, la necesidad de restringir la visibilidad de los dispositivos o mejorar la eficiencia de la red, son motivos para la creación de diferentes subredes (dominios de broadcast), necesitando por lo tanto el uso de routers que encaminen el tráfico entre las distintas subredes.

Los nodos de la red que necesiten conectividad directa con internet, deberán tener una dirección IP pública, esta IP debe ser asignada por el RIR, NIR o ISP correspondiente. Si la comunicación a internet solo es en sentido del host de la red privada hacia el servicio de internet, se puede ocupar en el host una dirección privada y realizar un cambio de esta IP a una pública mediante la técnica de traducción de direcciones de red NAT (Network Address Translation) permitiendo ahorros de direcciones públicas.

La organización dueña de la red privada, puede contratar los servicios de un ISP para tener acceso a internet, en caso de que se realice NAT a los hosts de la red, puede tener solo una IP pública en cada interfaz WAN del router que funge como CE, y todas las solicitudes hacia internet tendrán como origen la IP pública de esa interfaz.

El ISP deberá tener asignado el direccionamiento público que renta a la organización en cuestión, por el RIR que le corresponde, así como anunciarlo a internet con el ASN que le pertenece.

1.6.1.- Sistema Autónomo AS y Número de Sistema Autónomo ASN.

El sistema autónomo AS (Autonumus System) también llamado dominio de enrutamiento es un conjunto de dispositivos bajo una administración única. El hecho de tener una administración única, permite que existan dentro de un mismo sistema autónomo grupos de redes IP que poseen una política de rutas propia e independiente de otra administración.

Cada Sistema Autónomo tiene un número asociado el cual es usado como un identificador para el Sistema Autónomo en el intercambio de información del ruteo externo.

Internet es la unión de redes privadas. Una red que se une a internet se identifica por medio de su número se sistema autónomo ASN, este es único dentro de internet y el control de asignación de ASN está a cargo de IANA.

Los números de sistemas autónomos de 16 bits fueron definidos en la RFC 1930 y se utilizará para su identificación números enteros del 0 al 65535. Igualmente, los números de sistemas autónomos de 32 bits fueron definidos por la RFC 4893 y se utilizarán para su identificación números enteros del 0 al 4294967295. Utilizando en ambos casos la representación textual del valor decimal “asplain” definida en el RFC 5396.

Número de AS/bloque	asignación
0	Reservado
1-48127	Asignado
48128-54271	Sin asignar
54272-64511	Reservado por IANA
64512-65534	Libre para uso interno (*private range*)
65535	Reservado

Tabla 1.6: Tipos de ASN de 16 bits

Número de AS/bloque	asignación
0.0-0.65535	Antiguos ASN de 16 bits
1.0-1.65535	reservado
2.0-2.1023	Asignado a APNIC
2.1024-2.65535	Sin asignar
3.0-3.1023	Asignado a RIPE NCC
3.1024-3.65535	Sin asignar
4.0-4.1023	Asignado a LACNIC
4.1024-4.65535	Sin asignar
5.0-5.1023	Asignado a AfriNIC
5.1024-5.65535	Sin asignar
6.0-6.1023	Asignado a ARIN
6.1024-65535.65534	Sin asignar
65535.65535	reservado

Tabla 1.7: Tipos de ASN de 32 bits

Cada AS realiza su propia gestión de tráfico que fluye entre él y los otros sistemas autónomos que forman internet. Para que exista la comunicación entre redes pertenecientes a diferentes AS es necesario la implementación de un protocolo de ruteo del tipo EGP que una todos estos AS.

2. Enrutamiento

Para establecer comunicación entre dispositivos alojados en redes diferentes es necesario acudir a un dispositivo de capa 3, típicamente un router. Cada interfaz del router estará conectada a una red diferente, y está en capacidad de conmutar tráfico entre redes.

Para que un dispositivo de capa tres pueda determinar la ruta hacia un destino, debe conocer todas las rutas hacia el destino y cómo hacerlo. El aprendizaje y la determinación de estas rutas se lleva a cabo mediante un proceso de enrutamiento dinámico utilizando cálculos y algoritmos que se ejecutan en la red o mediante enrutamiento estático ejecutado manualmente por el administrador o incluso se pueden usar ambos métodos.

La información de enrutamiento que el router aprende desde sus fuentes se almacena en una base de datos llamada tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino.

La tabla de enrutamiento se construye a partir de estos dos métodos o ambos:

- Estáticamente.
  Las rutas estáticas son definidas por el Administrador. Las modificaciones necesarias al realizarse un cambio en la red son responsabilidad del Administrador.
- Dinámicamente.
  Utilizando protocolos de enrutamiento dinámico. El mantenimiento de la información de enrutamiento se realiza utilizando actualizaciones que se realizan de modo automático al generarse cambios en la red.

La tabla de enrutamiento contiene la información correspondiente a todos los destinos posibles conocidos, e incluye como mínimo para poder enrutar paquetes de información:

- **Dirección destino**: dirección a donde han de ser enviados los paquetes.
- **Fuentes de información**: fuente (otros routers) de donde el router aprende las rutas hacia los destinos especificados.
- **Descubrir las posibles rutas hacia el destino**: rutas iniciales posibles hasta los destinos deseados.

- **Seleccionar la mejor ruta**: determinar cuál es la mejor ruta hasta el destino especificado.
- **Mantener la tabla de enrutamiento actualizada**: mantener conocimiento actualizado de las rutas al destino.

El router al utilizar la información de la tabla de enrutamiento y la dirección IP de destino del paquete, determina hacia dónde se debe reenviar el tráfico.

Todas las redes directamente conectadas se agregan automáticamente a la tabla de enrutamiento en el momento en que la interfaz asociada a esa red alcanza estado operativo. Cuando la red de destino no está directamente conectada al dispositivo, la tabla de enrutamiento indica a cuál de los dispositivos directamente conectados (próximo salto) se debe enviar el paquete para que alcance el destino final. Si el dispositivo no tiene una entrada en la tabla de enrutamiento para el destino que se busca, el paquete es descartado y se envía un mensaje ICMP al origen.

Las rutas que generan una tabla de ruteo pueden ser de los siguientes tipos

1) Redes directamente conectadas.

   El origen de la información es el segmento de red directamente conectado a las interfaces del dispositivo y genera 2 entradas en la tabla de enrutamiento: una a la dirección IP de la interfaz (es una ruta /32 también llamadas rutas locales) y otra a la red o subred con la máscara de subred correspondiente. Si la interfaz deja de ser operativa, ambas redes son removidas de la tabla de enrutamiento. Su distancia administrativa es 0 y son preferidas a cualquier otra ruta.

2) Rutas estáticas.

   Son ingresadas manualmente por el Administrador de la red. Su distancia administrativa por defecto es 1. Son un método efectivo de adquisición de información de enrutamiento para redes pequeñas y simples que no experimentan cambios frecuentes.

3) Rutas dinámicas.

   Son rutas aprendidas automáticamente a través del intercambio de información con dispositivos vecinos generados por los protocolos de enrutamiento. Estas rutas se modifican automáticamente en respuesta a cambios en la red. Su distancia administrativa por defecto dependerá del protocolo dinámico que se implemente.

4) Ruta por defecto.

   Es una entrada opcional en la tabla de enrutamiento que se utiliza cuando no hay una ruta explícita hacia la red de destino.

La tabla de enrutamiento la construye un router utilizando un algoritmo para seleccionar la mejor ruta a los destinos conocidos considerando la distancia administrativa, la métrica y la longitud del prefijo.

2.1.- Distancia Administrativa

Los routers son multiprotocolo, lo que quiere decir que pueden utilizar diferentes protocolos al mismo tiempo incluidas las rutas estáticas. Si 2 o más protocolos proporcionan la misma información de enrutamiento, se les debe otorgar un valor administrativo. La distancia administrativa permite que un protocolo tenga mayor prioridad sobre otro si su distancia administrativa es menor. Este valor viene por defecto, pero un administrador puede asignar otro valor si así lo determina.

El valor de la distancia administrativa varia de 0 a 255, este puede variar dependiendo del fabricante, para el caso de CISCO se especifican los valores asignados por defecto en la siguiente tabla.

Fuente de información de ruteo	Valor
Ruta a una red directamente conectada	0
Ruta estática	1
Ruta EBGP	20
Ruta OSPF	110
Ruta IS-IS	115
Ruta RIP	120
Ruta IBGP	200
Ruta inalcanzable	255

Tabla 2.1 Distancia administrativa

Si bien las rutas estáticas y cada protocolo de enrutamiento tienen asignada un valor de distancia administrativa por defecto, puede ocurrir que ese valor no sea la mejor opción para una red en particular. En este caso, la distancia administrativa de los diferentes protocolos puede ser ajustada permitiendo que cuando se implementan varios protocolos simultáneamente se pueda lograr que, por ejemplo, las rutas aprendidas por OSPF sean preferidas a las aprendidas de manera estática.

2.2.- Métrica

Es el parámetro generado por el algoritmo de enrutamiento para calificar cada ruta hacia una red de destino y que refleja la “distancia” existente entre el dispositivo y la red de destino.

Las métricas utilizadas por los protocolos de enrutamiento pueden calcularse basándose en una sola o múltiples características de la ruta. Cada protocolo de enrutamiento utiliza métricas diferentes.

- **Ancho de banda**: capacidad de datos del enlace.
- **Número de saltos**: número de routers por los que pasará un paquete para llegar a una red destino.
- **Retraso (delay)**: Tiempo en mover un paquete de un origen a un destino.
- **Costo**: valor arbitrario que puede ser asignado por el administrador o calculado por alguna fórmula.
- **Sistema autónomo**: Cantidad de sistemas autónomos que se deben atravesar para llegar al destino.

Los valores de la métrica y la distancia administrativa pueden verse en la tabla de enrutamiento encerrados entre corchetes. El primero hace referencia a la distancia administrativa y el segundo a la métrica.

El ejemplo se basa en una topología BGP, donde el primero de los valores corresponde a la distancia administrativa (20) y el segundo a la métrica (0).

```
Gateway of last resort is 10.0.0.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.0.0.2, 00:11:18, GigabitEthernet2/0
      4.0.0.0/24 is subnetted, 1 subnets
O E2     4.2.2.0 [110/10] via 10.0.0.2, 00:11:18, GigabitEthernet2/0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.0.0/30 is directly connected, GigabitEthernet2/0
L        10.0.0.1/32 is directly connected, GigabitEthernet2/0
O        10.0.0.4/30 [110/2] via 10.0.0.10, 00:11:18, GigabitEthernet1/0
C        10.0.0.8/30 is directly connected, GigabitEthernet1/0
L        10.0.0.9/32 is directly connected, GigabitEthernet1/0
O        10.0.0.12/30 [110/2] via 10.0.0.2, 00:11:18, GigabitEthernet2/0
      87.0.0.0/30 is subnetted, 1 subnets
O        87.100.0.0 [110/2] via 10.0.0.2, 00:11:18, GigabitEthernet2/0
      200.36.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.36.0.0/30 is directly connected, GigabitEthernet0/0
L        200.36.0.1/32 is directly connected, GigabitEthernet0/0
      201.37.0.0/25 is subnetted, 2 subnets
B        201.37.0.0 [20/0] via 200.36.0.2, 00:11:22
B        201.37.0.128 [20/0] via 200.36.0.2, 00:11:22
```

Figura 2-1: Tabla de enrutamiento

2.3.- Longitud del prefijo

Es la longitud de la máscara de subred que caracteriza la red de destino de la ruta. Dado que es posible que en una misma tabla de enrutamiento convivan rutas a un destino específico y rutas sumarizadas, el algoritmo considera que la información más específica (mayor longitud de prefijo) es la más precisa. En este sentido si en la tabla de enrutamiento se tuvieran las rutas 172.168.0.0/16 y 172.16.20.0/24 y se requiere comunicación con el dispositivo que tiene la dirección IP 172.16.20.100, la decisión de reenvío que tomará el router será basada en la ruta 172.16.20.0/24 debido a que la máscara para esta red es más específica, sin embargo si el host que se desea alcanzar tiene la IP 172.16.2.10, la ruta que tomará el router es la indicada para la red 172.168.0.0/16 debido a que es la única ruta que se tiene para esa red.

2.4.- Enrutamiento estático

Una ruta estática es una ruta manualmente ingresada en la tabla de enrutamiento del dispositivo, establecen rutas específicas que han de seguir los paquetes

para pasar de un puerto de origen hasta un puerto de destino en un router, estas rutas establecen un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas se utilizan habitualmente en redes stub, ya que no existe más que una entrada y salida para la red interna, de esta manera se evita la sobrecarga de tráfico que genera un protocolo de enrutamiento dinámico.

En la figura siguiente se muestra una red stub donde solo existe una única salida hacia la infraestructura del ISP.

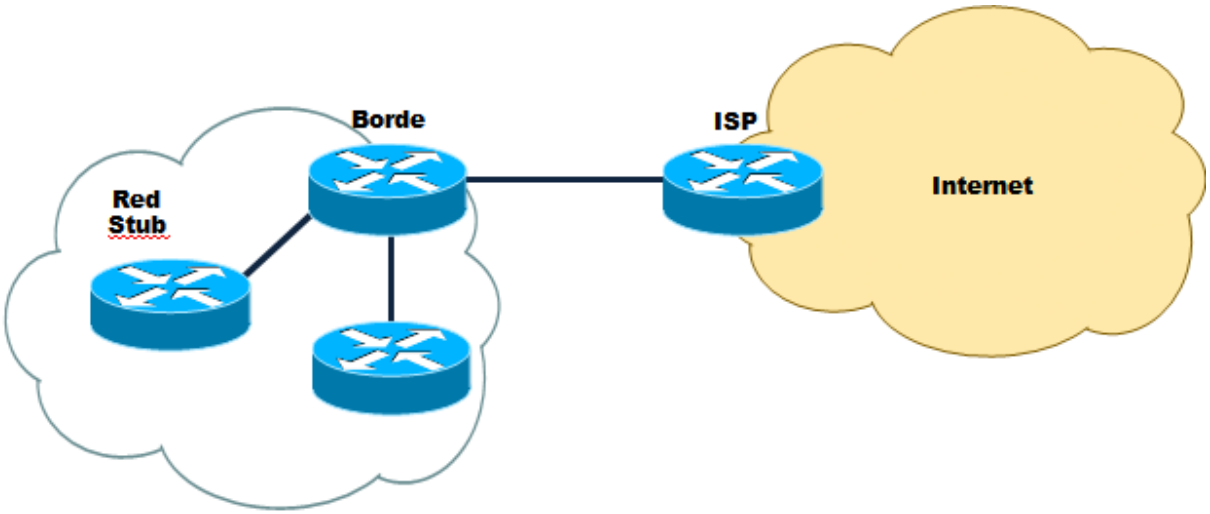

Figura 2-2: Red stub

La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo es necesario configurar la ruta en ambas direcciones, en la Figura 2-2 la ruta estática debe ser configurada en los routers ISP y Borde.

Existe una ruta estática especial llamada ruta por defecto o de último recurso, se utiliza cuando no existe en la tabla de enrutamiento una ruta hacia una red determinada o cuando no se puede almacenar en la tabla de enrutamiento la información relativa a todas las rutas posibles.

A continuación, se muestra un ejemplo de como aparece una ruta por defecto en la tabla de ruteo.

```
Gateway of last resort is 87.100.0.1 to network 0.0.0.0

     87.0.0.0/30 is subnetted, 1 subnets
C       87.100.0.0 is directly connected, GigabitEthernet2/0
     4.0.0.0/24 is subnetted, 1 subnets
B       4.2.2.0 [20/0] via 87.100.0.1, 00:01:22
     201.37.0.0/25 is subnetted, 2 subnets
O E2    201.37.0.128 [110/10] via 10.0.0.1, 00:00:37, GigabitEthernet1/0
O E2    201.37.0.0 [110/10] via 10.0.0.1, 00:00:37, GigabitEthernet1/0
     10.0.0.0/30 is subnetted, 4 subnets
O       10.0.0.8 [110/2] via 10.0.0.1, 00:00:37, GigabitEthernet1/0
C       10.0.0.12 is directly connected, GigabitEthernet0/0
C       10.0.0.0 is directly connected, GigabitEthernet1/0
O       10.0.0.4 [110/2] via 10.0.0.14, 00:00:37, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 87.100.0.1
```

Figura 2-3: Ruta por defecto

Esta información de enrutamiento requiere ser mantenida manualmente por el Administrador de la red lo cual representa ventajas y desventajas respecto de la utilización de protocolos de enrutamiento dinámico que se enlistan en la tabla siguiente.

Ventajas	Desventajas
No genera carga de procesamiento.	El Administrador debe tener una comprensión amplia de la red.
No utiliza ancho de banda.	El Administrador debe agregar manualmente la ruta hacia cada red.
Son más seguras.	La actualización de rutas puede convertirse en un trabajo full-time.
Fácil diagnóstico.	Requiere alto mantenimiento y no tiene adaptabilidad a los cambios.

Tabla 2.2: Tabla comparativa de ventajas y desventajas del ruteo estático

2.5.- Enrutamiento dinámico.

Los cambios que una red puede experimentar hacen poco factible la utilización de rutas estáticas, el administrador se vería forzado a reconfigurar los routers ante cada cambio. El enrutamiento dinámico permite que los routers actualicen las tablas de ruteo ante posibles cambios sin tener que recurrir a nuevas configuraciones.

En la tabla siguiente se mencionan las ventajas y desventajas que tiene el uso de protocolos de enrutamiento dinámico.

Ventajas	Desventajas
Alto grado de adaptabilidad a los cambios.	Requieren cantidades significativas de procesamiento y memoria RAM.
Requiere muy poco mantenimiento.	Utiliza ancho de banda para el intercambio de información.

Tabla 2.3: Ventajas y desventajas del enrutamiento dinámico

Existen dos grandes núcleos de protocolos de enrutamiento el primero es el protocolo de Gateway interior (IGP) ocupado para intercambiar información de enrutamiento dentro de un sistema autónomo, y el segundo es el protocolo de Gateway exterior (EGP) ocupado para intercambiar información de enrutamiento entre sistemas autónomos.

2.5.1.- Protocolos de enrutamiento por vector distancia

Este tipo de protocolos basa su operación en el envío a los dispositivos vecinos la información contenida en la tabla de enrutamiento, el equipo vecino formará su propia tabla de enrutamiento basado la información que reciba de sus vecinos. El envío de datos se hace en intervalos fijos de tiempo aun cuando no haya cambios en la red, este envío de información permite que las tablas de enrutamiento se mantengan actualizadas.

El dispositivo que recibe una actualización, compara la información recibida con la contenida en la propia tabla de enrutamiento tomando las siguientes consideraciones:

- Para establecer la métrica se toma la métrica recibida en la actualización y se le agrega la que existe entre él y su vecino.
- Si la ruta aprendida es mejor (menor métrica) que la contenida en la tabla de enrutamiento hasta ese momento, se actualiza la tabla de enrutamiento con la nueva información, en caso contrario la nueva ruta es descartada.

Existen eventos que pueden generar cambios en la tabla de enrutamiento sin esperar las actualizaciones, estos pueden ser, la falla de un enlace, la introducción de un nuevo enlace, la falla de un dispositivo o el cambio de los parámetros de un enlace.

Los protocolos de enrutamiento dinámico son sensibles a la posibilidad de generación de bucles de enrutamiento en redes complejas. Un bucle de enrutamiento es una condición por la cual un paquete se transmite ininterrumpidamente a través de una serie definida de dispositivos sin que logre alcanzar la red de destino.

Para prevenir o solucionar este inconveniente, los protocolos vector distancia implementan varias herramientas como son:

- **Horizonte dividido**: La regla que se establece es que una ruta no será anunciada por el mismo puerto donde fue aprendida.
- **Métrica máxima**: Un protocolo de enrutamiento permite la repetición del bucle de enrutamiento hasta que la métrica exceda del valor máximo permitido. En el caso de RIP la métrica que considera es el número de saltos, y la métrica máxima son 15 saltos, por lo tanto, si un paquete excede los 15 saltos para llegar al destino será descartado.
- **Ruta envenenada**: En el envenenamiento se usa la métrica máxima para indicar que una red destino es inalcanzable. Consiste en crear una entrada en la tabla de enrutamiento en la que se guarda la información respecto de una ruta que está fuera de servicio (ruta envenenada), esperando que el resto de la red converja en la misma información. En esa entrada la red de destino es marcada como inalcanzable, y esa información se publica con las actualizaciones del protocolo hacia todos los dispositivos vecinos.
- **Temporizadores de espera**: Fuerzan a que el dispositivo retenga algunos cambios por un período de tiempo determinado, antes de incorporarlos en la tabla de enrutamiento. Previenen que los cambios se hagan con excesiva rapidez, permitiendo que una ruta caída vuelva a ser operativa dentro de un lapso de tiempo sin que haya habido cambios.

2.5.2.- Protocolos de enrutamiento por estado de enlace

Los protocolos de estado de enlace basan la construcción de la tabla de enrutamiento en una base de datos de la topología. La base de datos de la topología se elabora a partir de paquetes de estado de enlace que se pasan entre todos los routers para describir el estado de una red.

Los protocolos de enrutamiento por estado de enlace recopilan la información necesaria de todos los routers de la red, cada uno de los routers calcula la mejor ruta hacia un destino de manera independiente a los demás routers de la red. De esta manera se producen muy pocos errores al tener una visión completa de la red por cada router.

Cuando se produce un fallo en la red el router que detecta el error utiliza una dirección multicast para enviar un mensaje acerca del error a los demás routers, que reciben y reenvían el mensaje a sus vecinos sin alterarlo. Las actualizaciones de rutas no se realizan de manera periódica, se realizan solo cuando existe un cambio en la red.

Los protocolos de estado de enlace son más rápidos y escalables que los de vector distancia, una de las razones es que los protocolos de estado de enlace solo envían actualizaciones cuando existen cambios en la topología no de manera periódica.

2.6.- Protocolo de Información de Enrutamiento (RIP)

RIP (Routing Information Protocol) Es uno de los protocolos de enrutamiento más antiguos utilizados por dispositivos basados por IP. Es un protocolo vector distancia que utiliza la cuenta de saltos como métrica. La cuenta de saltos máxima de RIP es 15 por lo tanto, cualquier ruta que exceda los 15 saltos se etiqueta como inalcanzable al establecer la cuenta de saltos en 16.

Existen dos versiones del protocolo llamas RIPv1 y RIPv2. RIPv1 es un protocolo de enrutamiento con clase que no admite la publicación de la información de la máscara de red. La versión 2 de RIP es un protocolo de enrutamiento sin clase que admite CIDR, VLSM y seguridad mediante texto simple y autenticación MD5.

Algunas características comparativas entre RIPv1 y RIPv2 se muestran en la tabla siguiente.

RIPv1	RIPv2
La métrica es el número de salto	La métrica es el número de salto
La métrica máxima es 15 saltos	La métrica máxima es 15 saltos
Por defecto actualiza la tabla de enrutamiento cada 30 segundos	Por defecto actualiza la tabla de enrutamiento cada 30 segundos
Es basado en clases	No se basa en clases por lo que soporta CIDR y VLSM
No permite el cifrado de paquetes	Puede cifrar los paquetes RIP con MD5

Tabla 2.4: Comparativa entre RIPv1 y RIPv2

2.7.- Protocolo de Abrir el Camino Más Corto Primero OSPF

OSPF (Open Shortest Path First) fue creado a finales de los ochentas para cubrir las necesidades de las grandes redes IP que otros protocolos como RIP no podían soportar incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de rutas de multidifusión. OSPF es especificado en el RFC2328.

OSPF funciona dividiendo una intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de las áreas se enlazan a un área de backbone mediante un router fronterizo. Todos los paquetes enviados desde una dirección de una estación de trabajo de un área a otra de un área diferente, atraviesan el área de backbone, independientemente de la existencia de una conexión directa entre las 2 áreas.

OSPF es un protocolo de enrutamiento por estado de enlace que a diferencia de RIP publican sus rutas solo a los routers vecinos. Los routers OSPF envían publicaciones de estado de enlace LSA (Link State Advertisement) a todos los routers pertenecientes de la misma área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo SFP (Shortest Path First), también conocido con el nombre de su creador Dijkstra, para calcular la ruta más corta a cada nodo.

Para determinar que interfaces reciben las publicaciones de estado de enlace los routers envían paquetes hello. Con los mensajes hello, un router determina que otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers.

Cuando se detecta u router vecino, se intercambian información de OSPF, cuando los routers están sincronizados se dice que han formado una adyacencia.

La métrica utilizada por OSPF es el **costo**, la fórmula para calcular el costo es:

Costo= 10^8 bps / Velocidad del enlace.

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

Todas las actualizaciones de OSPF se basan en tres tablas que deben mantenerse actualizadas:

- **Tabla de vecinos**: contiene la información de los vecinos con cuáles se realizan intercambios OSPF.
- **Tabla topológica**: mantiene una base de datos de todas las LSA recibidas de toda la red.
- **Tabla de enrutamiento**: contiene la información necesaria para alcanzar una red destino.

Los protocolos de estado de enlace anuncian una lista de todas sus conexiones, cuando un enlace se cae, el router OSPF que detecta esa caída envía LSA que son compartidas por los vecinos como así también una base topológica LSDB (Link State Database). Las LSA se identifican con un número de secuencia para reconocer la más recientes en un rango que va de 0x8000 0001 a 0xFFFF FFFF. Cuando los routers convergen tienen la misma LSDB a partir de ese momento SFP es capaz de determinar la mejor ruta hacia el destino. La tabla topológica es la visión que tiene el

router de la red dentro del área en que se encuentra incluyendo además todos los routers.

La tabla topológica se actualiza por cada LSA que envía cada uno de los routers dentro de una misma área, todos estos routers tienen la misma base de datos, las inconsistencias en ellas pueden ocasionar bucles y es el propio router el encargado de avisar que ha habido algún cambio e informar del mismo. Los routers que reciben una actualización de la tabla topológica, analizan la siguiente información y para tomar la decisión de si actualizar su tabla o no:

- Si la LSA es más reciente se añade a la base de datos, se reenvían a todos sus vecinos para que actualicen sus ases y SFP empieza a funcionar.
- Si el número de secuencia es el mismo que el router ya tiene registrado en la base de datos, ignorará esta actualización.
- Si el número de secuencia es menor al que tiene registrado, el router enviará la versión nueva al que envío la anterior, de esta forma se asegura que todos los routers tengan la misma versión.

OSPF establece relaciones con otros routers mediante el intercambio de mensajes hello. Luego del intercambio de estos mensajes, los routers elaboran sus tablas de vecinos, que lista todos los routers que están utilizando OSPF y están directamente conectados, los paquetes hello se envían a la dirección múlticast 224.0.0.5, en redes tipo broadcast con una frecuencia de 10 segundos mientras en redes de acceso múltiple sin broadcast NBMA (No Broadcast MultiAccess networks) es de 30 segundos.

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

Una vez lograda la adyacencia (estafo FULL), las tablas deben mantenerse actualizadas, las LSA son enviadas cuando exista un cambio o cada 30 minutos. La siguiente lista describe los estados de una relación de vecindad:

- DOWN: es el primer estado de OSPF y significa que no se ha escuchado ningún vecino.
- ATTEMPT: este estado es únicamente para redes NBMA, durante este estado, el router envía paquetes hello del tipo unicast hacia el vecino, aunque no se haya recibido un paquete hello del vecino.
- INIT: se ha recibido un paquete hello de un vecino, pero el ID del router no está listado en ese paquete.
- 2-WAY: se ha establecido una comunicación bidireccional entre dos roiters, ambos han recibido el paquete hello del vecino.
- EXSTART: una vez elegido el DR y BDR, el verdadero proceso de intercambiar información del estado de enlace, se hace entre los routers y su DR y BDR.
- EXCHANGE: en este estado los routers intercambian la información de la base de datos.
- LOADING: es en este estado cuando se produce el verdadero intercambio de información del estado de enlace.
- FULL: finalmente los routers son totalmente adyacentes, se intercambian las LSA y las bases de datos están actualizadas.

Los paquetes hello se siguen enviando periódicamente para mantener las adyacencias, en el caso de que no se reciba se dará por perdida dicha adyacencia. Tan pronto como OSPF detecta un 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.

Cuando varios routers están conectados a un mismo segmento de red del tipo broadcast, uno de esos routers tomará el control y mantendrá las adyacencias entre todos los routers del segmento. Este router tomará el nombre de router designado DR (Designate Router) y será elegido a través de la información que contienen los mensajes hello. Para una eficaz redundancia, también se elige un router designado de reserva BDR (Backup Designate Router). Los DR y BDR son creados en redes

multiacceso debido a que el número de adyacencias incrementaría significativamente la cantidad de tráfico en la red.

La elección de un DR y un BDR se basa en los siguientes requisitos:

- El router con el valor de prioridad más alto es el DR.
- El router con el segundo valor de prioridad más alto es el BDR.
- El valor de prioridad de un router es 1, en caso de que la prioridad sea la misma, se usa el ID del router. Un router con prioridad 0 no es elegible.
- ID del router. Este número de 32 bits identifica únicamente al router dentro de un sistema autónomo. Puede tener formato de una IPv4 o decimal

La capacidad de OSPF para separar una gran red en diferentes áreas más pequeñas se denomina enrutamiento jerárquico. Este enrutamiento permite dividir un AS en redes más pequeñas llamadas áreas que se conectan al área 0 o de backbone. Las actualizaciones de enrutamiento interno, se producen dentro de cada área. Es decir que si una interfaz se torna inestable el recalculo se distribuye en su área sin afectar al resto.

Las actualizaciones de estado de enlace LSU (Link State Update), pueden publicar rutas resumidas entre áreas, haciendo más selectivo y eficaz el enrutamiento dinámico.

La división en áreas hace que el desempeño de la red mejore notablemente, los routers dentro de este modelo jerárquico tienen diferentes responsabilidades y son llamados de diferente manera según la función que realicen:

- Internal Router: es el responsable de mantener una base de datos actualizada de cada una de las LSA dentro de cada área. Al mismo tiempo envía datos hacia otras redes empleando la ruta más corta. Todas las interfaces de este router están en la misma área.

- Backbone Router: las normas de diseño de OSPF requieren que todas las áreas 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 se encarga de la conexión entre 2 o más áreas, mantiene una tabla topológica de cada una de las áreas a las que pertenece y envía actualizaciones LSA a cada una de ellas.
- Autonomous System Boundary Router (ASBR): este router conecta hacia otros dominios de enrutamiento, normalmente ubicados dentro del área de backbone.

En el caso de que se deba configurar un área en un router que no tenga conectividad con el área 0, se puede hacer uso de los enlaces virtuales de OSPF o virtual link, creando un puente entre dos ABR para conectar de forma lógica el área remota con el área 0. De esta manera la información del área remota fluye a través del área intermedia o virtual. Desde el punto de vista de OSPF el ABR tiene una conexión directa con estas tres áreas.

En la figura siguiente se identifican los diferentes tipos de routers existentes en una red OSPF.

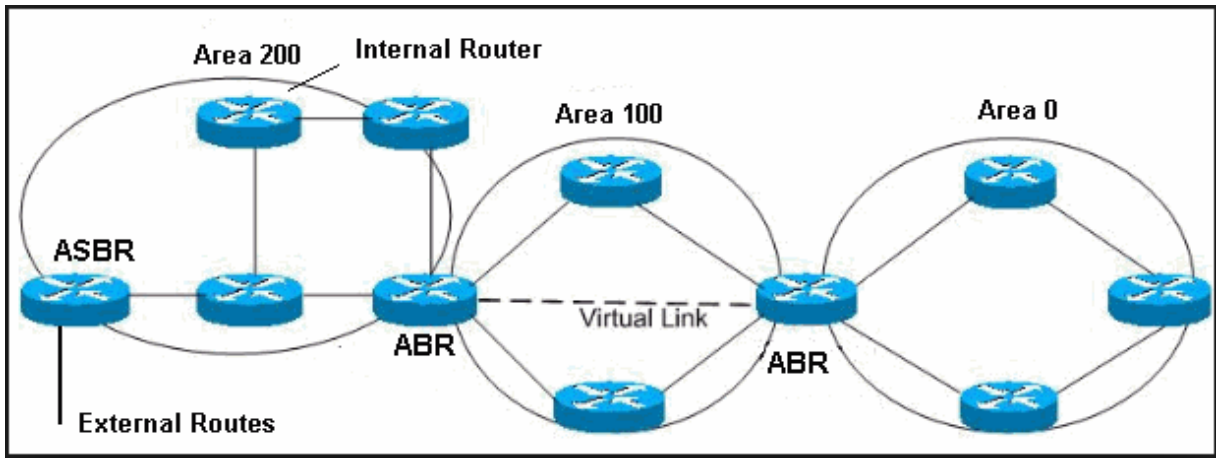

Figura 2-4: Topología OSPF

2.8.- Protocolo de puerta de enlace de frontera BGP

BGP (Border Gateway Protocol) es un protocolo de enrutamiento diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables entre las organizaciones. BGP soporta VLSM (Variable Length SubnetMask), CIDR (Classless Interdomain Routing) y sumarización de rutas.

El principal propósito de BGP es conectar grandes redes o sistemas autónomos, por esta razón su mayor uso está en internet y conexiones entre organizaciones que requieren conectividad de manera privada. Las grandes organizaciones utilizan BGP como el vínculo entre diferentes divisiones empresariales. BGP se utiliza en Internet para conectar diferentes organizaciones entre sí.

Es el único protocolo que actualmente soporta enrutamiento entre dominios. Los dispositivos, equipos y redes controlados por una organización son llamados sistemas autónomos, AS. Esto significa independencia, es decir, que cada organización es independiente de elegir la forma de conducir el tráfico y no se los puede forzar a cambiar dicho mecanismo. Por lo tanto, BGP comunica los AS con independencia de los sistemas que utilice cada organización.

Otro punto clave es que BGP pretende que las redes permanezcan despejadas de tráfico innecesario el mayor tiempo posible. Mientras que los IGP están buscando la última información y ajustando constantemente las rutas acordes con la nueva información que se recibe, BGP está diseñado para que las rutas sean estables y que no se estén advirtiendo e intercambiando constantemente. Las configuraciones de BGP requieren determinaciones de políticas, de modo que, dada la complejidad del protocolo y el inmenso tamaño de la tabla de enrutamiento, no se puede estar cambiando constantemente decisiones de enrutamiento haciendo que los routers estén constantemente sobrecargados.

Como ya se mencionó, BGP asocia redes con sistemas autónomos de tal manera que otros router envían tráfico hacia el destino a través de un sistema autónomo.

Cuando el tráfico llega a los routers frontera de BGP, es trabajo de los routers del IGP encontrar el mejor camino interno.

BGP es un protocolo path-vector, las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando y los bucles son evitados rechazando aquellas rutas que tienen el mismo número de sistema autónomo origen al cual están llegando.

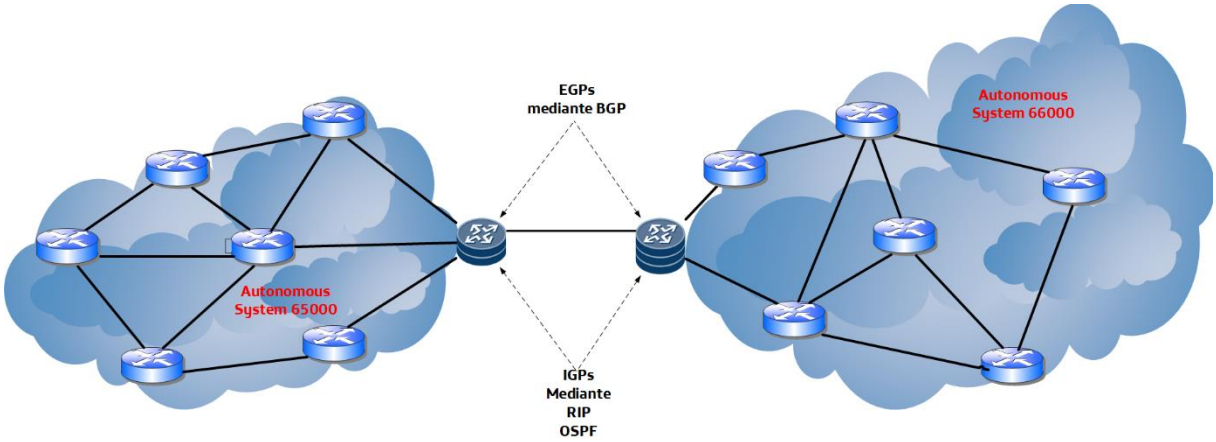

Figura 2-5: Entornos IGP y EGP

Los vecinos BGP son los llamados peers, éstos no son automáticamente descubiertos, sino que deben estar predefinidos. Existen cuatro tipos de mensajes en BGP para que la relación sea construida y posteriormente mantenida:

- Open.
- Keepalive
- Update
- Notification

Cuando el proceso de BGP comienza se crean y mantienen las conexiones entre los peers utilizando el puerto TCP 179 a través de mensajes BGP open, posteriormente las sesiones son mantenidas enviando constantemente mensajes keepalive y la información del peer se mantiene en una tabla de vecinos separada. Si un peer es reseteado, éste envía un mensaje de notificación para indicar la finalización de la relación. Cuando se establece por primera vez la relación de vecindad, los

routers BGP intercambian sus tablas de enrutamiento por completo utilizando mensajes update. Finalmente, sólo se enviarán actualizaciones incrementales cuando existan cambios en la red.

Debido a su complejidad y especialización para funciones externas, BGP

se utiliza para los siguientes casos:

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

BGP probablemente no sea necesario si algunos de los requerimientos anteriores no se cumplen. Si los requerimientos de enrutamiento que se necesitan pueden llevarse a cabo de una manera más simple, como por ejemplo con una ruta por defecto, no se debería estar pensar en BGP como solución. Los recursos necesarios para un buen funcionamiento de BGP son elevados, por lo tanto, otras opciones deben ser siempre analizadas antes de implementarlo, ahorrando de esta forma dinero en dispositivos y configuraciones complejas.

3. Anuncios a internet

BGP es el único protocolo del tipo EGP, es por esta razón que es utilizado para conectar hacia Internet las redes privadas, así como para enrutar tráfico dentro, de Internet manteniendo una ruta de AS. Es de suma importancia que los administradores de las redes privadas mantengan un control de los segmentos de red que se anuncian y se aprenden en internet para evitar en lo más posible errores humanos que pudieran afectar servicios a nivel internacional por alguna duplicidad de segmentos, para esto es recomendable que en las fronteras de internet se configuren filtros para permitir y negar segmentos de red. Se debe estar completamente seguro de que la cantidad de tráfico y rutas no saturará la red. Dos consideraciones importantes en el diseño de BGP son la necesidad de enlaces redundantes hacia Internet, llamados multihoming, y controlar cuánto tráfico de enrutamiento se quiere recibir desde Internet.

En organizaciones modernas la falta de conectividad a Internet puede llevar a la pérdida de conectividad a determinados servidores y páginas Web hasta la pérdida de telefonía IP. Internet contiene una cantidad enorme y variada de tráfico y de igual manera importante, es por lo tanto una tarea de los administradores poseer una solución a la falta de conectividad hacia Internet. Las conexiones redundantes son la solución a la pérdida de un enlace. Esta solución es conocida como multihoming.

La idea del funcionamiento de multihoming es que ante el fallo de un enlace active un segundo enlace hacia Internet. Si estos dos enlaces pueden estar activos a la vez proporcionará una mayor efectividad en la conexión a Internet, mayor rendimiento y redundancia. El balanceo de carga en BGP a través de múltiples enlaces o diferentes AS son las políticas de configuración del protocolo.

Multihoming podría efectuar múltiples conexiones al mismo ISP o a ISP diferentes. Conectado a más de un ISP puede generar algunos de los siguientes problemas:

1) El espacio de direccionamiento es advertido de forma incorrecta por el proveedor.

2) Las rutas que se advierten o las rutas externas de las que depende la red son advertidas con diferentes máscaras. Debido a que las más específicas serán siempre utilizadas, no se tendrán en cuenta los atributos de BGP.
3) Cuando la conexión es a más de un ISP, el AS puede llegar a ser un sistema autónomo de tránsito entre esos ISP. Esto es rechazado debido a que no es conveniente que el AS tenga tráfico ajeno al propio sistema autónomo.

Generalmente el ISP es capaz de tratar con este tipo de problemas y configurará su red para protegerse, aun así, no se puede confiar plenamente en que su parte esté bien configurada. También es importante el contacto entre los dos ISP implicados para que puedan planificar los cambios necesarios.

Al conectarse a Internet es necesario planificar qué actualizaciones serán enviadas y recibidas desde el mundo exterior.

Existen tres formas de conectarse a Internet:

1) Aceptar sólo rutas por defecto desde todos los ISP. En este caso los consumos de recursos serán muy bajos y la selección de rutas se hará utilizando el router BGP más cercano.
2) Aceptar algunas rutas más las rutas por defecto desde los ISP. En este caso el consumo de recursos de memoria y CPU será medio. El router seleccionará la ruta específica y si no la conoce lo hará a través del router BGP más cercano.
3) Aceptar todas las rutas desde todos los ISP, en este caso el consumo de recursos es alto, pero en contra posición siempre se elegirá la ruta más directa.

Cuando un AS proporciona un sistema de tránsito para otros AS y tiene router que no son BGP, el tráfico de tránsito podría ser descartado si los routers intermediarios que no ejecutan BGP desconocen esas rutas. La regla de BGP de sincronización dice que, si un sistema autónomo proporciona un servicio de tránsito a otro sistema autónomo, BGP no debería anunciar más rutas hasta que todos los routers dentro de ese AS hayan aprendido acerca de esa ruta vía un IGP.

La figura siguiente muestra un ejemplo de la sincronización.

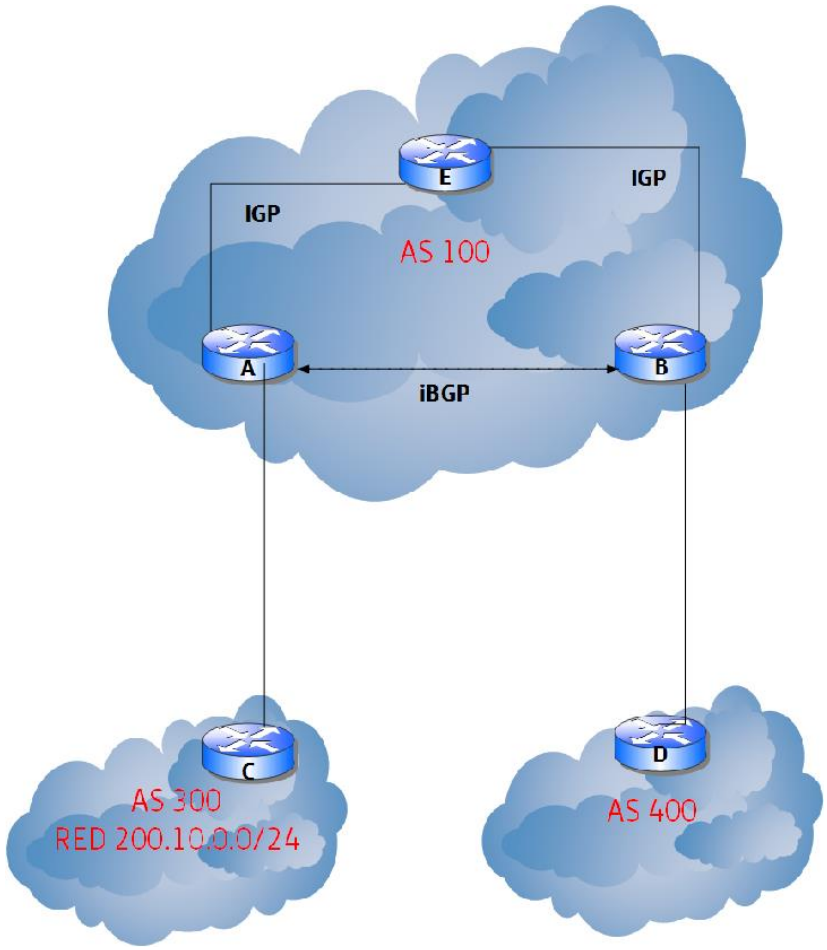

Figura 3-1: Sincronización en BGP

El router C envía actualizaciones acerca de la ruta 200.10.0.0/24 hacia el router A; el router A y el router B están ejecutando iBGP (Internal BGP). El router B recibe actualizaciones acerca de la red 200.10.0.0/24 vía iBGP, si el router B quiere alcanzar la red 200.10.0.0, enviará el tráfico hacia el router E. Si el router A no redistribuye la red 200.10.0.0 dentro de un IGP, el router E desconoce que la ruta 200.10.0.0 existe, por lo tanto, descartará los paquetes. Si el router B advierte al AS 400 que puede alcanzar dicha red antes de que el router E aprenda sobre dicha red vía un IGP, el tráfico que viene desde el router D hacia el router B con destino 200.10.0.0 pasará por el router E y será descartado.

Esta situación es controlada con la regla de sincronización de BGP, la cual dice que un sistema autónomo, en este caso ÁS 100, pasa tráfico desde un AS hacia otro y no advertirá una ruta antes de que todos los routers dentro del AS 100 hayan aprendido esa ruta vía un IGP. En este caso el router B espera hasta aprender sobre la red 200.10.0.0 vía un IGP antes de enviar las actualizaciones al router D. Hay casos en los que es preferible deshabilitar la sincronización permitiendo que BGP converja más rápidamente, pero en estos casos pueden producirse pérdidas de paquetes.

Si algunas de las siguientes condiciones se cumplen es posible que sea necesario deshabilitar la sincronización:

a) El sistema autónomo no pasa tráfico entre sistemas autónomos.
b) Todos los routers de tránsito ejecutan BGP.

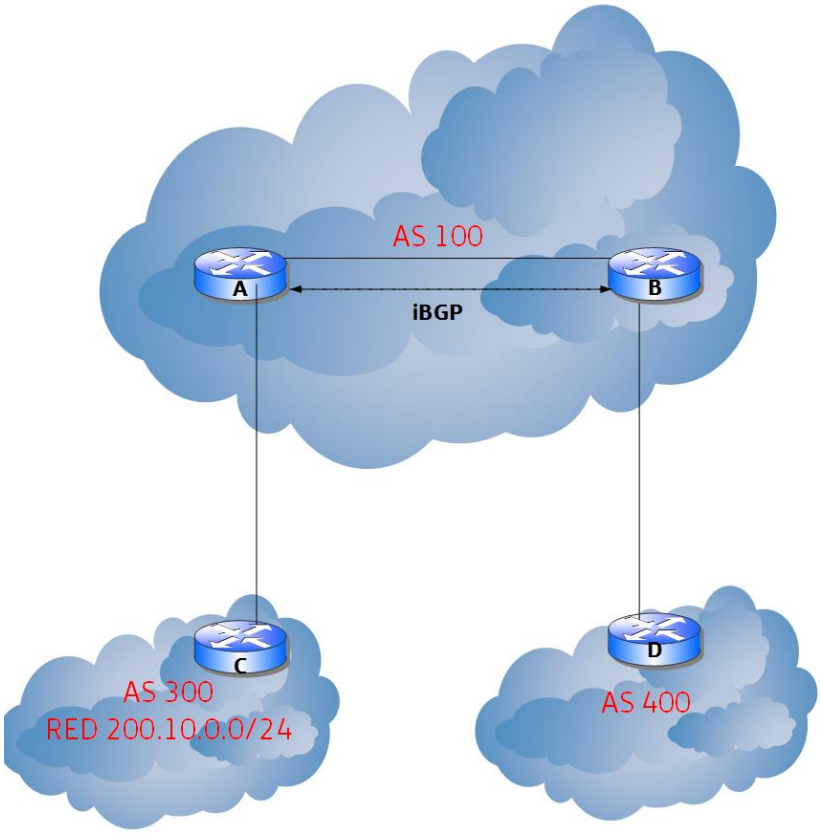

Figura 3-2: Escenario donde no es necesaria la sincronización de BGP

Los estados que puede tomar una sesión de BGP son los siguientes:

- **Idle**: durante este estado el router está buscando a los vecinos, técnicamente BGP espera una fase llamada start. Este evento puede ser iniciado por un administrador o por el sistema BGP. Un administrador estableciendo una sesión BGP o reseteando una sesión que ya existe causa un evento start.
- **Connect**: BGP espera que se complete la conexión del protocolo de transporte, en este caso TCP puerto 179. Si la conexión de TCP se realiza satisfactoriamente, el estado pasa a la fase open sent. En el caso de que no sea satisfactoria el estado cambiará a active.
- **Active**: intenta establecer una vecindad iniciando la conexión a través del protocolo de transporte. En caso de que lo consiga pasará al siguiente estado, open sent. Cuando el temporizador connect retray expira BGP lo reinicia y vuelve al estado connect. Si un router permanece entre los estados connect y active revela que la conexión TCP no se puede establecer. El estado active indica que el router está intentando iniciar la sesión TCP.
- **Open Sent**: en este estado BGP espera los mensajes open del vecino, estos mensajes son chequeados para verificar que los datos son correctos, que las versiones de BGP sean las debidas como así también el número del sistema autónomo.
- **Open Confirm**: BGP espera los mensajes keepalive, si recibe estos mensajes de su vecino entonces la sesión pasa al siguiente estado.
- **Established**: es el estado final y el necesario para que BGP comience a funcionar, hay intercambio de rutas, actualizaciones y keepalives.

Los vecinos de BGP interno no tienen que estar directamente conectados, normalmente un IGP es responsable del enrutamiento dentro del AS de tal forma que los routers que ejecutan BGP pueden alcanzarse mutuamente a través del enrutamiento proporcionado por el IGP.

En la siguiente figura, el router A tiene varias direcciones IP. Los routers A y B forman adyacencia y se encuentran directamente conectados por medio de la red 10.0.0/30, pero si el enlace se cae la interfaz del router B dejaría de responder, incluso cuando el router B está directamente conectado al router C, no sabría que hacer debido a que la dirección configurada para el peer esta caída.

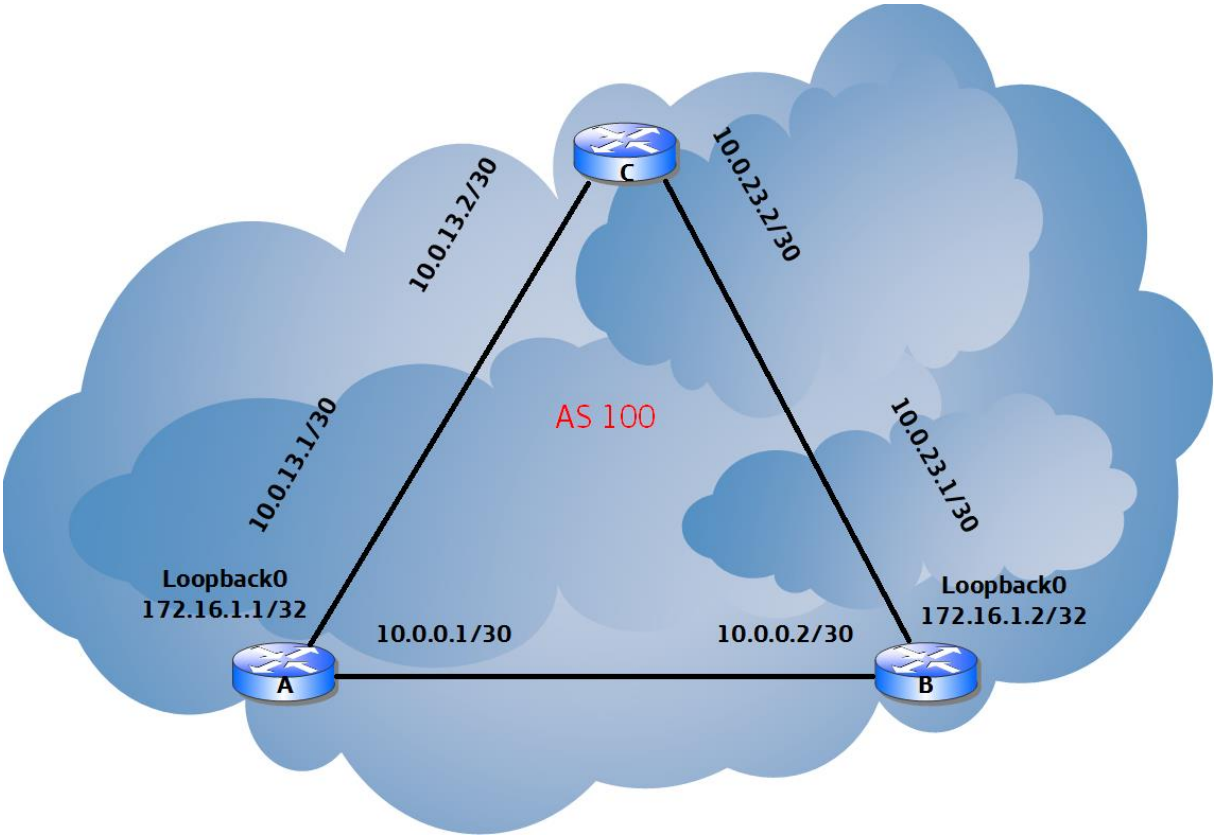

Figura 3-3: Conexión iBGP

Sin embargo, si el peering se establece mediante direcciones de loopback el problema puede solventarse porque a pesar de que el enlace podría caerse, el router B enviará el tráfico a través del router C. Para la configuración de este ejemplo hay que tener en cuenta que se han utilizado las dicciones de loopback en el IGP.

Otro problema que surge es que cuando BGP crea tráfico la dirección IP de origen es la de la interfaz de salida, en el router B el tráfico hacia el router A tomaría el camino directo desde la interfaz 172.16.1.2, pero si el enlace falla el tráfico redireccionará

desde la dirección IP 175.16.3.1. Esta nueva dirección de origen no encaja con la definida como peer, por lo tanto, la conexión será rechazada. Para permitir caminos redundantes el vínculo de origen tiene que ser el mismo que el vecino espera.

Para el establecimiento de BGP se recomienda que Ambos routers establezcan el peering hacia las direcciones de loopback de sus vecinos y originen tráfico desde sus propias loopback permitiendo de esa manera la redundancia.

Los routers BGP externos normalmente no utilizan ningún protocolo de enrutamiento haciendo peering con direcciones directamente conectadas. Por defecto los paquetes eBGP poseen un valor de TTL igual a uno, lo que previene que puedan viajar a más de un salto. Sería posible crear un modelo de redundancia en el ejemplo anterior, pero es necesario que se cumplan las siguientes condiciones:

- Tiene que existir una ruta hacia ambas direcciones por donde se establecerá el peer.
- Debe ajustarse el TTL para que sea capaz de atravesar el número necesario de saltos.

3.1.- Atributos BGP

Las rutas aprendidas vía BGP llevan asociados ciertos atributos que sirven para determinar qué rutas son la mejor opción hacia un destino y si existen varios caminos hacia ese destino en particular. Para diseñar redes robustas con BGP hay que comprender cómo los atributos de BGP influyen en el proceso de selección de rutas.

Es posible que BGP pueda recibir varios anuncios para la misma ruta desde diferentes orígenes. BGP solamente selecciona un camino como el más adecuado; una vez que dicho camino es seleccionado BGP lo pone en la tabla de enrutamiento y lo propaga a sus vecinos.

En la tabla siguiente se enlistan los atributos BGP soportados en IOS que se ocupan para determinar la mejor ruta a un destino.

Atributo	Categoría	Descripción
AS-PATH	Bien conocido y mandatorio.	Lista de todos los AS a través de los cuales ha pasado. Se prefiere el más corto.
Local preference	Bien Conocido opcional	Indica el nivel de preferencia para alcanzar prefijos externos a través de los routers internos. Se prefiere el valor más alto.
Múltiple Exit Discriminator (MED)	Bien Conocido Opcional	Indica a vecinos externos qué camino usar para alcanzar prefijos.
Weight	Propietario de CISCO Opcional	Propietario de Cisco. Se prefiere el más alto.

Tabla 3.1: Atributos BGP para determinar la mejor ruta

Los atributos de la siguiente tabla no son ocupados para determinar la mejor ruta a una red destino, pero también son considerados en el proceso de BGP.

Atributo	Categoría	Descripción
Aggregator	Opcional	ID y AS del router que lleva a cabo la sumarización. No se usa en el proceso de selección de caminos.
Atomic aggregate	Bien conocido, recomendado	Al generar una sumarización envía los AS de las rutas que componen dicha sumarización. No se usa en el proceso de selección de caminos.
Cluster ID	Opcional	Identifica un clúster, Route Reflectors. No se usa en el proceso de selección de caminos.
Community	Opcional	Etiqueta prefijos. No se usa en el proceso de selección de caminos.
Next Hop	Bien conocido y mandatorio.	Peer externo en el AS vecino. No se usa en el proceso de selección de caminos.
Origin	Bien conocido y mandatorio.	Código de origen. Preferidos en este orden: (i) IGP, (e) EGP, (?) Incomplete.

Tabla 3.2: Atributos BGP que no son considerados en la selección de mejor ruta

El proceso de selección de rutas completo de BGP sigue el siguiente orden:

1. Se prefiere el camino con el weight más alto. Este atributo es propietario de Cisco y es local al router en el que se configura.
2. Se prefiere el camino con local_pref más alto. Por defecto toma un valor de 100 pero es posible modificarlo.
3. Se prefieren caminos originados localmente vía el comando network o aggregate, o mediante redistribución desde un IGP. Los caminos locales originados por el comando network o redistribute son preferidos sobre los caminos para segmentos sumarizados.
4. Se prefiere el camino con el asjpath más corto.
5. Se prefiere el camino con el **origin** más bajo, donde IGP<EGP.
6. Se prefiere el camino con la med más baja. Por defecto es 0.
7. Se prefieren caminos EBGP sobre caminos IBGP.
8. Se prefiere el camino a través del IGP con la menor métrica hacia el next hop de BGP
9. Determinar si se requiere instalar múltiples caminos en la tabla de enrutamiento para BGP Multipath.
10. Cuando ambos caminos son externos se prefiere el que fue recibido primero (el más antiguo). Esto minimiza el flapping de rutas.

El propio sistema que BGP utiliza para controlar la selección de rutas es bastante sofisticado habrá momentos en que el administrador tendrá que influir en ese comportamiento modificando los atributos del protocolo. Existen muchos métodos para influenciar la selección de caminos en BGP, pero los route-maps son los más utilizados.

Los cuatro principales atributos qué se suelen modificar son Weight, Local-Preference, MED y AS-path prepending. Los dos primeros se modifican para influenciar cómo sale el tráfico del AS y los siguientes indicarán a otros AS cómo se prefiere que ellos alcancen al AS local.

El atributo Weight es propietario de Cisco, selecciona la interfaz de salida cuando existen múltiples rutas hacia un mismo destino. Cuanto más alto es el valor, mayor preferencia. Este atributo es local al router y no se propaga hacia los demás routers. Este atributo es extremadamente potente, porque es el primero que BGP utiliza en el proceso de selección y toma preferencia sobre cualquier otro. puede tomar valores entre 0 y 65535, por defecto es 0 a menos que el router esté originando la ruta,

en cuyo caso el peso por defecto será 32768. Cuando se modifican por segmento de red es común que se ocupen route-maps

El atributo Local-Preference puede definirse por segmento de red o por defecto siendo este aplicado a todos los segmentos de red, tiene un rango entre 0 y 4294967295, cuanto más alto el valor mayor preferencia. Por defecto lleva un valor de 100.

El atributo MED es advertido a los vecinos externos para influenciarlos en el sentido de cómo van a poder alcanzar a nuestro sistema autónomo, es decir, que se modifica el tráfico de entrada hacia nuestro AS. Por ejemplo, cuando existen enlaces redundantes hacia un ISP y se necesita que el tráfico fluya sobre el enlace con mayor capacidad. Con el Weight o con el Local-preference se puede controlar cómo los routers locales envían tráfico fuera del sistema autónomo, pero los vecinos externos no reciben esa información. Si se configura el atributo MED para que sea más bajo en uno de los caminos, éste será elegido por los vecinos para enviar tráfico hacia el AS local.

El valor de MED por defecto es 0.

El atributo AS-path es obligatorio para todas las actualizaciones. Es el mecanismo que BGP utiliza para detectar bucles de enrutamiento y que además es el sistema para decidir que ruta es la más corta. Mientras más AS sean atravesados peor será el camino, siempre se utilizará el AS-path más corto.

4. Implementación de BGP en redes redundantes para clientes

4.1.- Simulación Gráfica de Redes GNS3

GNS3 (Graphic Network Simulation) es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

• Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarias imágenes IOS de Cisco Systems.

• Dynagen, un front-end basado en texto para Dynamips.

• Qemu, un emulador de PIX.GNS3 es una excelente herramienta complementaria a los verdaderos laboratorios para los administradores de redes de Cisco.

Una vez instalado en GNS3 lo iniciamos, los routers no tiene IOS por lo que tenemos que descargarnos los sistemas. Una vez descargados los sistemas nos vamos a Edit y seleccionamos IOS imagen and hypervisos, como se muestra en la figura siguiente.

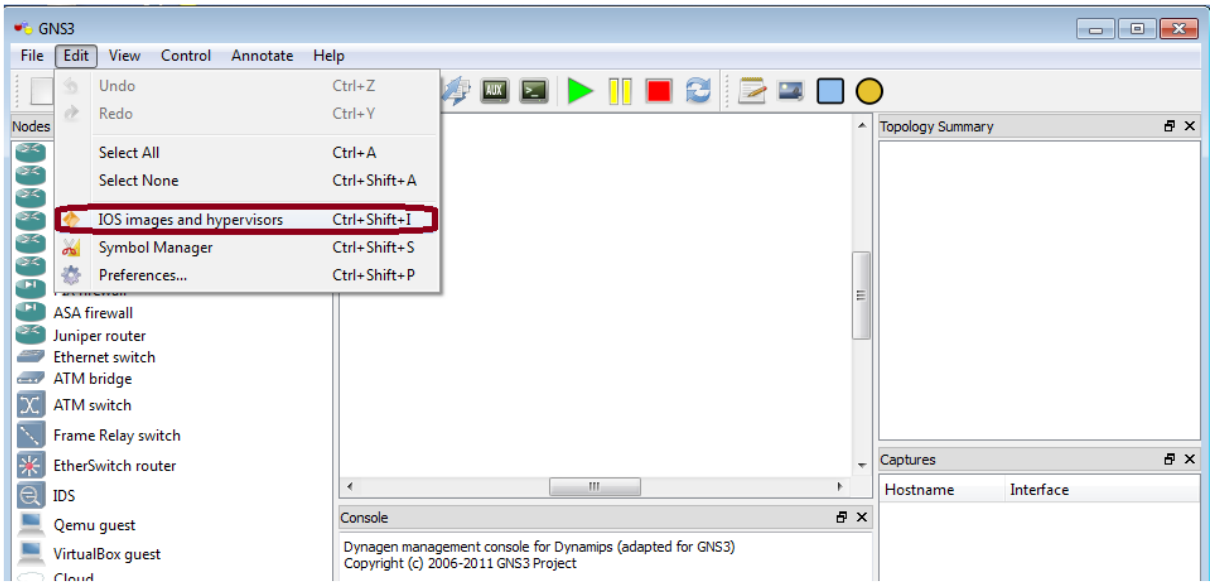

Figura 4-1: Agregar una imagen a GNS3

Pulsada la opción anterior, nos sale la siguiente diapositiva le damos “Image file” y seleccionamos las imágenes de los router que queremos.

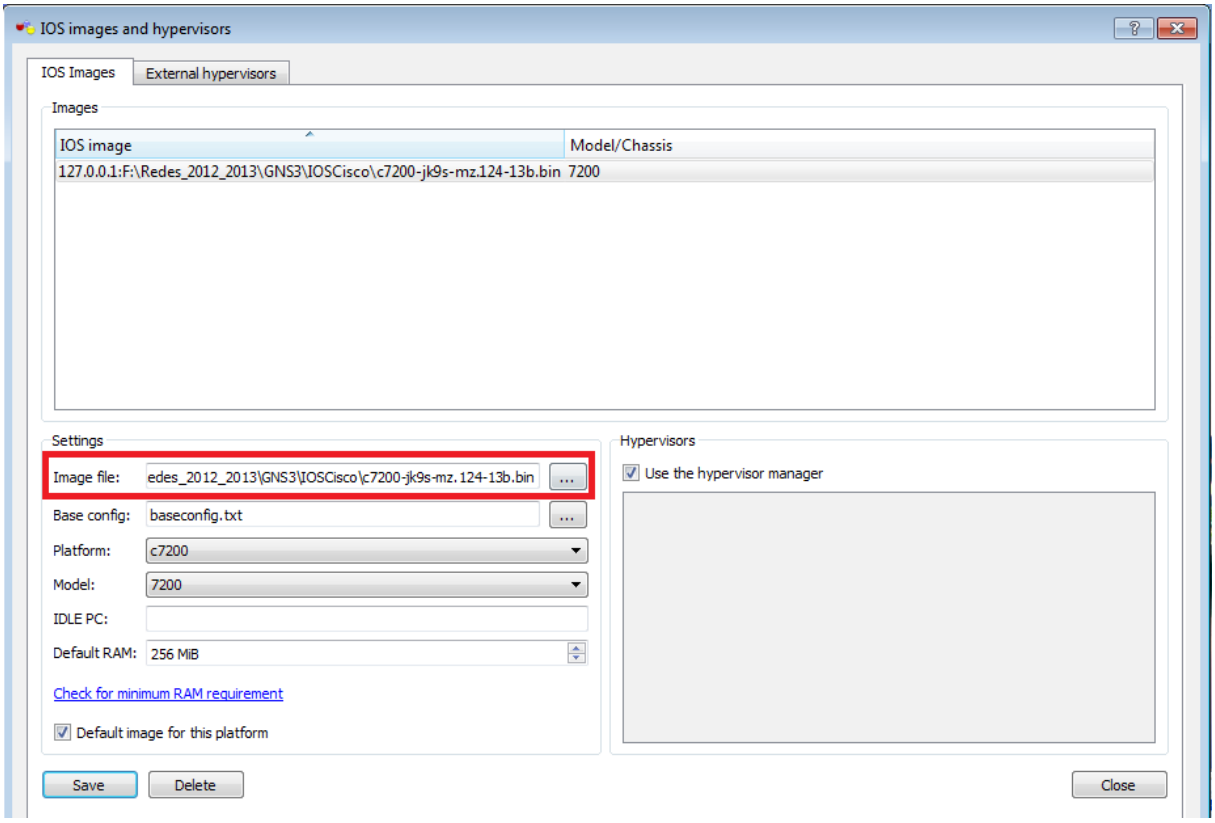

Figura 4-2: Seleccionar una imagen

Una vez escogido el IOS de los router solo tenemos que arrastra el router hacia nuestro escenario para poner empezar a utilizarlos. Hacemos clic derecho en el router y tenemos varias opciones como Cambiar Símbolo, Iniciar, etc.

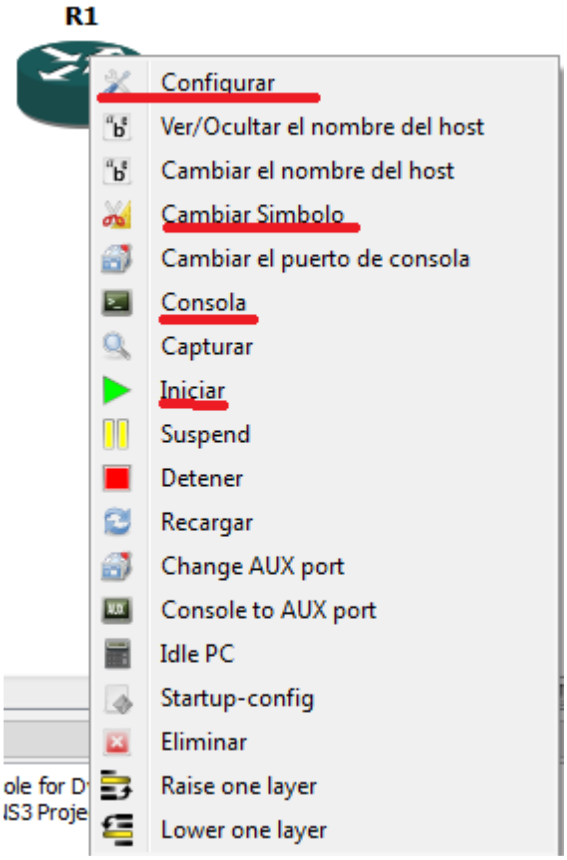

Figura 4-3: Configuración inicial del router en GNS3

Hacemos clic derecho sobre configuración y en la pestaña Slots podemos poner más ranuras para poner interfaz serial, ethernet, etc.

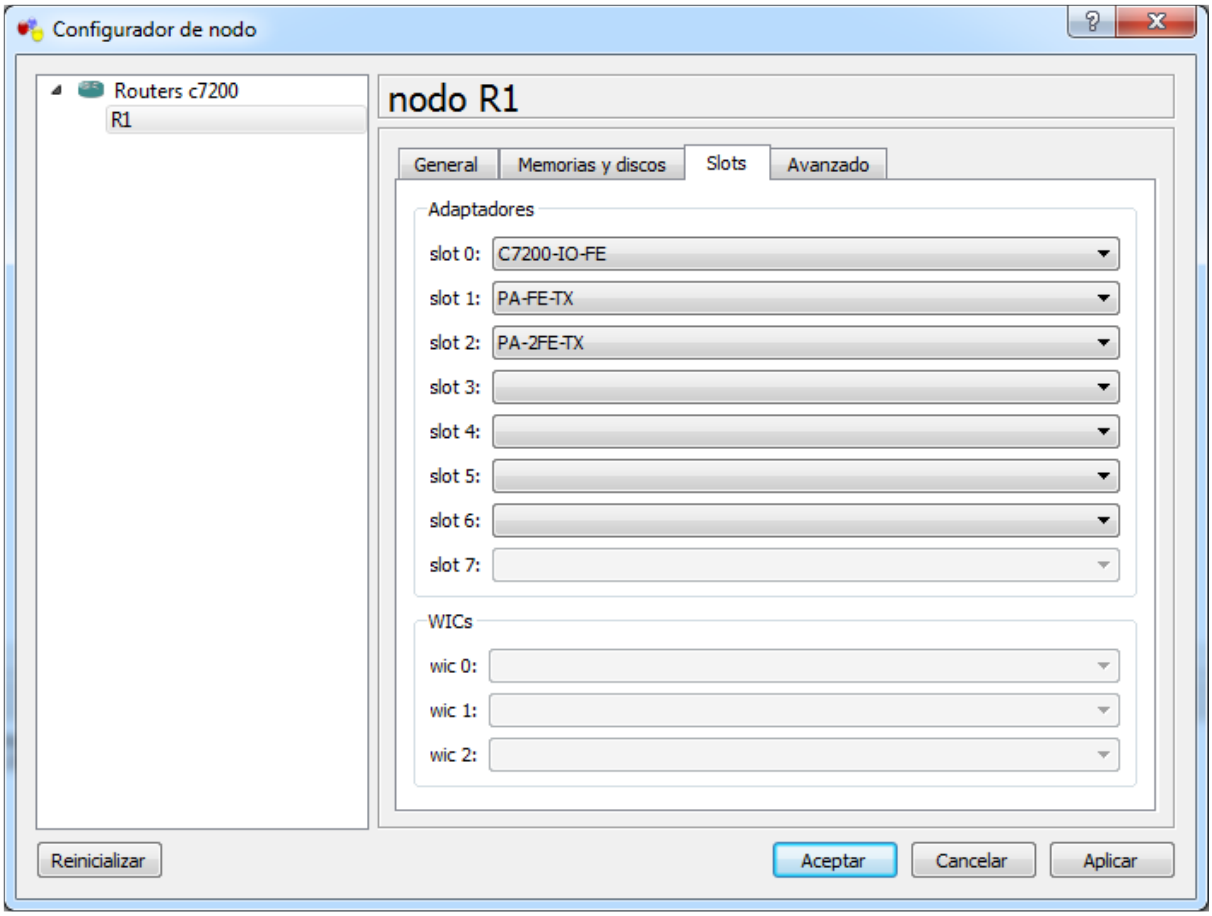

Figura 4-4: Selección de tarjetas para el router

Una vez realizados los pasos anteriores se puede empezar a configurar el router y simular redes para probar configuraciones y soluciones de conectividad.

4.2.- CISCO IOS

El sistema operativo internetwork IOS (Internetwork Operating System) es el software utilizado en la gran mayoría de routers y switches de Cisco Systems. IOS es un paquete de funciones de enrutamiento, conmutación, trabajo de internet y telecomunicaciones que se integra estrechamente con un sistema operativo multitarea.

La interfaz de línea de comandos de IOS (IOS CLI) proporciona un conjunto fijo de comandos de múltiples palabras. El conjunto disponible se determina mediante el "modo" y el nivel de privilegios del usuario actual. El modo "Global configuration" proporciona comandos para cambiar la configuración del sistema y el modo "interface

configuration" a su vez, proporciona comandos para cambiar la configuración de una interfaz específica. A todos los comandos se les asigna un nivel de privilegios, de 0 a 15, y pueden ser accedidos por usuarios con los privilegios necesarios. A través de la CLI, se pueden definir los comandos disponibles para cada nivel de privilegio.

Al arrancar un dispositivo de Cisco este realiza un Bootstrap (comprobación de hardware).

Después intentará cargar una imagen IOS desde la memoria Flash o desde un servidor TFTP. En el caso de no hallarla ejecutará una versión reducida de la IOS ubicada en la ROM.

Tras el arranque del sistema localizará la configuración del mismo, generalmente en texto simple. Puede estar ubicada en la memoria NVRAM o en un servidor de TFTP. En el caso de no encontrarla iniciará un asistente de instalación (modo Setup).

Con la siguiente imagen puede quedar más claro:

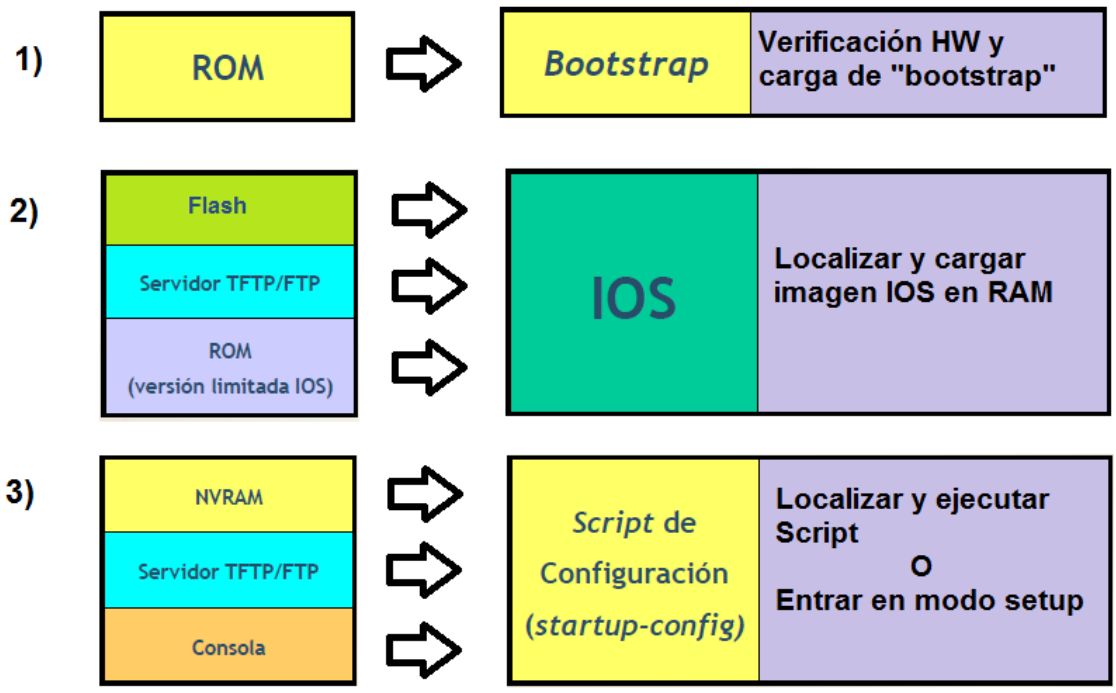

Figura 4-5: Arranque de CISCO IOS

La implementación del protocolo dinámico de enrutamiento BGP se realizará mediante una simulación en GNS3 debido a que este software al manejar imágenes del sistema operativo real de CISCO, no tiene limitaciones como en otros simuladores en cuanto a comandos y bondades de BGP y otros protocolos que se necesitan para implementar una red con eBGP redundante. Esta implementación estará basada en el escenario donde un cliente ha contratado un servicio Dual Homed a un ISP para tener su acceso a internet redundado con dos equipos CE. Todo el tráfico que se ocupará será en IPv4, los segmentos de red públicos que se ocuparán y los equipos CE pertenecen al ISP y son rentados al cliente. La red del ISP será simulada con 4 equipos router, internet se representará con un router conectado a la red del ISP.

Los sistemas autónomos y direccionamientos IP que se manejan en esta simulación son asignados al azar y no necesariamente existen en una red de ISP o de alguna organización.

La topología LAN no se incluye en la simulación, esta será representada mediante sub-interfaces entre los equipos del CDMX_PRI y CDMX_BKP, uniéndose a través de un switch.

El diagrama de red para esta simulación se muestra en la figura siguiente:

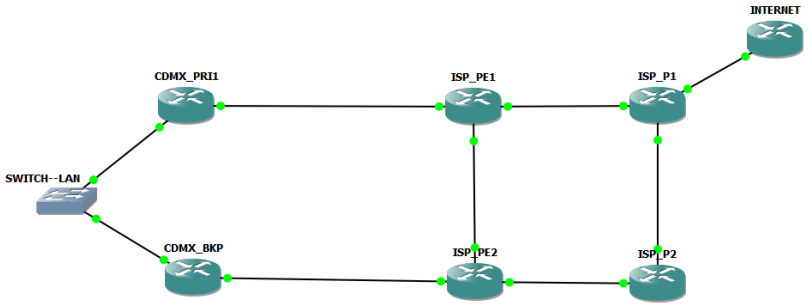

Figura 4-6: Diagrama general de red

Donde:

- CDMX_PRI: Es el enrutador principal del cliente.
- CDMX_BKP: Es el enrutador de respaldo para la solución del cliente.
- ISP_PE1: Es el enrutador del ISP donde se conecta el equipo principal del cliente.
- ISP_PE2: Es el enrutador del ISP donde se conecta el equipo de respaldo del cliente.
- ISP_P1 e ISP_P2: son equipos de la red de CORE del ISP.
- INTERNET: es equipo que simula internet y es la salida del ISP a esta red.

Los segmentos que se ocuparán en esta simulación son las siguientes:

- LAN 201.37.0.0/25
- LAN 201.37.0.128/25
- WAN 200.36.0.0/30
- WAN 200.36.0.4/30
- WAN 10.0.0.0/30
- WAN 10.0.0.4/30
- WAN 10.0.0.8/30
- WAN 10.0.0.12/30
- WAN 87.100.0.0/30

La distribución de las redes y la IP por interfaz queda de la siguiente manera.

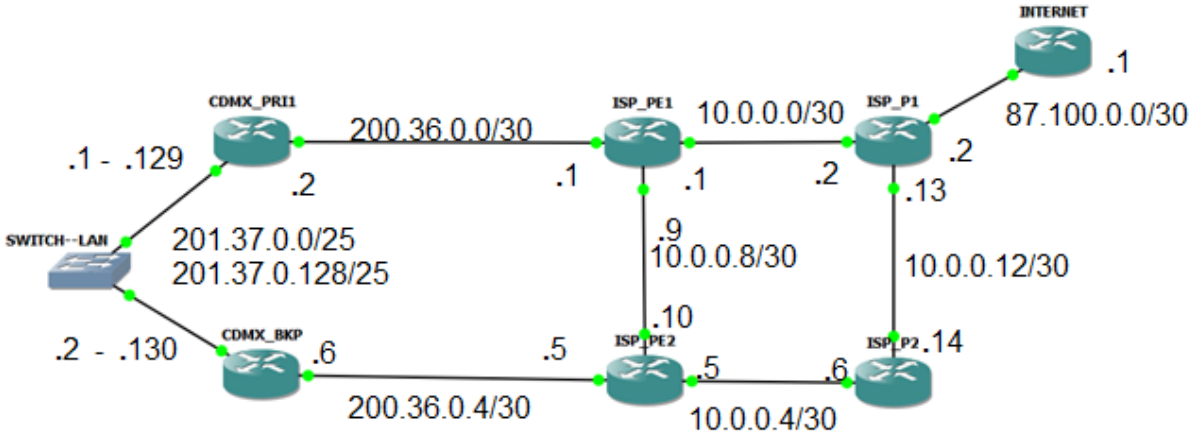

Figura 4-7: Distribución de direccionamiento

La simulación se realizará en equipos router CISCO 7206-VXR compatibles con el protocolo BGP y todas las bondades necesarias para el objetivo de la simulación y un switch genérico para unir las interfaces LAN entre los equipos CDMX_PRI y CDMX_BKP.

Figura 4-8: equipo CISCO 7206-VXR

Recordemos que GNS3 emula mediante Dynamips las imágenes de CISCO IOS por lo que al encender un equipo de estas características en GNS3, mostrará además del modo de arranque real de un router CISCO, la información sobre la conexión de la imagen con Dynamips.

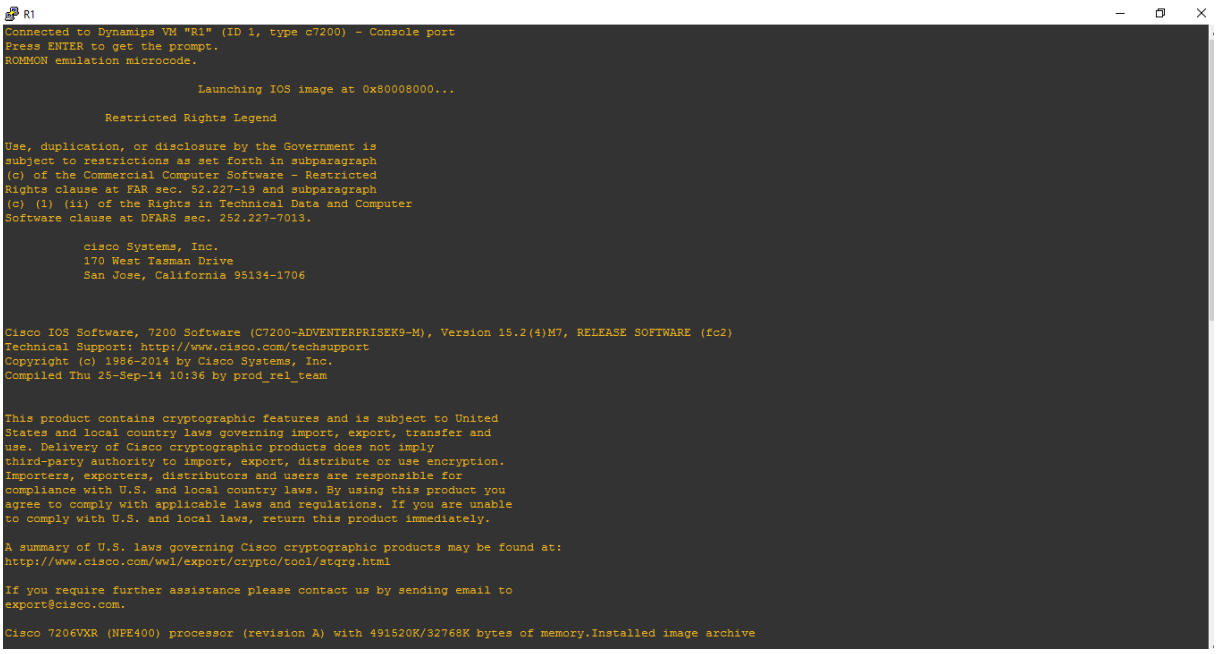

Figura 4-9: Arranque de un equipo CISCO IOS en GNS3

Una vez terminado el inicio del equipo, el router está listo para ser configurado. El router inicia con el prompt “nombre>”, esto nos indica el nivel de privilegio en que se encuentra el router. En CISCO existen 3 tipos de niveles identificados con un prompt diferente para cada uno, los cuales nos habilitarán o restringirán el uso de herramientas para la configurar y administración del equipo.

- Modo de usuario, en este modo podremos hacer uso de herramientas de monitoreo básicas del equipo como son:
  * ping.
  * show (limitado)
  * enable
- Modo privilegiado, en este modo podremos tener acceso al modo de configuración global y a herramientas avanzadas de monitoreo como:
  * show (sin limitantes)
  * comandos del tipo debug
  * Reload
  * Configure

- Modo de configuración global, en este modo de configuración podemos tener acceso a todas las características del router así como poderlo configurar a nuestro gusto.
  * hostname
  * enable secret
  * ip route
  * interface (El tipo de interfaz depende de cada equipo).
  * router (se puede ingresar la configuración de ruteo dinámico, el equipo debe soportrar este tipo de ruteo y los protocolos para realizarlo).
  * Line (vty, console etc).

Para poder realizar configuraciones sobre el router es necesario ingresar al modo de configuración global, el cual nos dará acceso a la configuración de interfaces y protocolos específicos, para ingresar al modo de configuración global es necesario acceder primero al modo privilegiado usando el comando “enable”, después de ejecutar este comando, el promp cambia de “nombre>” a “nombre#” identificando así el modo en que nos encontramos dentro del equipo, una vez en el modo privilegiado se accede al modo de configuración global con el comando “configure terminal” el modo es identificado con el prompt “nombre(config)#”. En el simulador GNS3, después del inicio de un equipo, el modo en el que se ingresa por defecto mediante la conexión de consola es el modo privilegiado por lo que no es necesario ingresar el comando enable.

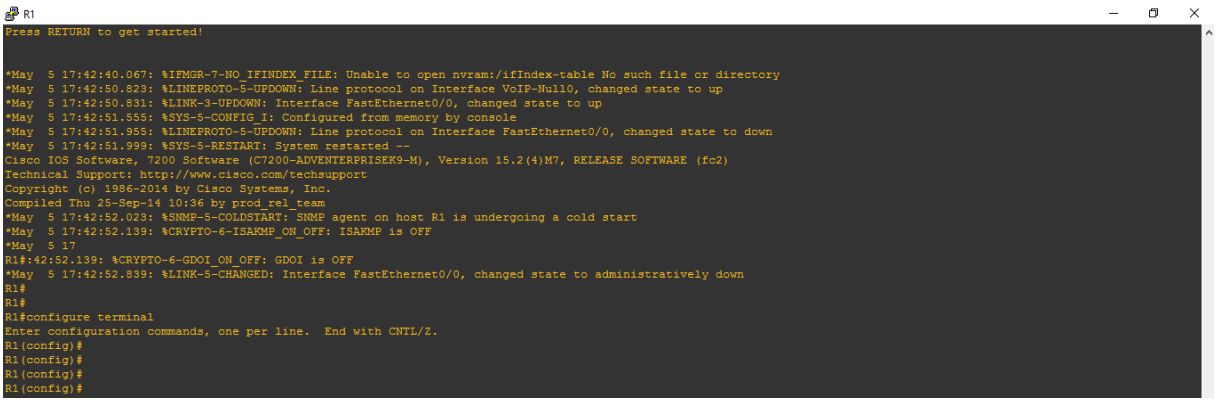

Figura 4-10: Acceso al modo de configuración global

En nuestro escenario los routers “CDMX_PRI”, “CDMX_BKP” e “INTERNET” solo ocuparán el protocolo dinámico BGP para formar la tabla de enrutamiento de cada uno, para los dos equipos CE también es con BGP que se brindará la redundancia en caso de falla en el enlace principal. La figura siguiente muestra la configuración de BGP en el router “CDMX_PRI” y “CDMX_BKP”.

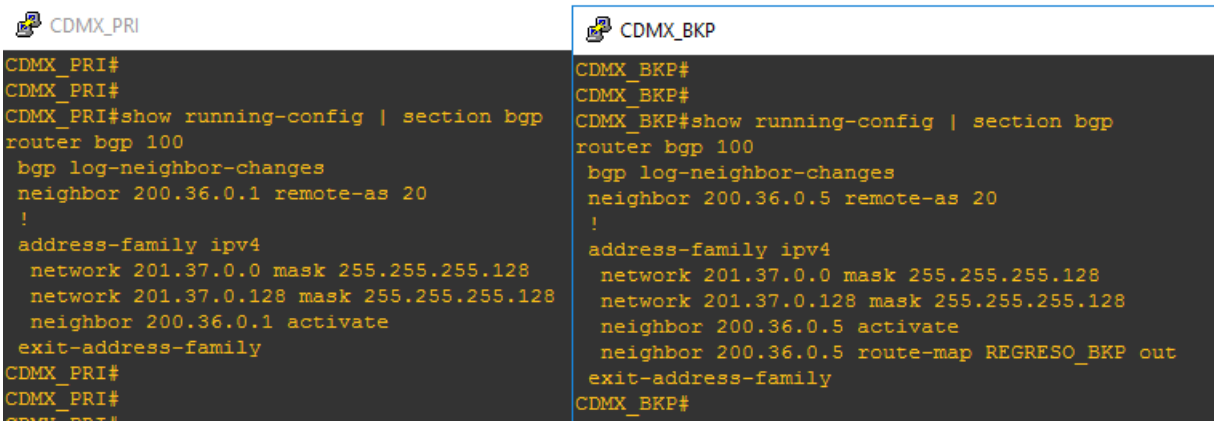

Figura 4-11: Configuración de BGP en los router CDMX_PRI y CDMX_BKP

Los equipos mencionados en la figura anterior representan los equipos CE (instalados en las instalaciones del cliente). Como se puede apreciar existe una ligera diferencia en los comandos ocupados para la configuración de ambas sesiones de BGP. A continuación, se explicará el funcionamiento de cada comando basados en el router CDMX_PRI. El comando “router bgp 100” crea la instancia de BGP con el AS 100, el comando “bgp log-neighbor-changes” aparece por defecto al introducir el comando anterior, permite habilitar o deshabilitar el registro de mensajes generado

cuando el estatus de un vecino BGP cambia. En BGP a diferencia de OSPF, un vecino debe indicarse puntualmente con el comando “neighbor” y la IP específica del vecino con el que se requiere establecer una adyacencia, también debe indicarse el ASN al que pertenece el vecino, si el ASN del vecino es el mismo que el de la instancia de BGP que corre en el router, la adyacencia será del tipo iBGP, si el ASN es diferente entonces la adyacencia será del tipo eBGP. En nuestra simulación se realiza una sesión eBGP con el comando “neighbor 200.36.0.1 remote-as 20”, es importante recordar que este comando debe existir en ambos lados de la sesión. El comando “network” se ocupa para anunciar redes hacia los vecinos, este comando no es lo único que se requiere pues además es necesario que exista una interfaz activa dentro de la red que se desee anunciar o una ruta hacia esa red en el router donde se realiza el anuncio, en la simulación las redes que se anuncian son “201.37.0.0/25 y 201.37.0.128/25” es necesario indicar la mascará de red en formato de 4 octetos, “address-family ipv4” no es un comando, es una sección dentro de BGP donde se pueden realizar anuncios de redes y aplicar otras características hacia uno o más vecinos de la misma “address family” que en este caso es IPv4. El comando “neighbor 200.36.0.1 activate” activa la sesión con el vecino, generalmente este comando se aplica por defecto después de declarar un vecino. El comando “neighbor 200.36.0.5 route-map REGRESO_BKP out” se aplica solo en el router que tiene el rol de respaldo, este comando lo que hace es aplicar un filtro de salida, para que las redes LAN sean anunciadas al vecino (ISP_PE2 es el equipo que realiza una adyacencia de BGP con el router de respaldo) con una métrica mayor para que la preferencia sea mejor por el equipo principal, en resumen con este comando se controla que el regreso del tráfico hacia la red LAN sea por el equipo principal siempre que este último mantenga activa su sesión BGP, la parte “REGRESO_BKP” es el nombre del filtro.

En la siguiente figura se muestra la configuración del filtro que se aplica al vecino de BGP en el equipo de respaldo.

```
route-map REGRESO_BKP permit 10
 match ip address prefix-list REDES_BKP
 set as-path prepend 100 100 100 100
CDMX_BKP#
```

Figura 4-12: configuración del filtro de salida

El comando “route-map REGRESO_BKP permit 10” crea el route-map llamado REGRESO_BKP mientras que permit 10 establece como permitido lo que se ingrese en el route-map y agreaga la secuencia 10. El comando “match ip address prefix-list REDES_BKP” establece que el route-map tendrá efecto solo en las redes redes IP que estén dentro de la lista de prefijos identificada como “REDES_BKP”. El comando “set as-path prepend 100 100 100 100” anexa 4 AS a la como ruta para las redes de la lista de prefijos mencionada, para que sean anunciadas al vecino de la sesión BGP donde se aplique este route-map.

La figura siguiente muestra la configuración de la lista de prefijos.

```
CDMX_BKP#sh run | sec ip prefix
ip prefix-list REDES_BKP seq 5 permit 201.37.0.0/25
ip prefix-list REDES_BKP seq 10 permit 201.37.0.128/25
CDMX_BKP#
```

Figura 4-13: Configuración de lista de prefijos

Los comandos mostrados en la figura anterior establecen las secuencias 5 y 10 que permiten las redes 201.37.0.0/25 y 201.37.0.128/25, como lo vimos en la descripción del filtro a estas redes se les modificará la métrica de la ruta que será anunciada al vecino de BGP en el router de respaldo.

Los routers que representan la red de core del ISP “ISP_PE1”, “ISP_PE2”, “ISP_P1” e “ISP_P2” armarán su tabla de ruteo con dos protocolos dinámicos, BGP y OSPF, el protocolo BGP se ocupará para aprender y anunciar redes a equipos que existen en un sistema autónomo diferente al del ISP, es decir, se ocupa como EGP, mientras el protocolo OSPF se ocupará como IGP para redistribuir las redes aprendidas de otros sistemas autónomos y tener comunicación entre todas las puntas de la red. Por temas de diseño, OSPF se implementará solo en el área de backbone.

En la figura siguiente se muestra la configuración del BGP y OSPF en los equipos frontera del ISP.

ISP_PE1

```
ISP_PE1#
ISP_PE1#
ISP_PE1#sh run | sec bgp
 redistribute bgp 20 metric 10 subnets
router bgp 20
 bgp log-neighbor-changes
 neighbor 200.36.0.2 remote-as 100
 !
 address-family ipv4
  redistribute connected
  redistribute static
  redistribute ospf 20 match internal external 1 external 2
  neighbor 200.36.0.2 activate
  neighbor 200.36.0.2 default-originate
 exit-address-family
ISP_PE1#
ISP_PE1#
ISP_PE1#sh run | sec ospf
router ospf 20
 redistribute bgp 20 metric 10 subnets
 network 10.0.0.0 0.0.0.255 area 0
  redistribute ospf 20 match internal external 1 external 2
ISP_PE1#
ISP_PE1#
```

ISP_PE2

```
ISP_PE2#
ISP_PE2#sh run | sec bgp
 redistribute bgp 20 metric 30 subnets
router bgp 20
 bgp log-neighbor-changes
 neighbor 200.36.0.6 remote-as 100
 !
 address-family ipv4
 redistribute connected
 redistribute static
 neighbor 200.36.0.6 activate
 neighbor 200.36.0.6 default-originate
 no auto-summary
 no synchronization
 exit-address-family
ISP_PE2#
ISP_PE2#
ISP_PE2#sh run | sec ospf
router ospf 20
 log-adjacency-changes
 redistribute bgp 20 metric 30 subnets
 network 10.0.0.0 0.0.0.255 area 0
ISP_PE2#
ISP_PE2#
```

Figura 4-14: Configuración de los routers frontera del ISP

En el router INTERNET se agregará un filtro para poder recibir solo las redes que sean acordadas entre el ISP e internet como se muestra en la imagen sigiente.

```
INTERNET#sh run | sec FILTRO_REDES_PERMITIDAS
ip prefix-list FILTRO_REDES_PERMITIDAS seq 5 permit 201.37.0.0/25
ip prefix-list FILTRO_REDES_PERMITIDAS seq 10 permit 201.37.0.128/25
ip prefix-list FILTRO_REDES_PERMITIDAS seq 15 permit 200.36.0.0/24 le 32
```

```
route-map REDES_IN permit 10
 match ip address prefix-list FILTRO_REDES_PERMITIDAS
```

```
router bgp 500
 bgp log-neighbor-changes
 neighbor 87.100.0.2 remote-as 20
 !
 address-family ipv4
 neighbor 87.100.0.2 activate
 neighbor 87.100.0.2 default-originate
 neighbor 87.100.0.2 route-map REDES_IN in
 neighbor 87.100.0.2 route-map DEFAULT out
 no auto-summary
 no synchronization
```

Figura 4-15: Filtro de redes permitidas en INTERNET

De igual manera en el router frontera del ISP hacia internet se aplica un filtro para anunciar solo las redes que necesitan ser anunciadas a INTERNET (sin este filtro las redes pueden ser anunciadas, pero no existiría un control en el anuncio dejando susceptible el anuncio de redes por error a internet) y un filtro para no permitir que el router INTERNET le anuncie las redes del ISP.

El filtro para permitir anuncios de prefijos desde el router ISP_P1 hacia el router INTERNET se muestra en la figura siguiente.

```
ip prefix-list FILTRO_REDES_OUT seq 5 permit 201.37.0.0/25
ip prefix-list FILTRO_REDES_OUT seq 10 permit 201.37.0.128/25
ip prefix-list FILTRO_REDES_OUT seq 15 permit 200.36.0.0/24 le 32
```

```
route-map REDES_OUT permit 10
 match ip address prefix-list FILTRO_REDES_OUT
```

```
router bgp 20
 bgp log-neighbor-changes
 neighbor 87.100.0.1 remote-as 500
 !
 address-family ipv4
 neighbor 87.100.0.1 activate
 neighbor 87.100.0.1 route-map FILTRO_IN in
 neighbor 87.100.0.1 route-map REDES_OUT out
 no auto-summary
 no synchronization
 network 201.37.0.0 mask 255.255.255.128
 network 201.37.0.128 mask 255.255.255.128
```

Figura 4-16: Configuración del filtro de salida para las redes anunciadas desde el router ISP_P1

La figura siguiente muestra la configuración del filtro para no permitir que el router ISP_P1 aprenda las redes propiedad del ISP desde el router INTERNET.

```
ip prefix-list FILTRO_REDES_IN seq 5 deny 201.37.0.0/16 le 32
ip prefix-list FILTRO_REDES_IN seq 10 deny 200.36.0.0/16 le 32
ip prefix-list FILTRO_REDES_IN seq 15 permit 0.0.0.0/0 le 32
```

```
route-map FILTRO_IN permit 10
 match ip address prefix-list FILTRO_REDES_IN
```

```
router bgp 20
 bgp log-neighbor-changes
 neighbor 87.100.0.1 remote-as 500
 !
 address-family ipv4
 neighbor 87.100.0.1 activate
 neighbor 87.100.0.1 route-map FILTRO_IN in
 no auto-summary
 no synchronization
 network 201.37.0.0 mask 255.255.255.128
 network 201.37.0.128 mask 255.255.255.128
```

Figura 4-17: Filtro para prevenir que INTERNET anuncie las redes del ISP al mismo ISP

De esta manera se puede brindar sobrevivencia al servicio redundado que ofrece un ISP a sus clientes.

Conclusiones

Las bondades del protocolo BGP permiten además de mantener un registro de todos los ASN por los que atraviesa un paquete IP para llegar a un destino específico, brindar a organizaciones la redundancia que requieran para tener acceso a internet mediante un ISP, haciéndolo de manera eficiente y sin afectar el registro mencionado.

Hablando desde el punto de vista de un ISP, siempre es recomendable aplicar filtros que permitan o no el anuncio o recepción de prefijos de red para evitar en lo más posible problemas de enrutamiento provocado por errores humanos.

La conectividad a internet y la disponibilidad del acceso hacia internet se vuelve cada vez más importante para la operación de la mayoría de organizaciones y empresas que tienen o planean tener servicios en la nube, pero debe tomarse en cuenta el cambio que se estará dando para los identificadores globales pasando de IPv4 a IPv6, la implementación de BGP en este escenario conlleva cambios de configuración aun cuando los métodos de acceso a la red del ISP sean los mismos, estas modificaciones podrán realizarse en tesinas futuras.

Anexos

Descarga de simulador GNS3.

https://www.gns3.com/software

Descarga de imágenes de SO para GNS3.

http://f.usht.ru/Cisco/IOS/

Configuración de equipos.

CDMX_PRI

Building configuration...

Current configuration : 2137 bytes

upgrade fpd auto

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname CDMX_PRI

boot-start-marker

boot-end-marker

no aaa new-model

no ip icmp rate-limit unreachable

no ip domain lookup

ip cef

no ipv6 cef

```
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
track 1 ip sla 1
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/1
 description ENACE_LAN
 no ip address
 duplex auto
 speed auto
```

```
interface FastEthernet1/1.10
 description LAN_1
 encapsulation dot1Q 10
 ip address 201.37.0.1 255.255.255.128
 standby 1 ip 201.37.0.3
 standby 1 priority 120
 standby 1 preempt
 standby 1 track 1 decrement 60
interface FastEthernet1/1.20
 description LAN_2
 encapsulation dot1Q 20
 ip address 201.37.0.129 255.255.255.128
 standby 2 ip 201.37.0.131
 standby 2 priority 120
 standby 2 preempt
 standby 2 track 1 decrement 60
interface GigabitEthernet2/0
 description ENLACE_ISP_PE1
 ip address 200.36.0.2 255.255.255.252
 negotiation auto
router bgp 100
 bgp log-neighbor-changes
 neighbor 200.36.0.1 remote-as 20
 address-family ipv4
```

```
 network 201.37.0.0 mask 255.255.255.128
 network 201.37.0.128 mask 255.255.255.128
 neighbor 200.36.0.1 activate
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip sla auto discovery
ip sla 1
 icmp-echo 200.36.0.1 source-ip 200.36.0.2
 frequency 5
ip sla schedule 1 life forever start-time now
ip sla logging traps
logging alarm informational
no cdp log mismatch duplex
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

password cisco

login

transport input all

end

CDMX_BKP

Building configuration...

Current configuration : 2121 bytes

upgrade fpd auto

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname CDMX_BKP

boot-start-marker

boot-end-marker

no aaa new-model

no ip icmp rate-limit unreachable

```
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
interface FastEthernet0/0
 description ENLACE_LAN
 no ip address
 duplex auto
 speed auto
interface FastEthernet0/0.10
 description LAN_1
 encapsulation dot1Q 10
 ip address 201.37.0.2 255.255.255.128
 standby 1 ip 201.37.0.3
 standby 1 preempt
interface FastEthernet0/0.20
 description LAN_2
 encapsulation dot1Q 20
 ip address 201.37.0.130 255.255.255.128
 standby 2 ip 201.37.0.131
 standby 2 preempt
interface FastEthernet0/1
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface GigabitEthernet2/0
 description ENLACE_ISP_PE2
 ip address 200.36.0.6 255.255.255.252
 negotiation auto
router bgp 100
 bgp log-neighbor-changes
 neighbor 200.36.0.5 remote-as 20
 address-family ipv4
  network 201.37.0.0 mask 255.255.255.128
  network 201.37.0.128 mask 255.255.255.128
```

```
 neighbor 200.36.0.5 activate
 neighbor 200.36.0.5 route-map REGRESO_BKP out
exit-address-family
ip forward-protocol nd
no ip http server
no ip http secure-server
ip prefix-list REDES_BKP seq 5 permit 201.37.0.0/25
ip prefix-list REDES_BKP seq 10 permit 201.37.0.128/25
logging alarm informational
no cdp log mismatch duplex
route-map REGRESO_BKP permit 10
 match ip address prefix-list REDES_BKP
 set as-path prepend 100 100 100 100
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
end
```

ISP_PE1

```
Building configuration...
Current configuration : 1930 bytes
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ISP_PE1
boot-start-marker
boot-end-marker
no aaa new-model
no ip icmp rate-limit unreachable
no ip domain lookup
ip cef
```

```
no ipv6 cef
multilink bundle-name authenticated
redundancy
ip tcp synwait-time 5
crypto map TunelTData 199 ipsec-isakmp
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
interface GigabitEthernet0/0
 description PUERTO_CLIENTES
 ip address 200.36.0.1 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
interface GigabitEthernet1/0
 description ENLACE_ISP_PE2
 ip address 10.0.0.9 255.255.255.252
 negotiation auto
interface GigabitEthernet2/0
 description ENLACE_ISP_P1
 ip address 10.0.0.1 255.255.255.252
 negotiation auto
```

```
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
router ospf 20
 redistribute connected subnets
 redistribute bgp 20 metric 10 subnets
 network 10.0.0.0 0.0.0.255 area 0
router bgp 20
 bgp log-neighbor-changes
 neighbor 200.36.0.2 remote-as 100
 address-family ipv4
  redistribute connected
  redistribute static
  redistribute ospf 20 match internal external 1 external 2
  neighbor 200.36.0.2 activate
  neighbor 200.36.0.2 default-originate
 exit-address-family
ip forward-protocol nd
no ip http server
```

```
no ip http secure-server
logging alarm informational
no cdp log mismatch duplex
control-plane
mgcp profile default
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
end
```

ISP_PE2

```
Building configuration...

Current configuration : 1847 bytes

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname ISP_PE2

boot-start-marker

boot-end-marker

no aaa new-model

resource policy

ip subnet-zero

no ip icmp rate-limit unreachable

ip cef

ip tcp synwait-time 5

no ip domain lookup

interface Ethernet0/0

 no ip address

 shutdown

 duplex auto

interface GigabitEthernet0/0

 description ENLACE_CDMX_BKP

 ip address 200.36.0.5 255.255.255.252

 duplex full
```

```
 speed 1000
 media-type gbic
 negotiation auto
interface GigabitEthernet1/0
 description ENLACE_ISP_PE1
 ip address 10.0.0.10 255.255.255.252
 negotiation auto
interface GigabitEthernet2/0
 description ENLACE_ISP_P2
 ip address 10.0.0.5 255.255.255.252
 negotiation auto
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
router ospf 20
 log-adjacency-changes
 redistribute connected subnets
 redistribute bgp 20 metric 30 subnets
 network 10.0.0.0 0.0.0.255 area 0
```

```
router bgp 20
 bgp log-neighbor-changes
 neighbor 200.36.0.6 remote-as 100
 address-family ipv4
 redistribute connected
 redistribute static
 redistribute ospf 20 match internal external 1 external 2
 neighbor 200.36.0.6 activate
 neighbor 200.36.0.6 default-originate
 no auto-summary
 no synchronization
 exit-address-family
ip classless
no ip http server
no ip http secure-server
logging alarm informational
no cdp log mismatch duplex
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 3
 login
line vty 4
 password cisco
 login
end
```

ISP_P1

```
Building configuration...
Current configuration : 2484 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ISP_P1
boot-start-marker
boot-end-marker
no aaa new-model
```

```
resource policy
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
no ip domain lookup
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
interface GigabitEthernet0/0
 description ENLACE_ISP_P2
 ip address 10.0.0.13 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
interface GigabitEthernet1/0
 description ENLACE_ISP_PE1
 ip address 10.0.0.2 255.255.255.252
 negotiation auto
interface GigabitEthernet2/0
 description ENLACE_INTERNET
 ip address 87.100.0.2 255.255.255.252
```

```
 negotiation auto
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
router ospf 20
 log-adjacency-changes
 redistribute connected subnets
 redistribute static subnets
 redistribute bgp 20 metric 10 subnets
 passive-interface GigabitEthernet2/0
 network 10.0.0.0 0.0.0.255 area 0
 network 87.100.0.0 0.0.0.3 area 0
 default-information originate always
router bgp 20
 bgp log-neighbor-changes
 neighbor 87.100.0.1 remote-as 500
 address-family ipv4
 neighbor 87.100.0.1 activate
 neighbor 87.100.0.1 route-map FILTRO_IN in
 neighbor 87.100.0.1 route-map REDES_OUT out
 no auto-summary
 no synchronization
 network 200.36.0.0 mask 255.255.255.252
```

```
 network 200.36.0.4 mask 255.255.255.252
 network 201.37.0.0 mask 255.255.255.128
 network 201.37.0.128 mask 255.255.255.128
 exit-address-family
ip classless
no ip http server
no ip http secure-server
ip prefix-list FILTRO_REDES_IN seq 5 deny 201.37.0.0/16 le 32
ip prefix-list FILTRO_REDES_IN seq 10 deny 200.36.0.0/16 le 32
ip prefix-list FILTRO_REDES_IN seq 15 permit 0.0.0.0/0 le 32
ip prefix-list FILTRO_REDES_OUT seq 5 permit 201.37.0.0/16 le 32
ip prefix-list FILTRO_REDES_OUT seq 10 permit 200.36.0.0/16 le 32
logging alarm informational
no cdp log mismatch duplex
route-map FILTRO_IN permit 10
 match ip address prefix-list FILTRO_REDES_IN
route-map REDES_OUT permit 10
 match ip address prefix-list FILTRO_REDES_OUT
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
```

```
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 password cisco
 login
end
```

ISP_P2

```
Building configuration...
Current configuration : 1308 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname ISP_P2
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
```

```
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
no ip domain lookup
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
interface GigabitEthernet0/0
 description ENLACE_ISP_P1
 ip address 10.0.0.14 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
interface GigabitEthernet1/0
 description ENLACE_ISP_PE2
 ip address 10.0.0.6 255.255.255.252
 negotiation auto
interface GigabitEthernet2/0
 no ip address
 shutdown
 negotiation auto
```

```
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
router ospf 20
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
ip classless
no ip http server
no ip http secure-server
logging alarm informational
no cdp log mismatch duplex
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
 stopbits 1
line vty 0 4
 password cisco
 login
end
```

INTERNET

```
Building configuration...
Current configuration : 1665 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname INTERNET
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
no ip domain lookup
interface Ethernet0/0
```

```
 no ip address
 shutdown
 duplex auto
interface GigabitEthernet0/0
 description ENLACE_ISP_P1
 ip address 87.100.0.1 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
router bgp 500
 bgp log-neighbor-changes
 neighbor 87.100.0.2 remote-as 20
 address-family ipv4
 neighbor 87.100.0.2 activate
 neighbor 87.100.0.2 default-originate
 neighbor 87.100.0.2 route-map REDES_IN in
 neighbor 87.100.0.2 route-map DEFAULT out
 no auto-summary
 no synchronization
 exit-address-family
ip classless
no ip http server
no ip http secure-server
```

```
ip prefix-list DEFAULT_LIST seq 10 permit 0.0.0.0/0
ip prefix-list FILTRO_REDES_PERMITIDAS seq 5 permit 200.36.0.0/16 le 32
ip prefix-list FILTRO_REDES_PERMITIDAS seq 10 permit 201.37.0.0/16 le 32
logging alarm informational
no cdp log mismatch duplex
route-map REDES_IN permit 10
 match ip address prefix-list FILTRO_REDES_PERMITIDAS
route-map DEFAULT permit 10
 match ip address prefix-list DEFAULT_LIST
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 3
 login
```

```
line vty 4
 password cisco
 login
end
```

Glosario

BGP: Border Gateway Protocol es un protocolo de ruteo dinámico cuyo uso mayor se da como EGP en la compartición de rutas entre dos intranets con AS distinto. Su métrica es el Sistema Autónomo.

iBGP: Internal Border Gateway Protocol, es el termino denominado a BGP cuando es usado como protocolo de puerta de enlace interno en un Sistema Autónomo.

eBGP: External Border Gateway Protocol, es el termino denominado a BGP cuando es usado como protocolo de puerta de enlace externo en la comunicación entre dos sistemas autónomos.

EGP: Exterior Gateway Protocol, es el término usado para identificar al protocolo de ruteo implementado entre dos redes bajo el control de dos organizaciones diferentes (entre 2 sistemas autónomos diferentes).

IGP: Interior Gateway Protocol, hace referencia a los protocolos de ruteo usados dentro de un sistema autónomo.

ISP: Internet Service Provider, el proveedor de servicios de internet es una empresa que brinda conexión a internet a sus clientes.

Internet: Unión de intranets alrededor del mundo.

Intranet: Red privada, donde la empresa dueña de ella puede alojar servidores de uso limitado a personal interno.

AS: Por sus siglas en inglés Autonomous System o sistema autónomo, son todos los dispositivos, equipos y redes controlados por una organización que poseen políticas de ruteo propias e independientes de otra entidad u organización

ASN: Por sus siglas en inglés Autonomous System Number, es el número que identifica un sistema autónomo y es único para cada organización en todo internet, es asignado por IANA.

IANA: Internet Assigned Numbers Authority, es la entidad encargada de supervisar la asignación global de Direccionamiento IPv4 e IPv6, asignar los Números de Sistemas Autónomos, la gestión de la zona radicular en el Domain Name System (DNS), los tipos de medios, y otros símbolos y números relacionados con el Protocolo de Internet.

RIR: (Regional Internet Registry). Registros Regionales de Internet

NIR: (National Internet Registry). Registros Nacionales de Internet

LIR: (local Internet registry). Registros Locales de Internet

AFRINIC: (African Network Information Centre). Es el RIR de África.

APNIC: (Asia-Pacific Network Information Centre). Es el RIR de Asia pacífico.

ARIN: (American Registry for Internet Numbers). Es el RIR de América del norte.

LACNIC: (Latin American and Caribbean Internet Address Registry). Es el RIR de Latinoamérica y el caribe.

RIPE NCC: (Réseaux IP Européens Network Coordination Centre). Es el RIR de Europa, medio oriente y Asia central.

HOST: la palabra huésped en ingles aplicada a las redes informáticas hace referencia a cualquier dispositivo que se encuentre conectado a una red teniendo comunicación con otros host y equipos de la misma red.

Bluetooth: es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) creado por Bluetooth Special Interest Group, Inc. que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace de radiofrecuencia en la banda de los 2.4 GHz.

LAN: Red de área local (Local Area Network).

CAN: Red de área de campus (Campus Area Network).

MAN: Red de área metropolitana (Metropolitan Area Network).

WAN: Redes de área amplia (Wide Area Network).

API: interfaz de aplicación (Application Programming Interface).

OSI: (Open System Interconnection). Modelo de referencia llamado interconexión de sistemas abiertos.

ISO: (International Organization for Standarization). Organización Internacional para la Normalización.

Plug-and-play: Conexión de aplicación o servicio que no necesita de configuración adicional, solo se requiere conectar a la red y el servicio se habilitará.

MTU: (Maximum Transmission Unit). unidad máxima de transmisión.

NIC: (Network Interface Card) tarjeta de red.

LLC: (Logical Link Control). control de enlace lógico.

MAC: (Media Access Control). control de acceso al medio.

CAM: (Content-Addressable Memory). memoria de contenido direccionable.

IP: (Internet Protocol). Protocolo de internet.

IPv4: (Internet Protocol version 4). Protocolo de internet versión 4

IPv6: (Internet Protocol version 6). Protocolo de internet versión 6

CE: (Customer Edge) hacen referencia a un router demarcador en la frontera de la red del cliente.

PE: (Provider Edge) son el equipo demarcador en la frontera de la red del ISP.

TCP: (Transmission Control Protocol). Protocolo de control de transmisión.

UDP: (User Datagram Protocol). Protocolo de datagramas de usuario.

PDU: (Protocol Data Unit). Unidad de datos del protocolo.

VLAN: (Virtual Local Area Network). rede de área local virtual.

SQL: (Structured Query Language). Lenguaje de consulta estructurado.

NFC: (Network File Servicios) Servicios de archivos de red.

SCP: (Simple Communications Protocol). Protocolo de Comunicaciones Simple.

HTTP: (Hypertext Transfer Protocol). Protocolo de transferencia de Hipertexto.

SNMP: (Simple Network Management Protocol).. Protocolo simple de administración de red.

FTP: (File Transfer Protocol). Protocolo de transferencia de archivos.

SSH: (Secure Shell). Cubierta segura.

STP: (Spanning Tree Protocol). Protocolo de árbol de expansión, es un protocolo de capa 2.

BPDU: (Bridge Protocol Data Units). Unidad de datos de protocolo del puente, son enviados por un switch.

VRRP: (Virtual Router Redundancy Protocol). Protocolo de redundancia de enrutador virtual. La redundancia se brinda hacia el primer salto.

HSRP: (Hot Standby Router Protocol). Es un protocolo propietario de CISCO usado para las rdeundancias del primer salto, su comportamiento es mililar al de VRRP.

NAT: (Network Address Translation). traducción de direcciones de red es una técnica usada para el ahorro de direccionamiento público.

RIP: (Routing Information Protocol). Protocolo de Información de Enrutamiento. Es un protocolo de enrutamiento por vector distancia.

VLASM: (variable length subnet mask). Máscara de Subred de Tamaño Variable.

OSPF: (Open Shortest Path First). Abrir el Camino Más Corto Primero. Es un protocolo de entutamiento por estado de enlace.

LSDB: (Link State Database). Base de datos de estado de enlace, es un mensaje usado por los routers OSPF.

DR: (Designate Router). Enrutador Designado, es un término utilizado para en OSPF que opera en redes broadcast y se le da al router que toma el control dentro de un segmento donde convive con más routers OSPF.

BDR: (Backup Designate Router). Enrutador Designado de Respaldo, es un término utilizado para en OSPF que opera en redes broadcast y se le da al router que se encuantra de respaldo en caso que falle el router designado él tomará el control de las adyacencias de ese segmento.

CIDR: (Classless Interdomain Routing). enrutamiento entre dominios sin clase, consiste en realizar una sumarización de redes para poder reducir las tablas de ruteo en router de CORE.

TTL: (Time To Life). Es el tiempo de vida asignado en la cabecera de un paquete IP, el número establecido será igual al número de routers que pueda atravesar un paquete para llegar a su destino, después de esta cantidad el paquete será descartado.

IOS: (Internetwork Operating System). es el software utilizado en la gran mayoría de routers y switches de Cisco Systems.

GNS3: (Graphic Network Simulation 3). es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

Bibliografía

LIBROS

Redes CISCO. CCNP a fondo. Guía de estudios para profesionales.

Ernesto Ariganello, Enrique Barrientos Sevilla.

Alfaomega Grupo Editor, S.A. de C.V., México, 2010 - 924pag.

Guía de preparación para el examen de certificación CCNA R&S 200-120 v5.1

Oscar Antonio Gerometta.

Biblioteca CCNA, 895pag.

REDES CISCO Guía de estudios para la certificación CCNA routing and switching 4°Edición.

Ernesto Ariganello.

RA-MA editorial, 559pag.

PÁGINAS WEB

Sistema autónomo

https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo

Exterior Gateway Protocol (EGP)

https://www.ecured.cu/Exterior_Gateway_Protocol_(EGP)

Proveedor de servicios de Internet

https://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

Border Gateway Protocol

https://es.wikipedia.org/wiki/Border_Gateway_Protocol

Number Resources

https://www.iana.org/numbers

Lacnic. 1. Definiciones

https://www.lacnic.net/544/1/lacnic/

Registro Regional de Internet

https://es.wikipedia.org/wiki/Registro_Regional_de_Internet

Concepto de RED LAN

https://concepto.de/red-lan/

¿Qué es una red informática?

http://www.redusers.com/noticias/que-es-una-red-informatica/

Archivo:Red LAN.gif

https://es.wikipedia.org/wiki/Archivo:Red_LAN.gif

Mi Blog Educativo/Informática

http://cbtconceptosdeinternet.blogspot.com/2016/04/clasificacion-de-redes-por-su-alcance-y.html

Topologías de red

http://eveliux.com/mx/curso/topolog.html

Topología en anillo

https://moodle2017-18.ua.es/moodle/pluginfile.php/67444/mod_resource/content/7/conexiones/page_07.htm

TOPOLOGÍA DE REDES

http://topologiaderedurp.blogspot.com/

Redundancia y alta disponibilidad (I)

https://blogs.salleurl.edu/es/networking-and-internet-technologies/alta-redundancia-y-disponibilidad-i

Topologías redundantes de Capa 2

https://sites.google.com/site/cursosciscoccna/cisco-3/5-stp/1-topologias-redundantes-de-capa-2

Single/Dual Homed and Multi-homed Designs

https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/singledual-homed-and-multi-homed-designs

Red privada

https://es.wikipedia.org/wiki/Red_privada

Cisco IOS

https://es.wikipedia.org/wiki/Cisco_IOS

Lacnic. 3. Distribución de Números de Sistema Autónomo (ASN)

https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomo-asn

BGP AS Number Privados y Publicos

http://areaip.blogspot.com/2014/09/bgp-as-number-privados-y-publicos.html