

CASO DE ESTUDIO REDES Y COMUNICACIONES

Presentado por

YOHANN DAVID PARDO PINZON

OSMAN ARMANDO JIMENEZ CORTES

HANS YDIEL SANCHEZ MORA

EDWIN SMIT PATIÑO LARA

Presentado a

WILSON DANIEL GORDILLO OCHOA

UNIVERSIDAD DE CUNDIMAMARCA DE SUFAGASUGA

COMUNICACIÓN DE DATOS II

INGENIERIA DE SISTEMAS

2019

Contenido

1. DIRECCIONAMIENTO IP	3
1.2. Direccionamiento Classful	3
1.4. Cidr.....	8
1.5. Vlsn.....	9
2. PROCESO PARA LA DISTRIBUCIÓN Y ASIGNACIÓN DE DIRECCIONES IP.....	9
2.1. tabla de descripción de router Bogotá	11
3. PROTOCOLO DE ENRUTAMINETO	12
3.1. Enrutamiento Estático	14
3.2. Enrutamiento Predeterminado	15
3.3. Enrutamiento Dinámico	15
3.4. Vector Distancia.....	15
3.5. Estado de Enlace	16
3.6. Métrica	16
3.7. RIP.....	17
3.8. RIP Version 2.....	18
3.9. IGRP.....	19
3.10. OSPF.....	20
3.11. EIGRP	20
4. CONMUTACIÓN.....	21
4.1. Lans Virtuales	21
4.2. Detalles Configuración De Switchs.....	22
5. SERVIDORES	24
5.1. Dhcp.....	24
Bibliografía.....	25

1. DIRECCIONAMIENTO IP

Es un protocolo de nivel de red que nos va a permitir enviar paquetes entre redes diferentes. Estas redes pueden ser de tecnologías existentes para el direccionamiento, la forma de direccionar a los interfaces a nivel de enlace puede ser distinto dependiendo de la tecnología escogida. El protocolo IP son números de 32 bits que ofrece un espacio de direcciones único para todas las interfaces conectadas a la red. Además, se organizan en grupos o redes de forma que sea más sencillo para los encaminadores saber dónde (en qué red) está conectada la máquina de cierta IP. (D Morato, 2013).

A lo largo de la historia se han ido estableciendo formas de crear redes y subredes IP, por lo cual se nombrarán en este documento, de igual manera hay que tener claro que las técnicas actuales empleadas son el VLSM y CIDR, pero resulta útil entender los conceptos de cada una de estas técnicas. (D Morato, 2013).

1.2. Direccionamiento Classful

Originalmente Internet era la interconexión de una serie de LANs donde cada LAN tiene un router de acceso que la conecta con el backbone de Internet (en sus comienzos, ARPANET) y así con las otras redes. A cada una de estas LAN se le asigna un rango de direcciones IP. (D Morato, 2013).

Se pensó que podría haber redes de diferentes tamaños (respecto a número de hosts conectados) por tal razón se crearon 3 tipos de redes: Clase A, Clase B y clase C.

- *En las direcciones de una red de clase A:* El primer bit vale siempre 0 con lo que el primer byte puede ir de 0 a 127, junto con los siguientes 7 bits forman el identificador de la red o Network ID, donde los últimos 24 bits son el identificador del host o Host ID, y en algunas direcciones son especiales: la dirección de Host ID=0 es la dirección que hace referencia a toda la red, la dirección de Host ID="todo 1s en binario" es la dirección que hace referencia a todos los hosts de la red (dirección de broadcast de red), dentro de cada red hay $2^{24}=16.777.216$, más de 16 millones de direcciones IP posibles con lo que podríamos tener $2^{24}-2$ hosts (la dirección de la red y la de broadcast no son válidas para hosts), algunos identificadores de red están reservados y tienen un significado especial: El Network ID=0 hace referencia a "esta red", la red en la que se esté y el Network ID=10 está reservado para redes privadas, y el Network ID=127 está reservado para los interfaces de loopback. (D Morato, 2013).
- *En las direcciones de una red de clase B:* Los dos primeros bits valen siempre 10 con lo que el primer byte vale siempre entre 128 y 191, junto con los siguientes 14 bits forman el identificador de la red o network id, los últimos 16 bits son el identificador del host o Host ID y para algunas direcciones son especiales: la dirección de Host id=0 es la dirección que hace referencia a toda la red, en la dirección de Host id="todo 1s en binario" es la dirección de broadcast de la red, dentro de cada red hay $2^{16}-2=65.534$ direcciones IP posibles para hosts, algunos identificadores de red están reservados tienen un significado especial: por ejemplo el network id=169.254 se emplea cuando el

host no obtiene configuración IP ni manual ni automática, y los Network id`s desde 172.16 a 172.31 están reservados para redes privadas, de igual manera hay $2^{24}-2=16.777.216$ posibles redes de clase B. (D Morato, 2013).

- *En las direcciones de una red de clase C:* Los tres primeros bits valen siempre 110 con lo que el primer byte vale siempre entre 192 y 223, es así que junto con los siguientes 21 bits forman el identificador de la red o Network id, los últimos 8 bits son el identificador del host o Host y algunas direcciones son especiales: La dirección de red Host ID=0 y la de Broadcast (todo 1s). Dentro de cada red hay $2^{24}-2=16.777.216$ direcciones IP posibles para hosts, algunos identificadores de red están reservados y tienen un significado especial, por ejemplo, el network ID=192.0.2 se llama la “TEST-NET”, se emplea en ejemplos de documentación y no en Internet, Los Network IDs desde 192.168.0 a 192.168.255 están reservados para redes privadas • Los Network IDs 192.18.0 y 192.19.255 están reservados para pruebas de prestaciones de equipos de red - Hay $2^{24}-2=16.777.216$ posibles redes de clase C. (D Morato, 2013).
- *Existe lo que se llama la Clase D:* Se emplean para el Multicast IP - Junto con los siguientes 28 bits forman el identificador de un Grupo Multicast bit 0 bit 31 1110 Grupo multicast, los cuatro primeros bits valen siempre 1110 con lo que el primer byte vale siempre entre 224 y 239.
- *Existe lo que se llama la Clase E:* Están “reservadas para su futuro uso”, los cuatro primeros bits valen siempre 1111 con lo que el primer byte vale siempre al menos 240 • Hay una dirección IP más que es especial, la todo 1s: 255.255.255.255 - Se llama la dirección de “broadcast limitado” - Hace

referencia a todos los hosts de la red - Paquetes a esa dirección destino nunca deben ser reenviados por los routers. . (D Morato, 2013).

Los routers emplean el Network ID para decidir por dónde deben reenviar un paquete, cuando reciben un paquete deben averiguar rápidamente cuál es el Network ID de la red a la que pertenece el destino, si el primer bit es un 0 entonces pertenece a una red de clase A y el NetID son los primeros 8 bits, si el primer bit es un 1 pero el segundo un 0 entonces pertenece a una red de clase B y el NetID son los primeros 16 bits, si los dos primeros bits son 1 pero el tercero es un 0 entonces pertenece a una red de clase C y el NetID son los primeros 24 bits. En la propia dirección IP está codificado el número de bits del NetID, Son comprobaciones rápidas de realizar, Cuanto menos tiempo emplee el router con cada paquete más paquetes podrá procesar por segundo. . (D Morato, 2013).

- **¿Cómo actúan los host?**

Tienen configurado su dirección IP, la dirección IP que tiene el router de salida de su LAN en el interfaz conectado a la misma, pueden averiguar el NetID de su LAN a partir de su IP, dada la IP del destino al que desean enviar un paquete, se calculan el NetID de la red a la que pertenece, ¿Es el mismo que el de mi red? si está en mi red, se lo envío directamente (a su MAC), si está en otra red, se lo envío al router (a la MAC del router). . (D Morato, 2013).

- **¿Cómo actúan los routers?**

Sin estado, toman decisiones paquete a paquete. Tienen configurado la dirección IP de cada uno de sus interfaces (cada interfaz está en una LAN y por lo tanto tiene una IP de dentro de esa LAN, una tabla de rutas que indica por dónde enviar el paquete según el destino del mismo, si recibe un paquete que no es para ninguna de sus direcciones IP Busca en la tabla si hay alguna fila que en el campo Red destino tenga esa dirección IP, y si es una ruta a ese host en concreto, lo envía según indica la fila. No calcula el NetID de la red a la que pertenece esa IP y busca una ruta a esa red en la tabla. ¿Encuentra una entrada?, Es una ruta a esa red, lo envía según indica la fila, de lo contrario busca en la tabla una ruta por defecto. ¿Encuentra una?, lo envía según indica la fila, pero si no sabe cómo hacer llegar el paquete al destino. Lo descarta (lo tira). . (D Morato, 2013).

- **Desventajas practicas del esquema Classful**

Las redes pueden llegar a ser muy grandes.

- Una red de clase A contiene direcciones para millones de hosts pero es difícil que una tecnología de LAN soporte esa cifra de máquinas conectadas
- Podemos necesitar conectar dentro de la red con otro tipo de tecnología que nos permita llegar mayores distancias
- Puede que el tráfico de broadcast a nivel de enlace sea demasiado abundante y queramos reducir el tamaño de la red. . (D Morato, 2013).

1.3. Subneting

Empezó como una solución interna practicada por algunas redes muy grandes hasta que se estandarizó. También llamado FLSM (Fixed Length Subnet Masks). Desde el exterior es como si la LAN no hubiera cambiado, y en el interior se divide la LAN en LANs más pequeñas interconectadas por routers. . (D Morato, 2013).

Generalmente se aplicó en redes de clase B porque las redes de clase A eran muy pocas y las de clase C son muy pequeñas (solo 254 hosts). Lo que se hace es dividir la parte del HostID en dos: bit 0 bit 31 10 Network ID Host ID, a la primera parte se le llama el Subnetwork ID e identifica a la Subred dentro de la Red Subnetwork ID y a la segunda parte es el Host ID e identifica al host dentro de la Subred Host ID, la concatenación del Network ID y el Subnetwork ID se le llamó el Extended Network ID. . (D Morato, 2013).

1.4. CIDR

Es posible gracias a que existen nuevos protocolos de routing que permiten el envío de máscaras de subred. Si una empresa necesita múltiples clase C consecutivas se asignarán sin necesidad de utilizar una clase B y se utilizara como una única red. ARIN, RIPE y APNIC procuran asignar espacios consecutivos a los ISP, de forma que esto reduzca las tablas de routing de internet.

Tenemos que tener en cuenta que si una empresa cambia de ISP cambiara también de espacio de direccionamiento IP.

Algunas ventajas del prefijo de routing CIDR, es que se utiliza para reducir el tamaño de las tablas de routing. Esta técnica permite que los routers de internet tengan solo

240.000 para definir el total de internet y consiste en agrupar las redes a la máscara menos restrictiva posible. 1) reducción de las tablas de routing. 2) menos sobre carga en términos de tráfico, CPU y memoria. 3) Mayor flexibilidad en el direccionamiento de las redes.

1.5. VLSM

El subneting IP hace referencia a como a como están direccionadas las redes IP.

Una subred puede ser utilizada como dirección de host o hacer subnetting.

Originalmente no se podían utilizar porciones de subred todo 1s o todos 0s, para poderlas utilizar hay que usar el comando ip subnet-zero. El protocolo de routing debe llevar la máscara en sus actualizaciones. Múltiples subredes que se quieran sumarizar deben de tener los mismos bits de mayor peso.

Las dimensiones de routing se realizan para la subred completa, el router escoge de la máscara más restrictiva a la menos restrictiva para realizar sus decisiones.

2. Proceso Para la Distribución y Asignación de Direcciones IP.

Para calcular el número de hosts de cada una las redes, se utilizará como base la variable **X** que será el resultado de sumar los tres últimos dígitos del documento de identidad de cada uno de los estudiantes que componen el grupo, multiplicado por diez (10). En caso de que la variable **X** resulte inferior a 3000, los estudiantes solicitarán al profesor la asignación de un valor para dicha variable.

Tabla 1

NOMBRES Y APELLIDOS	ÚLTIMOS TRES DÍGITOS DOC. ID
Osman Armando Jiménez Cortes	370
Yohann David Pardo Pinzón	983
Edwin Smit Patiño Lara	048
Hans Yamile Sánchez Mora	258
SUMA * 10	16590

La siguiente tabla muestra los requisitos de host para cada una de las redes con base en la variable **X**. Es de resaltar que se tiene en cuenta los segmentos de red libre, pensando en el crecimiento de la red de la universidad, asegurando de esta forma la escalabilidad de la misma.

Tabla 2

RED	FACTOR	TOTAL HOST REQUERIDOS	CANTIDAD DE HOST
Administrativa – Bogotá	2X	33180	65536
Segmento libre 1	2X	33180	65536
Usuarios – Bogotá	X	16590	32768
Segmento libre 2	X	16590	32768
Administrativa – Pereira	X/2	8295	16384
Segmento libre 3	X/2	8295	16384
Usuarios – Pereira	X/4	4147	8192
Administrativa – Girardot	X/6	2765	4096
Usuarios – Girardot	X/12	1382	2048
Servidores - Bogotá	X/500	33	64
Servidores - Pereira	X/1000	17	32
Servidores - Girardot	X/1000	17	32

Se define la red **10.0.0.0** con mascara de subred **255.0.0.0**, clase **A**. Para lo cual se realiza una tabla en la que figuran todas las subredes posibles que satisfagan los requisitos de la Universidad, utilizando un diseño VLSM.

Tabla 3

DIRECCION DE SUB RED	MASCARA DE HOST	MASCARA DE SUB RED	DIRECCION DE HOST	BROADCAST
10.0.0.0	/16	255.255.0.0	10.0.0.1 - 10.0.255.254	10.0.255.255
10.1.0.0	/16	255.255.0.0	10.1.0.1 - 10.1.255.254	10.1.255.255
10.2.0.0	/17	255.255.128.0	10.2.0.1 - 10.2.127.254	10.2.127.255
10.2.128.0	/17	255.255.128.0	10.2.128.1 - 10.2.255.254	10.2.255.255
10.3.0.0	/18	255.255.192.0	10.3.0.1 - 10.3.63.254	10.3.63.255
10.3.64.0	/18	255.255.192.0	10.3.64.1 - 10.3.127.254	10.3.127.255
10.3.128.0	/19	255.255.224.0	10.3.128.1 - 10.3.159.254	10.3.159.255
10.3.160.0	/20	255.255.240.0	10.3.160.1 - 10.3.175.254	10.3.175.255
10.3.176.0	/21	255.255.248.0	10.3.176.1 - 10.3.183.254	10.3.183.255
10.3.184.0	/26	255.255.255.192	10.3.184.1 - 10.3.184.62	10.3.184.63
10.3.184.64	/27	255.255.255.224	10.3.184.65 - 10.3.184.94	10.3.184.95
10.3.184.96	/27	255.255.255.224	10.3.184.97 - 10.3.184.126	10.3.184.127

2.1. tabla de descripción de router

Tabla 4

BOGOTÀ

TIPO Y N° DE INTERFAZ	DCE / DTE	CLOCK RATE	NOMBRE RED	DIRECCIÓN RED	DIR IP INTERFAZ	MÁSCARA SUBRED
Se6/0	DCE	128000	BOGOTÀ-ISP	172.1.1.0	172.1.1.2	/30
Se2/0	DTE	N/A	BOGOTÀ-GIRARDOT	172.1.1.4	172.1.1.5	/30
Se3/0	DTE	N/A	BOGOTÀ-PEREIRA	172.1.1.12	172.1.1.14	/30
Gig7/0	N/A	N/A	BOGOTÀ LAN	10.0.0.0	10.0.0.1	/16

Tabla 5

GIRARDOT

TIPO Y N° DE INTERFAZ	DCE / DTE	CLOCK RATE	NOMBRE RED	DIRECCIÓN RED	DIR IP INTERFAZ	MÁSCARA SUBRED
Se3/0	DCE	128000	GIRARDOT-BOGOTA	172.1.1.4	172.1.1.6	/30
Se2/0	DCE	128000	GIRARDOT-PEREIRA	172.1.1.8	172.1.1.9	/30
Gig9/0	N/A	N/A	GIRARDOT LAN	10.3.176.0	10.3.176.1	/21

Tabla 6 **ISP**

TIPO Y N° DE INTERFAZ	DCE / DTE	CLOCK RATE	NOMBRE RED	DIRECCIÓN RED	DIR IP INTERFAZ	MÁSCARA SUBRED
Se2/0	DTE	N/A	ISP-BOGOTÀ	172.1.1.0	172.1.1.1	/30
Se7/0	DCE	128000	ISP-NUBE	200.21.30.0	200.21.30.2	/24

Tabla 7 **PEREIRA**

TIPO Y N° DE INTERFAZ	DCE / DTE	CLOCK RATE	NOMBRE RED	DIRECCIÓN RED	DIR IP INTERFAZ	MÁSCARA SUBRED
Se3/0	DTE	N/A	PEREIRA-GIRARDOT	172.1.1.8	172.1.1.10	/30
Se2/0	DCE	128000	PEREIRA-BOGOTÀ	172.1.1.12	172.1.1.13	/30
Gig7/0	N/A	N/A	PEREIRA LAN	10.3.128.0	10.3.128.1	/19

Tabla 8

ENLACES					
RED	DIRECCION DE SUB RED	MASCARA DE HOST	MASCARA DE SUB RED	DIRECCION DE HOST	BROADCAST
INTERNET-ISP	200.21.30.0	/24	255.255..255.0	200.21.30.1-200.21.30.2	200.21.30.3
ISP-BOGOTA	172.1.1.0	/30	255.255.255.252	172.1.1.1 - 172.1.1.2	172.1.1.3
BOGOTA-GIRARDOT	172.1.1.4	/30	255.255.255.252	172.1.1.5 - 172.1.1.6	172.1.1.7
GIRARDOR-PEREIRA	172.1.1.8	/30	255.255.255.252	172.1.1.9 - 172.1.1.10	172.1.1.11
PEREIRA-BOGOTA	172.1.1.12	/30	255.255.255.252	172.1.1.13 - 172.1.1.14	172.1.1.15

3. PROTOCOLO DE ENRUTAMINETO

La Universidad desea que se recomiende un protocolo de enrutamiento para la red, que sea el más adecuado para las condiciones que se tienen, sin embargo, es de tener en cuenta que se debe realizar el enrutamiento estático como media ante la contingencia de

una falla con el protocolo seleccionado. La elección del protocolo estará condicionada al resultado de la valoración que se obtenga en la siguiente tabla:

Tabla 9

PROTOCOLO DE ENRUTAMIENTO	CARACTERÍSTICAS PRINCIPALES	VENTAJAS	DESVENTAJAS	VALORACIÓN
RIP	<ul style="list-style-type: none"> es ideal para redes pequeñas. el número de saltos máximo hacia un destino es 15. Protocolo Abierto. Distancia Administrativa: 120 Actualizaciones cada 30 segundos 		<ul style="list-style-type: none"> Solo sirve para redes pequeñas. No Permite VLSM, CIDR 	0
PROTOCOLO DE ENRUTAMIENTO	CARACTERÍSTICAS PRINCIPALES	VENTAJAS	DESVENTAJAS	VALORACIÓN
RIP VERSION 2	<ul style="list-style-type: none"> Envía las Actualizaciones en forma de Multicast. Protocolo sin clase. 	<ul style="list-style-type: none"> Permite VLSM, CIDR. 	<ul style="list-style-type: none"> No es adecuado para ser usado en un AS. 	2
IGRP	<ul style="list-style-type: none"> Se considera el ancho de banda a confiabilidad para crear una métrica compuesta Ancho de Banda (BandWidth – Bw) 	<ul style="list-style-type: none"> Fiabilidad: va de 0 a 255, donde 255 es 100% confiable. 		3
OSPF	<ul style="list-style-type: none"> Reconoce conexiones de líneas punto a punto entre dos dispositivos de encaminamiento. Actualizaciones de estado de enlace. Descripción de la base de datos. Solicitud de estado de enlace. 	<ul style="list-style-type: none"> se usa muy frecuentemente como protocolo de encaminamiento interior en redes encontrar la trayectoria más corta. Bajo consumo de ancho de banda 		5
EIGRP	<ul style="list-style-type: none"> Utiliza el Algoritmo de actualización 	<ul style="list-style-type: none"> Permite VLSM, CIDR. 	<ul style="list-style-type: none"> Propietario cisco 	

	<p>difusa (DUAL) para el cálculo de la ruta más corta</p> <ul style="list-style-type: none"> Las actualizaciones son mensajes de multicast a la dirección generadas por cambios en la topología 	<ul style="list-style-type: none"> Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace. 		4
--	--	---	--	---

Se decide optar por implementar el protocolo OSPF, entendiendo que se adapta muy bien a la necesidad de la universidad, además es uno de los protocolos que se usa por excelencia en empresas que están proyectadas a seguir creciendo, lo que infiere en la escalabilidad de la red.

Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento. Dicha información se usa para construir y mantener las tablas de enrutamiento. (Modesto. L. 2013).

3.1. Enrutamiento Estático

El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.

- Un cliente no desea intercambiar información de enrutamiento dinámico. (Modesto. L. 2013).

3.2. Enrutamiento Predeterminado

Es una ruta estática que se refiere a una conexión de salida o Gateway de “último recurso”. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0. .(Modesto. L. 2013).

3.3.Enrutamiento Dinámico

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero. .(Modesto. L. 2013).

3.4. Vector Distancia

Determina la dirección y la distancia hacia cualquier enlace de la red. Su métrica se basa en lo que se le llama en redes “Numero de Saltos”, es decir la cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino, la ruta que tenga el menor número de saltos es la más óptima y la que se publicará.

- Visualiza la red desde la perspectiva de los vecinos
- Actualizaciones periódicas
- Transmite copias completas o parciales de las tablas de enrutamiento
- Convergencia lenta
- Incrementa las métricas a través de las actualizaciones. .(Modesto. L. 2013).

3.5. Estado de Enlace

También llamado “Primero la Ruta Libre Más Corta” (OSPF – Open Shortest Path First), recrea la topología exacta de toda la red. Su métrica se basa el retardo, ancho de banda, carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra. Estos protocolos utilizan un tipo de publicaciones llamadas Publicaciones de estado de enlace (LSA), que intercambian entre los routers, mediante estas publicaciones cada router crea una base datos de la topología de la red completa. - Buscan una unión común de la topología de la red.

- Cada dispositivo calcula la ruta más corta a los otros routers.
 - Las actualizaciones se activan por los eventos (cambios en la topología) de la red.
- (Modesto. L. 2013).

3.6. Métrica

La métrica es el análisis, y en lo que se basa el algoritmo del protocolo de enrutamiento dinámico para elegir y preferir una ruta por sobre otra, basándose en eso el protocolo creará la tabla de enrutamiento en el router, publicando sólo las mejores rutas.

Un protocolo de enrutamiento utiliza métrica para determinar qué vía utilizar para transmitir un paquete a través de un Intercambio. Las métricas utilizadas por protocolos de enrutamiento incluyen:

- Numero de saltos: Número de routers por los que pasará un paquete.
- Pulsos: Retraso en un enlace de datos usando pulsos de reloj de PC.
- Coste: Valor arbitrario, basado generalmente en el ancho de banda, el coste económico u otra medida.
- Ancho de banda: Capacidad de datos de un enlace.
- Retraso: Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- Carga: Cantidad de actividad existente en un recurso de red, como un router o un enlace.
- Fiabilidad: Se refiere al valor de errores de bits de cada enlace de red.
- MTU: Unidad máxima de transmisión. Longitud máxima de trama en octetos que puede ser aceptada por todos los enlaces de la ruta. (Modesto. L. 2013).

3.7. RIP

RIP, es un protocolo de enrutamiento Dinámico de vector distancia, esto quiere decir que su métrica para llegar a una red destino se basa en el número de saltos. Es un protocolo abierto a diferencia de por ejemplo IGRP y EIGRP que son propietarios de Cisco. Es relativamente simple ideal para redes pequeñas, el número de saltos máximo hacia un destino es 15 (cuando hablo de numero de saltos, me refiero a la cantidad de

router, por la que tiene que atravesar el paquete para llegar a destino), ya con 16 la red se declara como inalcanzable. Existen dos versiones de este protocolo versión 1 y 2, la diferencia más importante, es que RIP v1 es lo que se llama un Protocolo con clase, lo que significa que cuando publica las tablas de enrutamiento, este no adjunta las máscaras de subred. En cambio, Rip v2 es un Protocolo sin clase, que, si adjunta la máscara de subred, por lo que permite el uso de VLSM, CIDR, summarización. Otra diferencia es que RIP v1 publica sus actualizaciones en forma de Broadcast, es decir a todos los equipos de la red, mientras que RIP v2 lo hace en modo de Multicast, es decir solo a un grupo de host de una red. Resumiendo, las características de las 2 versiones:

RIP Versión 1: - Protocolo Abierto - Distancia Administrativa:120 - Protocolo con clase
- Métrica numero de saltos - Actualizaciones cada 30 segundos - Envía las Actualizaciones en forma de Broadcast - Numero Máximo de Saltos 15. (Modesto. L. 2013).

3.8. RIP VERSION 2

Routing Information Protocol version 2 (RIPv2) es uno de los protocolos de enrutamiento interior más sencillos y utilizados. Esto es particularmente verdadero a partir de la versión 2 que introduce algunas mejoras críticas que la constituyeron en un recurso necesario para cualquier administrador de redes.

El dispositivo envía su tabla de enrutamiento completa a todos los vecinos conectados cada 30 segundos. Puede haber actualizaciones disparadas por eventos si, por ejemplo, una interfaz cae antes de que expire el timer de 30 segundos.

Por ser un protocolo de vector distancia, es sensible a la aparición de bucles de enrutamiento. Esto es consecuencia de la inexistencia de relaciones de vecindad o

recálcalos de la topología de la red, como ocurre con los protocolos de estado de enlace.

Esto afecta directamente la calidad de la información de enrutamiento que proporciona RIP.

Soporte para VLSM.

Actualizaciones de enrutamiento por multicast.

Actualizaciones de enrutamiento con autenticación con clave encriptada. (Malkin, G.1994).

3.9. IGRP

El Interior Gateway Routing Protocol (IGRP) es un protocolo patentado desarrollado por Cisco. Las características principales de diseño del IGRP son las siguientes:

Se considera el ancho de banda, el retardo, la carga y la confiabilidad para crear una métrica compuesta. Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos. El IGRP es el antecesor de EIGRP y actualmente se considera obsoleto. IGRP es un protocolo de métrica vector-distancia, perteneciente a Cisco, utilizado para el intercambio de información entre routers. Lo que se encarga de hacer es buscar la mejor vía de envío mediante el algoritmo de métrica vector-distancia. (D Morato, 2013).

3.10. OSPF

es un protocolo de enrutamiento interior altamente flexible y escalable que permite interconectar diferentes tipos de redes de una organización (o las redes de un proveedor de Internet) para obtener una sola red unificada basada en el protocolo IP (lo que comúnmente se denomina intranet). El protocolo OSPF posibilita que el intercambio de información de enrutamiento quede confinado a los equipos que pertenecen a una misma área y que se pueda obtener información de otras áreas por medio de los encaminadores de borde de área (que interconectan dichas áreas). La motivación del presente capítulo se orienta a que el lector gane experiencia en la interconexión de redes basadas en IP mediante el uso del protocolo de enrutamiento OSPF, razón por la que se aborda la configuración de OSPF para operar en el ambiente de área cero y en el ambiente multi-área. (Buriol, L. S. 2003).

3.11. EIGRP

El protocolo EIGRP es utilizado por los routers Cisco para anunciar su existencia a todos los routers vecinos. Para ello se envía vía multicast, en el interfaz habilitado para EIGRP, un mensaje de anuncio. Cuando dos routers se descubren el uno al otro, intentan intercambiar información sobre la topología de la red. En las redes Ethernet es preciso que cada router obtenga la dirección MAC de su interlocutor. Si un atacante envía una gran cantidad de mensajes de anuncio EIGRP, con direcciones IP aleatorias, todos los routers Cisco que reciban estos paquetes intentarán contactar con el dispositivo emisor. Debido a la existencia de un problema en el sistema operativo IOS, cada router obtiene la dirección MAC del emisor de forma continua hasta que no expire el periodo de tiempo indicado dentro el mensaje EIGRP. Como este valor está

establecido por el emisor del mensaje, en el caso de un ataque hemos de considerar que se utilizará el valor máximo de 18 horas. (Bautista, B. 2016).

4. CONMUTACIÓN

Tabla 10

RED	HOSTS REQUERIDOS (ÚTILES)	DIRECCIÓN DE RED	DIRECCIÓN BROADCAST	MÁSCARA SUBRED	HOST UTILIZABLES
Switches Bogotá	33180	10.1.0.0	10.1.255.255	255.255.0.0	65536
Switches Pereira	16590	10.2.128.0	10.2.255.255	255.255.128.0	32768
Switches Girardot	8295	10.3.64.0	10.3.127.255	255.255.192.0	16384

4.1. LANS VIRTUALES

Tabla 11

SEDE	SWITCH SERVIDOR	SWITCHES CLIENTE	DOMINIO VTP	VERSIÓN VTP	CONTRASEÑA VTP
Bogotá	Servidores B	AdministrativaB- usuarios B	ucundinamarca	Versión 2	unicundi2019
Pereira	Servidores P	AdministrativaP- usuarios P	ucundinamarca	Version 2	unicundi2019
Girardot	Servidores G	AdministrativaG- usuarios G	ucundinamarca	Version 2	unicundi2019

4.2. Detalles Configuración De Switchs

Sede: Bogotá

Tabla 12

Nombre Switch	Modelo	Nº Ptos	Piso	Dir Ip	Gateway	VTP Modo	ST P Raíz	Ptos Trunk	Ptos VLAN
Administrativa B	Catalyst 2950 series	24	2	10.0.0.2	10.0.0.1	cliente	no	Feth0/1-5, Geth0/1	Feth0/9-24 vlan20
Usuarios B	Catalyst 2950 series	24	1	10.2.0.4	10.2.0.1	cliente	no	Feth0/1-4	Feth0/9-24 vlan10
Servidores B	Catalyst 2950 series	24	8	10.3.184.7	10.3.184.1	servidor	raíz	Feth0/1-4	Feth0/9-24 vlan30

Sede: Girardot

Tabla 13

Nombre Switch	Modelo	Nº Ptos	Piso	Dir Ip	Gateway	VTP Modo	ST P Raíz	Ptos Trunk	Ptos VLAN
Administrativa G	Catalyst 2950 series	24	2	10.3.160.2	10.3.160.1	cliente	no	Feth0/1-4, Geth0/1	Feth0/9-24 vlan20
Usuarios G	Catalyst 2950 series	24	1	10.3.176.4	10.3.176.1	cliente	no	Feth0/1-4	Feth0/9-24 vlan10
Servidores G	Catalyst 2950 series	24	8	10.3.184.9	10.3.184.7	servidor	raíz	Feth0/1-4	Feth0/9-24 vlan30

Sede: Pereira

Tabla 14

Nombre Switch	Modelo	Nº Ptos	Piso	Dir Ip	Gateway	VTP Modo	ST P Raíz	Ptos Trunk	Ptos VLAN
Administrativa P	Catalyst 2950 series	24	2	10.3.0.2	10.3.0.1	cliente	no	Feth0/1-4, Geth0/1	Feth0/9-24 vlan20
Usuarios P	Catalyst 2950	24	1	10.3.128.4	10.3.128.1	cliente	no	Feth0/1-4	Feth0/9-24 vlan10

	mseries								
Servidores P	Catalyst 2950 mseries	24	8	10.3.184.67	10.3.184.65	servidor	raiz	Feth0/1-4	Feth0/9-24 vlan30

5. SERVIDORES

Tabla 14

Servidor	Ciudad Ubicación	Servicios	Dirección IP	Puertos
WEB G	GIRARDOT	http	10.3.176.2	Feth0/24
WEB P	PERERIRA	http	10.3.184.66	Feth0/24
FTP B	BOGOTÀ	FTP	10.3.184.2	Feth0/24
MySQL	BOGOTÀ	BD	10.3.184.3	Feth0/21
HTTP y DNS	BOGOTÀ	HTTP - DNS	10.3.184.4	Feth0/23
TFTP	BOGOTÀ	TFTP	10.2.184.5	Feth0/22

5.1. DHCP

Tabla 15

Nombre del Pool DHCP	Dirección de Red / Máscara	Direcciones Excluidas	Nombre Dominio	Gateway por defecto	Servidor DNS
Vlan10	10.2.0.0/17	10.2.0.1 - 10.2.0.10	Sw_userb	10.2.0.1	10.3.184.4
Vlan20	10.0.0.0/16	10.0.0.1 - 10.0.0.10	Sw_adminb	10.0.0.1	10.3.184.4
Vlan30	10.3.184.0/26	10.3.184.1 - 10.3.184.10	Sw_servidoresb	10.3.184.1	10.3.184.4

Bibliografía

- Luis Modesto González Lucas. (2013). PROTOCOLOS DE ENRUTAMIENTO. IES Los Viveros Dpto. Electrónica.
- Morató, D., & de Redes, L. D. P. (2013). Direccionamiento IP. 2da Parte.
- Malkin, G. (1994). Routing Information Protocol Version 2 (RIP v2). RFC 1723, November.
- Buriol, L. S. (2003). Roteamento do tráfego na internet: algoritmos para projeto e operação de redes com protocolo OSPF.
- Bautista, B. (2016). Diseño y simulación de una topología y gestión de red basadas en túneles GRE y enrutamiento dinámico OSPF Y EIGRP, caso de estudio–grupo automotriz Eljuri (Master's thesis, PUCE).