CONFIGURACIÓN Y OPTIMIZACIÓN DE SWITCHES ADMINISTRABLES MULTICAPA PARA GARANTIZAR TOLERANCIA A FALLAS, ESCALABILIDAD, Y CALIDAD EN EL SERVICIO.

ALESSANDRO BARSOTTI HERRERA
MIGUEL ANGEL MARTELO QUIROZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
PROGRAMA DE INGENIERÍA DE SISTEMAS
MINOR DE TELECOMUNICACIONES Y REDES
CARTAGENA DE INDIAS D.T. Y C
2012

CONFIGURACIÓN Y OPTIMIZACIÓN DE SWITCHES ADMINISTRABLES MULTICAPA PARA GARANTIZAR TOLERANCIA A FALLAS, ESCALABILIDAD Y CALIDAD EN EL SERVICIO.

ALESSANDRO BARSOTTI HERRERA
MIGUEL ANGEL MARTELO QUIROZ

ASESOR:
GONZALO GARZÓN
INGENIERO DE SISTEMAS

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
PROGRAMA DE INGENIERÍA DE SISTEMAS
MINOR DE TELECOMUNICACIONES Y REDES
CARTAGENA DE INDIAS D.T. Y C
2012

Nota de aceptación

_____

_____

_____

_____

Jurado

_____

_____

_____

_____

ARTICULO 105

La Universidad Tecnológica de Bolívar, se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados, y no se pueden ser explotados comercialmente sin autorización.

DEDICATORIA

A Dios por bendecirme, cuidarme y permitirme siempre ser la persona que soy hoy día.

A mi madre Vivian Herrera Plaza por permitirme la vida, por enseñarme a ser una persona de bien y por su apoyo incondicional durante toda mi carrera estudiantil.

A mi tía Damaris Herrera Plaza por apoyarme siempre y enseñarme que las cosas en la vida se ganan con mucho esfuerzo, sacrificio y trabajo.

A mi abuela Dabeiba Plaza por cuidarme siempre y mantenerme en el camino del bien.

A mi primo Juan Guillermo Muñoz Herrera por ser parte fundamental en mi vida.

A mi novia Yesenia Sierra Marrugo por brindarme su apoyo incondicional en toda mi carrera universitaria.

A mis profesores Moises Quintana, Issac Zuñiga, Giovanni Vasquez, Efrain Herrera, Luz Estella Robles, Gonzalo Garzon por enseñarme todos sus conocimientos durante mi carrera de ingeniería de sistemas.

A la universidad tecnológica de bolívar por darme la oportunidad de ser parte de tan prestigioso lugar.

ALESSANDRO BARSOTTI HERRERA

DEDICATORIA

Primero que todo agradecer a Dios por permitirme existir y llegar hasta donde he llegado e ir cumpliendo mis metas paso a paso.

A mi Madre Leslie Quiroz por regalarme la vida y estar siempre acompañándome en todo momento y brindándome el apoyo necesario para seguir adelante.

A mi abuelo Pablo Justiniano Quiroz Cabrera (Q.E.P.D), por enseñarme todos los valores que una buena persona debe tener para ser integra y por todo el apoyo que me da y me sigue dando desde arriba.

A mi abuela Leticia Mariano de Quiroz, quien siempre me acompaña en todos mis caminos y me brinda su apoyo incondicionalmente.

A mis Tías Mabel y Alexis Quiroz y Tíos Pablo y Vladimir Quiroz por regalarme ese cariño que siempre me brindan y apoyarme siempre fuera cual fueran los resultados y los momentos.

A mi hermano Julio Andrés Jiménez Quiroz por brindarme su amor, su confianza y lealtad en todo momento y acompañarme en las buenas y en las malas.

A mis amigos quienes siempre me acompañaron y estuvieron pendiente de una u otra manera para que cumpliera esta meta y saliera adelante, a todos aquellos que pusieron su pedacito de arena para que este sueño se haga realidad.

A todo el cuerpo de docente que pusieron un grano de arena para la formación de mi persona como un gran profesional.

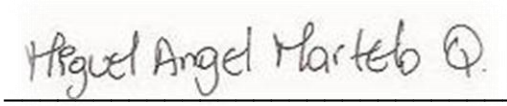
MIGUEL ANGEL MARTELO QUIROZ

AUTORIZACIÓN

Cartagena de Indias D. T. y C.

Nosotros MIGUEL ANGEL MARTELO QUIROZ, con cédula de ciudadanía 73.007.049 de Cartagena y ALESSANDRO BARSOTTI HERRERA con cédula de ciudadanía 73.009.127, autorizamos a la Universidad Tecnológica de Bolívar para hacer uso de nuestro trabajo de grado y publicarlo en el catálogo online de la biblioteca.

Cordialmente,



MIGUEL ANGEL MARTELO QUIROZ	ALESSANDRO BARSOTTI HERRERA
CC. 73.007.049 de Cartagena	CC. 73.009.127 de Cartagena

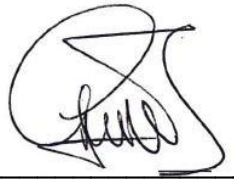
Cartagena de Indias D. T. y C.

Señores:
COMITÉ CURRICULAR
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
Ciudad

Respetados señores:

Por medio de la presente me permito hacer entrega de la monografía titulada **CONFIGURACIÓN Y OPTIMIZACIÓN DE SWITCHES ADMINISTRABLES MULTICAPA PARA GARANTIZAR TOLERANCIA A FALLAS, ESCALABILIDAD, Y CALIDAD EN EL SERVICIO.** Para su estudio y evaluación, la cual fue realizada por los estudiantes MIGUEL ANGEL MARTELO QUIROZ y ALESSANDRO BARSOTTI HERRERA y de la cual acepto ser su director.

Atentamente,



_____

ING. GONZALO GARZÓN

Cartagena de Indias D. T. y C.

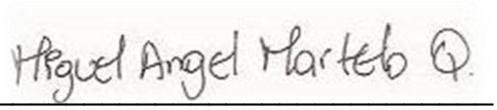
Señores:
COMITÉ CURRICULAR
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
Ciudad

Estimados Señores.

Con todo el interés me dirijo a Uds. Para presentar a su consideración, estudio y aprobación la monografía titulada **CONFIGURACIÓN Y OPTIMIZACIÓN DE SWITCHES ADMINISTRABLES MULTICAPA PARA GARANTIZAR TOLERANCIA A FALLAS, ESCALABILIDAD, Y CALIDAD EN EL SERVICIO**, como requisito para obtener el título de Ingeniero de Sistemas.

Esperamos que el presente trabajo se ajuste a las expectativas y criterios de la Universidad para los trabajos de grado.

Cordialmente,



MIGUEL ANGEL MARTELO QUIROZ
CC.1047.367.270 de Cartagena

ALESSANDRO BARSOTTI HERRERA
C.C. 73.009.127 de Cartagena

TABLA DE CONTENIDO

INDICE DE FIGURAS E ILUSTRACIONES

INTRODUCCIÓN

En la actualidad las redes son configuradas con dispositivos muy convencionales como lo son routers y switches “Plug and Play”, lo cual hace que la red funcione de manera eficaz hasta cierto crecimiento de la transferencia de datos. Cuando la transferencia de datos aumenta y el número de ordenadores conectados a la red crece, la red se ve deteriorada en cuanto a velocidad, calidad, seguridad y muchas otras cosas.

El funcionamiento de una red consiste en conectar los ordenadores y periféricos al usar 2 tipos de equipos: los *Routers* y los *Switches*. Este tipo de equipos permiten a los dispositivos que estén conectados a la red comunicarse entre sí así también como con otras redes. Existen switches que cumplen los 2 papeles al mismo tiempo, y son los denominados *Switches Administrables*, los cuales proporcionan una gran flexibilidad debido a que el switch puede ser gestionado por el administrador.

La investigación presentará la ventaja de diseñar e implementar las redes de computadores con los switches administrables que ofrecen una mayor fiabilidad, escalabilidad, calidad en el servicio y manejo en una red tanto de pequeño como de amplio alcance, ¿Por qué? Porque los switches administrables poseen características avanzadas con respecto a los switches convencionales, lo cual implica un mejor nivel de seguridad en la red en cuanto a mantenimiento, pero sobretodo en la transferencia de datos, debido a que las caídas de la red disminuyen en un alto porcentaje.

CAPITULO 1

1. EL ESTUDIO DEL SWITCH

En los inicios de la década de los años 80, con el crecimiento de la Industria, muchos centros de cómputos y salas de servidores, se encontraron con el inconveniente de tener docenas y en algunos casos cientos de monitores, teclados y ratones, ocupando mucho espacio en los Rack, incrementando innecesariamente la temperatura en el ambiente. Otro gran inconveniente fue la administración de los servidores, los técnicos necesitaban moverse de un servidor a otro, para realizar las tareas. [1]

Actualmente existe una disputa sobre quién fabricó el primer Switch KVM. Probablemente el primer nombre asignado fue *KV Switch*. El ambiente gráfico y los ratones no eran muy comunes en esa época. El primer Switch solamente soportaba teclado y vídeo. Los primeros Switch tenían botones o perillas que conmutaban entre una y otra computadora, siendo luego actualizada por funciones "Hot-Key" y finalmente por funciones en pantalla. [1]

Los Switch KVM permitían que un usuario pueda acceder a varios servidores o computadores, utilizando solamente un monitor, teclado y ratón. Además de mejorar el tiempo de administración, disminución en las emisiones de calor de los monitores y ahorrando espacio físico, se logra una reducción de costos y un ahorro en compras de monitores, teclados y ratones. [1]

Hoy en día es muy común encontrarlo en las salas de servidores *(Datacenters*), en administración de varios equipos, e incluso en pequeñas empresas y hogares.

¿Por qué son importantes los switches dentro de las redes de computadoras? Como se sabe, el funcionamiento de una red consiste en conectar los ordenadores

y periféricos al usar 2 tipos de equipos: los routers y los switches, este tipo de equipos permiten a los dispositivos que estén conectados a la red comunicarse unos con otros, así como con otras redes. Los switches son “El Corazón de las Redes” Ahora bien, existen switches que cumplen los 2 papeles al mismo tiempo, y son los denominados switches administrables, los cuales proporcionan una gran flexibilidad debido a que el switch puede ser gestionado por el administrador. Esto le da una gran importancia dentro de la correcta administración y configuración de una red.

¿Pero que es un Switch? Un switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. [2]

1.1 CLASIFICACIÓN DE LOS SWITCHES.

Se tiene una gran variedad de switches con distintas características y por ello distintos criterios de clasificación, los cuales son:

1.1.1 Por el Tipo de Administración:

1.1.1.1 Switches Administrables: Aquellos que permiten cierta funcionalidad de administración del switch.

1.1.1.2 Switches No Administrables: Son aquellos que no permiten ninguna o escasa funcionalidad de configuración y administración.

1.1.2 Por la Capacidad:

1.1.2.1 Switches Apilables: Permiten agrupar varias unidades sobre un bus de expansión, el bus debe proporcionar suficiente ancho de banda para manejar

comunicaciones full-duplex. Se recomienda comprarlos del mismo fabricante para evitar problemas de administración global e intercomunicación entre los switches. Por lo general son switches administrables.

***1.1.2.2 Switches No Apilables*:** Son aquellos que no soportan un bus de expansión.

1.1.3 Por la Modularidad:

***1.1.3.1 Switches Modulares*:** Tienen la capacidad de soportar la agregación de puertos, como nuevos módulos, por lo general son switches multicapa que trabajan en las capas 2, 3, u otras superiores (Modelo OSI). Son comúnmente usados como switches de troncal (Backbone ó columna vertebral de la red). Por lo general son switches administrables.

1.1.3.2 Switches No Modulares: no poseen ninguna capacidad de agregación de módulos.

1.1.4 Por la Capacidad de Tráfico:

Se clasifican por las velocidades con las que trabajan, siendo estas 10, 100 y 1000 Mbps Los de mayor velocidad por lo general son utilizados como switch de troncal (Backbone), pueden ser Switches Modulares y Administrables.

Existen 2 métodos para clasificar los switches, en cuanto al *método de direccionamiento de los paquetes utilizados* existen: *Store-and-Forward, Cut-Through o Adaptative Cut Through.* Y en cuanto a *la segmentación de las subredes están los de* Layer 2 (Capa 2), Layer 3 (Capa 3), y Layer 4 (Capa 4) [3]

1.1.4.1 Store-and-Forward

En estos switches, los paquetes se guardan en un buffer antes de ser transportados hacia el puerto de salida. Mientras el paquete está en el buffer, el switch calcula el CRC y mide el tamaño del paquete. Si el CRC falla, o el tamaño es muy pequeño o muy grande, el paquete es descartado. De lo contrario, el paquete es encaminado hacia el puerto de salida. Este método asegura operaciones sin error y aumenta la confianza de la red. La única desventaja es que el tiempo utilizado para “guardar” y “chequear” cada paquete conlleva a un tiempo adicional lo cual causa una demora en el procesamiento de dichos paquetes.

1.1.4.2 Cut-Through

Los Switches *Cut-Through* fueron proyectados para reducir esta demora. Estos switches minimizan el delay leyendo sólo los 6 primeros bytes de datos del paquete, que contiene la dirección de destino, e inmediatamente mandan el paquete. Pero tiene un problema, que no detecta paquetes corruptos causados por colisiones (conocidos como Runts), ni errores de CRC. Cuanto mayor es el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar paquetes corruptos. Para solucionar el problema de los Runts, se crea un segundo tipo de switch Cut-Through Fragment Free el cual lee los primeros 64 bytes de cada paquete asegurando un tamaño mínimo de los paquetes, evitando la salida de Runts a la red.

En el modo adaptativo, estos switches soportan tanto Store-and-Forward como Cut-Through. Cualquiera de los modos puede ser activado por el administrador de la red, o el switch puede ser lo bastante inteligente como para escoger entre los dos métodos, basado en el número de paquetes con error que pasan por los puertos.

1.1.4.3 Layer 2 Switches

Son los switches tradicionales, que funcionan como bridges multi-puertos. Su principal finalidad es de dividir una LAN en múltiples dominios de colisión, o, en los casos de las redes en anillo, segmentar la LAN en diversos anillos.

Los switches de capa 2 posibilitan, por lo tanto, múltiples transmisiones simultáneas sin embargo, no consiguen filtrar broadcasts, multicasts (en el caso en que más de una sub-red contenga las estaciones pertenecientes al grupo multicast de destino), ni cuadros cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

1.1.4.4 Layer 3 Switches

Además de las funciones tradicionales de la capa 2, incorporan algunas funciones de ruteo, como por ejemplo la determinación del camino de repaso basado en informaciones de capa de red, validación de la integridad del cableado por checksum, y soporte a los protocolos de ruteo tradicionales (RIP, OSPF, etc.)

Los switches de capa 3 soportan también la definición de redes virtuales (VLAN's), y posibilitan la comunicación entre las diversas VLAN's, sin la necesidad de utilizar un router externo. Se recomienda para la segmentación de LAN muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de performance y eficiencia de la LAN, debido a la cantidad excesiva de broadcasts.

1.1.4.5 Layer 4 Switches

Están en el mercado hace poco tiempo, y existe una controversia en relación con la adecuada clasificación de estos equipos. Muchas veces son llamados de Layer 3+ (Layer 3 Plus). Básicamente, incorpora a las funcionalidades de un switch de

capa 3 la habilidad de implementar la aplicación de políticas y filtros a partir de informaciones de capa 4 o superiores, como puertas TCP y UDP, o SNMP, FTP, etc.

1.2 SWITCHES ADMINISTRABLES

Como se dijo anteriormente, un switch es un dispositivo digital de lógica de interconexión de redes de computadores el cual posee la funcion de interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. [2]

Un switch administrable cumple con las mismas funciones de un switch normal (de capa 2) además, ofrece funciones adicionales en las diferentes capas superiores OSI, es decir, que tiene las funcionalidades de un *"router".*

La principal diferencia que existe entre un switch de capa 3 y un router en cuanto a la operación de conmutación de paquetes, es la implementación física. ¿Cómo así? En los routers, la conmutación de los paquetes se lleva a cabo utilizando el software que se ejecuta en el microprocesador, mientras que los switches de capa 3 lo hacen usando aplicaciones especificas dedicadas que se encuentran en su circuito integrado de hardware. [5]

Estos switches no se limitan a trabajar exclusivamente en la capa 3, existen switches que pueden usar funciones hasta la capa 7 y son llamados "Switches de Capa 4-7", "Switches de Contenido", "Switches de Contenido de Servicios", "Switches Web o Switches de Aplicación". Este tipo de Switches son comúnmente utilizados para lo que se denomina el "Load Balancing" ó "Balanceo de Carga" dentro de un grupo de servidores.

1.2.1 Funciones Básicas De Un Switch Multicapa

Los Switches multicapa al igual que cualquier otro switch, cumplen con 4 funciones básicas que son: Learning, Flooding, Forward y Aging. Se aprenderán estos conceptos con un ejemplo:

1.2.1.1 Learning: Se supone que se envía una trama de un nodo A hacia un nodo B, cuando la trama del nodo A llega al switch, este guarda la dirección MAC en su tabla de conmutación. Ahora el switch sabe exactamente donde se encuentra el nodo A en la red. En otras palabras el switch se aprendió la dirección del nodo A.

1.2.1.2 Flooding: Continuando con el ejemplo anterior, supongamos ahora que además del nodo B esta el nodo C. Cuando la trama del nodo A llega al Switch, éste como aun no sabe dónde está el nodo B, envía la misma trama por "todos" los puertos (Con excepción del puerto de entrada), a esto es a lo que se denomina "Flooding". Cuando la trama llega al nodo C, éste le enviará una notificación de respuesta al switch. Ahora el switch sabe la dirección del nodo B en la red.

1.2.1.3 Forward: supongamos que el nodo A quiere enviar otra trama al nodo B. Cuando la trama llega al switch busca el nodo B en la tabla de conmutación y si lo encuentra envía exclusivamente la trama a ese nodo, en otras palabras, solo se envía la trama única y exclusivamente al nodo de destino.

1.2.1.4 Aging: supongamos que el nodo A envía una trama al nodo C y el switch aprendió donde estaba el nodo C. ahora el switch sabe donde están los nodos B y C. ahora bien, el nodo A sigue enviando constantemente tramas hacia el nodo B y el nodo C se encuentra en un estado de inactividad. Es aquí donde se utiliza el "Aging". Cada vez que una trama pasa por el switch, un temporizador se actualiza y si durante cierto tiempo un nodo no presenta actividad (en este caso el nodo C)

se borra su entrada (Dirección MAC) de la tabla de conmutación. Esto se hace por 2 razones fundamentales. La primera es que la capacidad de memoria de un switch es muy limitada, y la segunda es que se ahorran recursos muy importantes al switch.

La principal ventaja de un switch multicapa es la velocidad. Estos switches son 10 veces más rápido que un router convencional. Además, poseen chips especializados para que el ruteo y switcheo de paquetes se haga lo más rápido posible. Lo que comúnmente se denomina “Wirespeed”. Esto se logra porque integran “Routing” y “Switching” para producir altas velocidades.

Estos switches pueden filtrar información no deseada incluso a usuarios que ya estén con acceso a la red. Esto con el fin de prevenir ataques a los servidores, aplicaciones, bases de datos, etc. O incluso proteger aplicaciones con ciertos niveles de seguridad.

Otra ventaja, es que estos switches son lo suficientemente inteligentes como para interactuar con el trafico de internet y participar activamente en el manejo eficiente del mismo. Además de esto, un switch multicapa tienen la capacidad de distinguir cuando los puertos están saturados, ocupados, o caídos, de manera que puede enviar de una manera eficiente el tráfico hacia aquellos puertos que estén habilitados o que puedan responder. [6] a continuación se conocerán los parámetros básicos de un switch multicapa.

1.2.2 Parámetros Básicos de un Switch Multicapa

Como se dijo anteriormente que los switches multicapa trabajan como un switch convencional (de capa 2) y poseen funciones adicionales en las otras capas superiores (funciones del router), los parámetros configurables son los mismos

que un capa 2, además de los parámetros de las capas superiores. A continuación se hará una breve descripción de cada uno.

1.2.2.1 Puerto del Switch: Aquí encontramos cuatro parámetros configurables los cuales son: Velocidad (Se realiza de forma manual; Fija/Automática), método de transmisión (Half Duplex/Full Duplex), nombre del puerto, y la prioridad de acceso al bus del switch (Normal/Alta)

1.2.2.2 Control de Flujo: Esta solo disponible sobre los puertos Gigabit-Ethernet. Son tramas de "pausa" que inhiben la transmisión de paquetes desde un puerto por un tiempo determinado.

1.2.2.3 Tabla de direcciones: Se construye de forma automática a medida que el switch va aprendiendo las direcciones de origen de un paquete.

1.2.2.4 Protección EthernetChannel: Aquí se configuran enlaces paralelos para agregar tráfico. Se trata de un enlace de mayor velocidad y en caso de que ocurra alguna falla de uno de ellos, el enlace continúa funcionando. Utiliza el protocolo **PagP** (*Port Aggregation Protocol*) para la creación automática de EtherChannel. De esta forma, en caso de corte, una sola línea abastece al medio, reduciendo el rendimiento, pero manteniendo el servicio. Aquí se maneja la calidad en el servicio QoS.

1.2.2.5 Protección Spanning Tree: Se configura la red de switch con enlaces en loops (Mejor conocidos como enlaces redundantes). Los loops están prohibidos en Ethernet pero mediante el protocolo **STP** (*Spanning-Tree Protocol*) se puede configurar la red en forma automática para detectar estos loops e interrumpirlos hasta que una falla los habilite como necesarios, en otras palabras si un enlace

falla automáticamente el enlace paralelo se habilita garantizando la estabilidad de la red. Las posibles configuraciones son:

1.2.2.6 VLAN: Aquí encontraremos varias opciones configurables. Con la funcion VLAN (Virtual LAN) se divide la red en grupos virtuales para limitar el tráfico de “multicast” y “broadcast”. El protocolo VTP (VLAN Trunk Protocol) minimiza los riesgos de violaciones de seguridad y especificaciones en la generación de VLANs (Se crean Puertos Troncales entre switches). Con la funcion VMPS (VLAN Managment Policy Service) se asignan puertos de VLAN en forma dinámica. Con la funcion ISL (InterSwitch Link) se crean enlaces punto-a-punto en la red de switch. Y la funcion InterVLAN que es la que permite la conexión entre las distintas VLANs.

1.2.2.7 Servicios Multicast: El servicio multicast se provee mediante el protocolo **IGMP** (*Internet Group Management Protocol*) y otros asociados. Un host puede ser inscrito en el grupo de multicast y el switch debe inscribir dicha dirección MAC en la lista de direcciones adheridas.

1.2.2.8 Supresión Multi-Broadcast: Esta función permite la supresión del tráfico multicast y broadcast cuando el mismo inunda la red. Este tráfico ciertas veces degrada el rendimiento. Se puede configurar midiendo el ancho de banda (basado en hardware) o el número de paquetes (basado en software) en un período de tiempo (mayor a 1 seg). La medición se realiza por puerto del switch.

1.2.2.9 Multilayer Switching: Esta técnica se conoce de diversas formas (Tag switching o MPLS, Netflow o MLS) su principal objetivo es intentar reducir el tiempo de procesamiento mediante el análisis del primer paquete y la asignación de un tag o label (Etiqueta) en MPLS o la conmutación de puertos del switch en

MLS. En MLS el switch enruta el primer paquete y crea una “MLS-Cache” para mantener los flujos en proceso. Es necesario rescribir las direcciones MAC. En la configuración se debe tener en cuenta el *Accounting*, Criptografía, NAT, CAR, etc. Se puede configurar la función de exportación de datos (estadísticas de tráfico por cada usuario, protocolo, puerto y tipo de servicio).

1.2.2.10 Filtro de Protocolos: Esta función previene cierto tráfico de protocolo sobre un puerto. Por ejemplo, si una PC está configurada para IP e IPX, pero solo emite IP, es eliminado del tráfico IPX hasta cuando emita un paquete IPX será nuevamente colocado en el grupo de IPX.

1.2.2.11 Lista de IP Permitidas: Esta función permite limitar el tráfico entrante al switch del tipo Telnet y SNMP. El tráfico Ping y Traceroute continúan trabajando normalmente.

1.2.2.12 Seguridad de Puertos: Se trata de indicar las direcciones MAC que pueden ser conectadas a un Puerto. Si la dirección MAC de origen es distinta la conexión se inhibe y se genera un reporte SNMP.

1.2.2.13 SNMP/RMON: Se configura la función de reporte “Trap” en el protocolo SNMP del switch y habilitar las funciones de grupos (estadísticas, historias, alarmas y eventos).

1.2.2.14 Chequeo de Conectividad: Se efectúan las operaciones *Ping* y *Traceroute*. Las cuales permiten detectar la presencia de los componentes conectados al puerto y trazar (Paso-a-Paso) la ruta que dispone hasta un elemento bajo estudio en una red remota.

1.2.2.15 Analizador de Puertos: La función **SPAN** (*Swithed Port Analyzer*) realiza un espejado de tráfico desde uno o más puertos hacia otro donde se coloca un analizador de red.

1.2.2.16 Reportes por Puertos: Con la función *Switch TopN Repor,* Se pueden coleccionar datos estadísticos de cada puerto. Los datos son: utilización del puerto, número de Bytes y paquetes de Entrada/Salida, tráfico multicast y broadcast en los puertos, número de errores y de overflow del buffer.

1.2.2.17 Configuración de DNS (*Domain Name System*): Aquí se organiza la información de routing entre una denominación (seudónimo) simple de recordar y el número de dirección IP verdadero (se denomina resolución de nombre). El nombre completo tiene como máximo 63 caracteres. De ellos, 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, Etc.) y 2 el país (ar-Argentina, it-Italia, Etc.). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*. DNS opera sobre UDP por lo cual no existe una conexión propiamente dicha; solo sirve para resolver la relación entre dominio en formato de texto y la dirección IP asignada. Con posterioridad, la conexión es establecida sobre TCP hacia el servidor (por ejemplo de web).

1.2.2.18 Archivos de Configuración: Aquí se pueden crear archivos con la configuración del switch. Los mismos pueden ser usados en caso de falla absoluta del mismo o para descargarse en un switch similar nuevo.

1.2.2.19 Sincronización de Tiempo: Mediante el protocolo **NTP** (*Network Time Protocol*) se puede llevar la hora del UTC (*Coordinated Universal Time*) obtenida en general desde el sistema GPS (*Global Position System*). Se trata de un modelo Cliente-Servidor. Existen servidores públicos de NTP.

1.2.2.20 Routing: Se configura las distintas posibilidades de protocolos de routing: RIP, IGRP, OSPF, BGP, etc. Se pueden configurar rutas estáticas, direccionamiento secundario o filtrado de rutas.

1.2.2.21 Direcciones: Se configuran las funciones **NAT/PAT** para la traslación automática de direcciones IP y puertos de TCP entre la Internet y el sistema autónomo AS. Se configura la función de asignación de direcciones IP automática mediante **DHCP** (*Dynamic Host Configuration Protocol*).

1.2.2.22 Caching: Se refiere a la conexión de una memoria *Cache* de borde de la red para reducir el tráfico de paquetes web (http). Se configura el protocolo **WCCP** *(Web Cache Control Protocol)* para la conexión entre switch y cache.

1.2.2.23 Protección hot-standby HSRP (*Hot Standby Routing Protocol*): Este protocolo de *Cisco* entrega una protección hot-standby automática entre dos switches. Cuando el switch de trabajo falla el otro toma el control. Un switch configurado con HSRP posee 4 estados posibles: Activo, Standby, S*peaking* (recibe y emite mensajes *hello*) y *Listening* (solo recibe mensajes *hello*).

1.2.2.24 Control de Congestión: Se configuran los mecanismos de control de colas de espera en buffer. Se dispone de las siguientes variantes:

-**FIFO** (*First In, First Out*). El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *Default* y es válido solo en redes con mínima congestión.

-**PQ** (*Priority Queuing*). Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles. Se configuran las prioridades y se monitorea la cola de espera.

-**CQ** (*Custom Queuing*). Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. Se reserva un espacio de buffer y una asignación temporal a cada tipo de servicio.
-**WFQ** (*Weighted Fair Queuing*). Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *Socket* -puertos de TCP/UDP-) y por el ToS en el protocolo IP.

1.2.2.25 Control de Tráfico: Se configuran los mecanismos para descarte de paquetes en caso de congestión en la red.
-**WRED** (*Weighted Random Early Detection*). Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma “aleatoria” si la congestión aumenta (TCP se encarga del control de flujo reduciendo la velocidad de transferencia).
-**GTS** (*Generic Traffic Shaping*). Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera.

1.2.2.26 Políticas de Enrutamiento: El **PBR** (*Policy-Based Routing*) permite mejorar la QoS mediante la determinación de políticas. Se debe configurar un mapa de rutas para verificar la adaptación del paquete. Se basa en dirección IP, puertos TCP, protocolo, tamaño del paquete, etc.

1.2.2.27 CAR (*Committed Access Rate*): Permite generar una política de QoS basada en los bits de precedencia de IP. Se denomina señalización en banda.

1.2.2.28 Reservación de Banda: La señalización fuera de banda se logra mediante el uso de un protocolo externo denominado **RSVP** (*Resource Reservation Protocol*). Sobre el mismo se configura su habilitación y la operación multicast.

1.2.2.29 Fagmentación-interleaving: Se fragmentan los paquetes extensos en pequeños y el intercalado de los mismos para reducir la ocupación prolongada por parte de un paquete. Trabaja con el protocolo **MLP** (*Multilink point-to-point Protocol*) sobre enlaces con PPP.

1.2.2.30 Compresión en Tiempo-Real: Comprime el encabezado de paquetes para la operación con **RTP** (*Real-Time Protocol*). Contribuye a la seguridad.

1.2.2.31 IPsec: Configurando este parámetro, se provee seguridad entre pares en túnel. Permite la autentificación de acceso, integridad de datos, privacidad, etc.

1.2.2.32 Firewall: El módulo de firewall se instala como un software sobre el switch o en un servidor de acceso. Es un parámetro fundamental para la seguridad del mismo Permite realizar las siguientes funciones:

-Control de acceso. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas".

-Logging. Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones.

-Funciones de NAT (*Network Address Translator*) para direcciones públicas y privadas.

-Autentificación. Involucra a 3 componentes: el servidor, el agente y el cliente.

-Reportes. Ofrece un punto conveniente para monitorear (*Audit and log*) y generar alarmas.

2. EL SWITCH MULTICAPA

2.1 Conmutacion Multicapa – Mls

Los switches Cisco disponen de 2 generaciones de MLS (Multilayer Switching):

Route Catching: ésta es la generación más antigua de MLS, la cual requiere un *RP* (Route Processor) y un *SE* (Switching Engine), este tipo de MLS también es conocida como *LAN Switching*. En este caso *RP* se encarga de buscar el camino más adecuado y almacenarlo, *SE* es la encargada de "Recordar" la decisión tomada por *RP*.

Basado en topología: ésta es la generación actual y utiliza *ASIC* (Application-Specific Integrated Circuit o Circuito integrado para una aplicación específica) especializados para construir una base de datos única con toda la topología de la red. Este tipo de comunicación es conocido como ***CEF*** (Cisco Express Forwarding). Una vez determinada la ruta, se almacena en la ***FIB*** (Forwarding Information Base), que es donde se puede consultar cada vez que entre una petición idéntica.

2.1.1 ¿Qué es CEF (Cisco Express Forwarding)?

CEF es una característica avanzada de la IOS de Cisco que permite realizar una conmutación más rápida en los dispositivos Cisco. Una tarea esencial en los dispositivos de capa 3 (Routers y Switches de capa 3), es la toma de decisiones respecto de a dónde deben reenviar los paquetes que reciben. Este proceso de decisión es conocido con el nombre de conmutación "Switching en inglés", y es diferente del proceso de conmutación que se realiza en un switch Ethernet de capa 2. En la *Figura 1* se observa un esquema de las tablas CAM y FIB en un Switch multicapa.

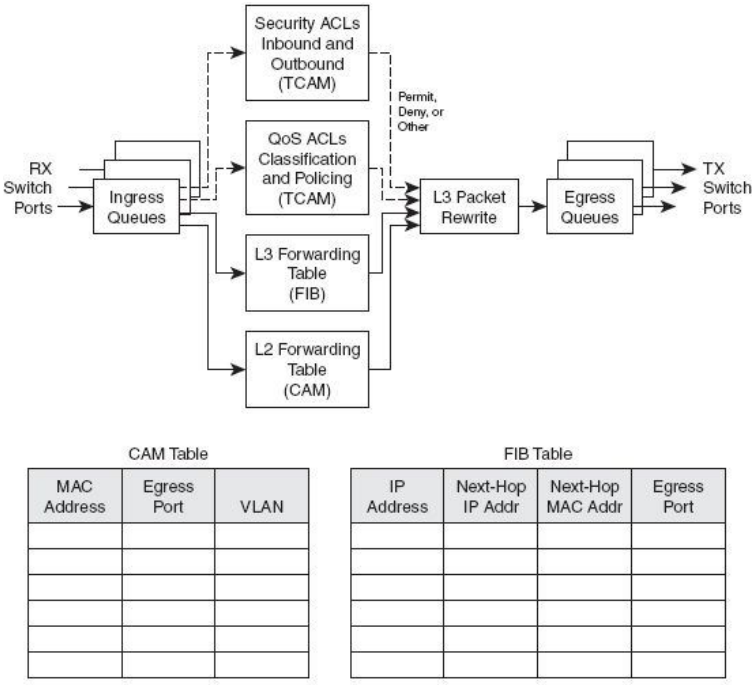


Figura 1. Multilayer Switch CAM & FIB Table

L2 Forwarding Table: La dirección MAC de destino junto con la VLAN ID se buscan en la tabla CAM, si se encuentra se coloca la trama en la cola de salida para ser procesada, en caso contrario se prepara la trama para ser enviada por todos los puertos excepto el origen (inundación).

L3 Forwarding Table: La tabla FIB se consulta, utilizando la dirección IP de destino como índice. El resultado más largo que podemos encontrar en la tabla FIB, es la (dirección IP y máscara), con esto obtenemos la dirección de capa 3 del próximo salto. La tabla FIB también contiene la dirección MAC de capa 2 del siguiente salto y el puerto de salida del switch (y VLAN ID), de modo que las búsquedas en la tabla no son necesarias. (No hay Inundación)

Security ACLs: Las listas de acceso de entrada y salida se compilan en las entradas de la tabla TCAM para que las decisiones de si se debe enviar un paquete se puedan determinar como una sola tabla de búsqueda.

Qos ACLs: Se clasifican las tramas entrantes en función de la QoS, estas decisiones las realiza la tabla (TCAM QoS).

Al igual que con conmutación de Capa 2, el paquete finalmente debe ser colocado en la cola de salida correspondiente al puerto de salida del switch adecuado.

Cuando un dispositivo (Capa 3) conmuta, realiza las siguientes operaciones:

1. Decidir si debe o no reenviar un paquete después de verificar que la red de destino del paquete es alcanzable.
2. Si el destino es alcanzable, ¿Cuál es el próximo salto y que interfaz debe utilizarse para alcanzar este destino?
3. ¿Se debe modificar la dirección MAC con la que se encapsula el paquete?

Tomando como referencia la tabla de enrutamiento IP, ***CEF*** crea su propia tabla de enrutamiento llamada ***FIB***, la cual se utiliza para definir a qué interfaz se debe reenviar el paquete. Existen paquetes que no pueden ser conmutados directamente por ***CEF*** y tienen que ser procesados de forma diferente:

- Peticiones ARP.
- Paquetes IP con TTL expirado o MTU excedida.
- Broadcast IP que son reenviados como unicast como las peticiones DHCP o ip-helper.
- Actualizaciones de enrutamiento.
- Paquetes CDP.
- Paquetes encriptados.
- Paquetes no IP y no IPX.

CEF se encuentra deshabilitado por defecto en todos los dispositivos Cisco, excepto en los routers de la serie 7xxx, 6500 y 12000. Los routers de la serie

2600, 3600 y 3800 incorporan esta característica a partir de la versión de la IOS de cisco 12.2 (11) T.

Ahora se pueden observar algunos comandos relacionados con este tipo de conmutación.

Habilitar CEF

Router#**configure terminal**
Router(config)#**ip cef**
Router(config)#

Deshabilitar CEF

Router#**configure terminal**
Router(config)#**no ip cef**
Router(config)#

Verificar el estado de CEF

Router#**show ip cef**

Prefix	Next Hop	Interface
0.0.0.0/0	192.168.1.5	FastEthernet0/0
192.168.0.0/24	192.168.1.1	Serial0/2/0
192.168.2.0/30	192.168.1.1	Serial0/2/0
192.168.3.0/30	192.168.1.1	Serial0/2/0
192.168.4.0/24	192.168.1.1	Serial0/2/0
192.168.5.0/30	192.168.1.1	Serial0/2/0

El comando ***show ip cef detail*** muestra información detallada sobre cada entrada de la tabla ***FIB***.

El comando ***show ip cef summary*** permite ver un resumen de las entradas contenidas en la tabla FIB. [8]

2.2 REDUNDANCIA EN UNA RED

Para empezar a hablar de redundancia se hace la pregunta ¿Qué es realmente la redundancia en una red? Bueno, en la arquitectura de redes actuales, la redundancia es la premisa básica. Su objetivo principal, *"Evitar Fallas en la Red"*. La expectativa de que Internet está siempre disponible para millones de usuarios requiere de una arquitectura de red diseñada y creada con *"Tolerancia a Fallas"*.

Una red tolerante a fallas es la que limita el impacto de una falla, ya sea de software o de hardware, y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace falla, la red garantiza que los mensajes se enruten en forma instantánea a un enlace distinto de manera transparente para los usuarios que se encuentren en cada extremo de la red. En otras palabras las exigencias del usuario nunca se ven afectadas por dicha falla. En la *Figura 2*, se puede observar un tipo de red redundante.

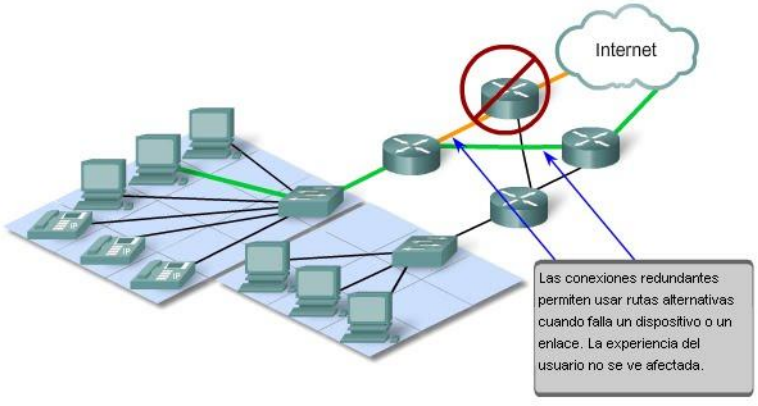


Figura 2. Red Redundante Disponible en:
http://2.bp.blogspot.com/_hU3VRyW6rnM/TD8fyf0TyAI/AAAAAAAAAJQ/ms6F4bNC7rs/s1600/redes12.bmp

El desarrollo de nuevas tecnologías LAN va dirigido a garantizar una alta disponibilidad de interconexión de los dispositivos de una red. Por ejemplo, la capacidad de soportar fallos de una tarjeta de interfaz en un servidor de balanceo de carga, o la configuración redundante de las fuentes de alimentación de los switches en un Backbone. Para esto existen “Protocolos Redundantes” que pueden ser aplicados en switches y routers de capa 3 o multicapa. Protocolos redundantes *HSRP, VRRP y GLBP*. La redundancia en una red va ligada con el balanceo de carga de la misma, a continuación se explicará el balanceo de carga y como trabajan cada unos de estos protocolos.

2.2.1 Spanning Tree Protocol – STP [9]

Cuando se agregan enlaces adicionales a switches y routers de la red, se generan bucles en el tráfico que deben ser administrados de manera dinámica, cuando se pierde la conexión con un switch, otro enlace debe reemplazarlo rápidamente sin introducir nuevos bucles en el tráfico. Cuando existen varias rutas entre dos dispositivos en la red, puede generarse un bucle de Capa 2. Las tramas de Ethernet no poseen un tiempo de existencia (TTL, Time to Live) como los paquetes IP que viajan por los routers. En consecuencia, si no finalizan de manera adecuada en una red conmutada, las mismas siguen rebotando de switch en switch indefinidamente o hasta que se interrumpa un enlace y elimine el bucle.

Las tramas de broadcast se envían a todos los puertos de switch, excepto el puerto de origen. Esto asegura que todos los dispositivos del dominio de broadcast puedan recibir la trama. Si existe más de una ruta para enviar la trama, se puede generar un bucle sin fin; una tormenta de broadcast se produce cuando existen tantas tramas de broadcast atrapadas en un bucle de Capa 2 que se consume todo el ancho de banda disponible. La redundancia aumenta la disponibilidad de la red por si algún punto falla, como un cable de red o switch,

cuando se introduce la redundancia en un diseño de la Capa 2, pueden generarse bucles y tramas duplicadas, los bucles y las tramas duplicadas pueden tener consecuencias graves en la red, es por eso que el protocolo Spanning Tree (STP) fue desarrollado para enfrentar estos inconvenientes, porque STP se asegura de que sólo exista una ruta lógica entre todos los destinos de la red, al bloquear de forma intencional aquellas rutas redundantes que puedan ocasionar un bucle, para esto STP asigna estados y roles para los puertos del switch.

2.2.1.2 Características de STP [10]

STP utiliza el algoritmo Spanning-Tree (STA) para determinar los puertos de switch de la red que deben configurarse para el bloqueo, y así evitar que se generen bucles. El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. Todos los switches que comparten STP intercambian tramas de BPDU para determinar el switch que posee el menor ID de puente (BID) en la red. El switch con el menor BID se transforma en el puente raíz de forma automática según los cálculos del STA.

La BPDU es la trama de mensaje que se intercambia entre los switches en STP.
La información contenida dentro de una trama BPDU incluye:
Root ID: Que es el Bridge ID (BID) más bajo de la topología.
Costo de la Ruta: Que es el costo de todos los enlaces del switch que esté transmitiendo en ese momento hacia el puente raíz.
BID: BID del Switch que transmite
Port ID: El ID del Puerto que transmite
STP Timer Values:

- ***Maximum Age:*** Le dice al puente que tanto tiempo debe mantener los puertos en estado “Bloqueado” antes de pasar al estado “Escuchando”. Por defecto son 20 segundos.

- ***Hello Time:*** Determina que tan frecuentemente el puente raíz envía la configuración de las BPDUs. Por defecto son 2 segundos.
- ***Forward Delay:*** Determina que tanto tiempo debe estar en estado "Escuchando" antes de pasar al estado de "Aprendiendo" y cuanto tiempo debe estar en estado "Aprendiendo" antes de pasar al estado "Enviando". Por defecto son 15 segundos.

Cada BPDU contiene un BID que identifica al switch que envió la BPDU. El BID contiene un valor de prioridad, la dirección MAC del switch emisor y un ID de sistema extendido opcional. Se determina el BID de menor valor mediante la combinación de estos tres campos. Después de determinar el puente raíz, el STA calcula la ruta más corta hacia el mismo. Todos los switches utilizan el STA para determinar los puertos que deben bloquearse. Al determinar el STA las mejores rutas hacia el puente raíz para todos los destinos del dominio de broadcast, se evita que todo el tráfico sea enviado a través de la red. El STA considera los costos tanto de la ruta como del puerto cuando determina la ruta que debe permanecer desbloqueada. Los costos de la ruta se calculan mediante los valores de costo de puerto asociados con las velocidades de los puertos para cada puerto de switch que atraviesa una ruta determinada. La suma de los valores de costo de puerto determina el costo de ruta total para el puente raíz. Si existe más de una ruta a escoger, el STA elige la de menor costo de ruta. Cuando el STA determina las rutas que deben permanecer disponibles, configura los puertos de switch de acuerdo con distintas funciones. Las funciones de los puertos describen su relación en la red con el puente raíz y si los mismos pueden enviar tráfico.

- **Puertos raíz:** Los puertos de switch más cercanos al puente raíz.
- **Puertos Designados:** Todos los puertos que no son raíz y que aún pueden enviar tráfico a la red.

- **Puertos No Designados:** Todos los puertos configurados en estado de bloqueo para evitar los bucles.

2.2.1.2.1 El puente Raíz [10]

Toda instancia de Spanning-Tree (LAN conmutada o dominio de broadcast) posee un switch designado como puente raíz. El puente raíz sirve como punto de referencia para todos los cálculos de Spanning-Tree para determinar las rutas redundantes que deben bloquearse.

Todos los switches del dominio de broadcast participan del proceso de elección. Cuando se inicia un switch, el mismo envía tramas de BPDU que contienen el BID del switch y el ID de raíz cada dos segundos. De manera predeterminada, el ID de raíz coincide con el BID local para todos los switches de la red. El ID de raíz identifica al puente raíz de la red. Inicialmente, cada switch se identifica a sí mismo como puente raíz después del arranque.

2.2.1.3 Comandos en Switches Cisco para configurar el Protocolo Spanning Tree

- *Show Spanning Tree*: Permit ever la configuracion actual del protocolo.
- *Spanning-tree Vlan [Vlan_number] root primary:* Para cambiar el Puerto Raiz
- *Spanning-tree Vlan [Vlan_number] root secondary:* Para Designar un Puerto Raiz Secundario
- *Debug Spanning-tree events:* Para monitorear los cambios en la topología
- Spanning-tree port-priority [prioridad]: Para cambiar la prioridad de un puerto
- Spanning-tree cost [costo]: Para cambiar el costo de un Puerto.

Existen ventajas y desventajas cuando se usa un simple Spanning Tree. Como ventaja se tiene que permite a simplicidad de los switches en cuanto al diseño y mucho menos carga en la CPU. Por otro lado, un Spanning Tree Simple impide el balanceo de carga, y puede llevar a que la conectividad en ciertas VLANs este incompleta (un simple STP de una Vlan podría seleccionar un enlace que no esté incluido en otra VLAN). Por estas razones muchos diseñadores de red han concluido que la desventaja de tener un STP simple, disminuye los beneficios de la red. Es aquí donde nace una mejora denominada RSTP (Rapid Spanning Tree Protocol).

2.2.2 Rapid Spanning Tree – RSTP [10]

La consideración inmediata del Spanning Tree es el tiempo de convergencia. Dependiendo del tipo de fallo, le toma entre 30 y 50 segundos converger en la red. RSTP ayuda con el tema de la convergencia que daña al legado de STP. RSTP posee características adicionales similares a UplinkFast y BackboneFast que ofrece un mejor desempeño en la capa 2.

RSTP se basa en el estándar IEEE 802.1w. Existen numerosas diferencias entre RSTP y STP. RSTP requiere una conexión full-duplex punto a punto entre switches adyacentes para lograr una convergencia más rápida. RSTP no puede lograr una convergencia rápida en Half-Duplex. STP y RSTP también poseen diferencias en cuanto a la designación de puertos. RSTP posee designación de puertos alternada y de reservas, las cuales están ausentes en un ambiente STP. Los puertos que no participan en el Spanning Tree se les denominan “Edge Ports”. “Edge Ports” pueden ser estáticamente configurados por el parámetro PortFast. Un “Edge Port” deja de serlo si un BPDU es “Escuchado” en el puerto. Los puertos que no son “Edge Ports” participan en el algoritmo de STP y solo este tipo de

puertos pueden generar cambios en la topología de red cuando se transiciona al estado “Enviando”.

2.2.2.1 Comandos del RSTP

- *Spanning-Tree mode rapid-pvst:* Para habilitar el modo RSTP.
- *Show Spanning-Tree Vlan [Vlan_Number]:* Para verificar el estado del protocolo en determinada vlan.
- *Show Spanning-tree [bridge-group* | ***active*** | ***backbonefast*** | *{**bridge** [id]}*| ***detail*** | ***inconsistentports*** | *{**interface** interface interface-number}* | ***root*** | ***summary** [**total**]* | ***uplinkfast*** | *{**vlan** vlan-id}* | *{**port-channel** number}* | ***pathcost-method**]:* Permite mostrar las distintas opciones del protocolo e acuerdo a lo que se quiera observar.

Referirse a la documentación del software del equipo que se esté utilizando para una completa explicación de cada parámetro.

2.3 BALANCEO DE CARGA

Antes de empezar a explicar cada uno de los protocolos, se explicará el concepto de balanceo de carga y como funciona.

Cuando un servidor de internet se vuelve lento debido a la congestión de la información, la solución más obvia sería ampliar la memoria, el disco duro o incluso actualizar el procesador. Pero esta solución se queda corta cuando el tráfico de internet crece exponencialmente lo cual la convertiría en una solución meramente temporal. Pero, la opción más razonable sería conectar más servidores y repartir las peticiones de los clientes entre ellos. Esto incrementaría la velocidad de acceso del usuario al servidor, mejoraría la fiabilidad del sistema y sobretodo la tolerancia a fallos, permitiendo así mantener cualquier servidor en

línea sin que afecte al resto. Pero a pesar de todo esto, una vez se hayan utilizado varios servidores para responder todas las peticiones que van a determinada dirección, ¿Cómo las dividimos entre los distintos servidores? ¿Cómo se puede saber que rendimiento se está ofreciendo y que tiempo de CPU está generando cada petición? El simple hecho de conectar más servidores a una red no garantiza la mejora del servicio. Es aquí donde entra lo que se denomina *"Balanceo de Carga" o "Load Balancing"*. En la *Figura 3*, se puede observar un esquema de balanceo de carga.

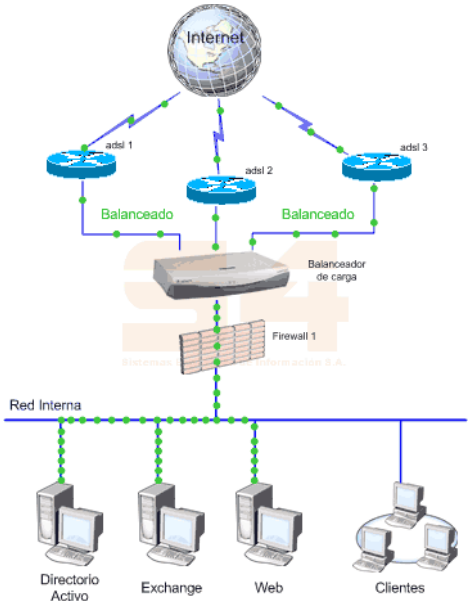


Figura 3. Esquema de Balanceo de Carga

¿Qué es realmente Balanceo de Carga? Balanceo de Carga es simplemente la manera en que las peticiones de internet son distribuidas sobre una fila de servidores. Existen varios métodos para realizarlo, pero el más simple es el *"Round Robin"* Las peticiones clientes son distribuidas equitativamente entre todos los servidores existentes. Ahora bien, este método cíclico no tiene en cuenta las condiciones y carga de cada servidor por lo cual nos puede llevar a tener servidores que reciben peticiones de carga mucho mayor, mientras tenemos

servidores que apenas se encuentran utilizando recursos. Otra limitación es que los problemas de los servidores no son recogidos inmediatamente. Es decir, esto nos puede llevar a enviar peticiones a un servidor que se encuentra fuera de servicio o que responde lentamente. Finalmente, el método Round Robin no aprovecha las diferentes prestaciones de los servidores.

En la *primera generación* de balanceo de carga, las soluciones "reales" de balanceo de carga necesitan descubrir el rendimiento del servidor. La primera generación puede detectar el rendimiento del servidor vía *"Passive Polling"*, lo que significa que el balanceador de carga mide el tiempo de respuesta de los servidores y por ello tiene una idea de cómo están funcionando. De nuevo, tampoco se tiene en cuenta la variedad de servidores empleados. Además, sólo descubre que los servidores tienen un problema después de que se producen retrasos o, en el peor de los casos, cuando los servidores están completamente caídos.

En la *segunda generación* de balanceo de carga, El balanceo de carga más seguro sólo se puede conseguir considerando el uso real de los servidores, permitiendo que los recursos existentes se empleen al máximo, al conocer cómo están siendo utilizados estos recursos incluso antes de que las peticiones de los clientes lleguen a ellos. El tráfico se enruta proactivamente, cambiando el antiguo concepto existente de balanceo de carga, hacia una solución de optimización del servidor, consiguiendo el mejor resultado posible con la tecnología disponible.

Como se mencionó anteriormente, existen 3 protocolos redundantes los cuales se utilizan para lograr la existencia del balanceo de carga en switches multicapa. Estos son el HSRP, VRRP, y el GLBP. A continuación se procede a explicar cada uno de ellos con sus características.

2.3.1 HSRP (Hot Standby Router Protocol)

El Hot Standby Router Protocol, es un protocolo propiedad de CISCO, pertenece al *RFC221.* Permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Se crea un grupo HSRP con 3 routers o 3 switches multicapa (Como Routers). Existe un router maestro o "Active Router" el cual enruta el tráfico, un Standby Router el cual es el backup del Active Router en caso de que este se caiga. Y un Virtual Router (que no es un router en realidad) el cual representa al grupo HSRP y es el default Gateway para los hosts. Entre los routers del grupo, se intercambian mensajes *"Hello"* para conocer el estado en el que se encuentra cada uno. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985. Dado el caso que el active router no envié mensajes "Hello" dentro de un periodo de tiempo, otro router del grupo se convierte en el nuevo active router. En la *Figura 4* se puede observar un esquema HSRP.

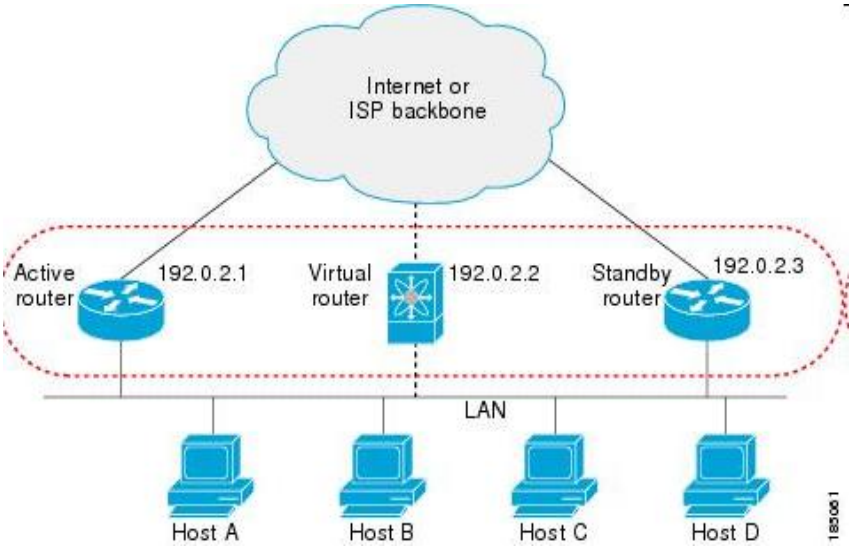


Figura 4. Esquema HSRP

Disponible en: http://www.cisco.com/en/US/i/100001-200000/120001-130000/127001-128000/127024.jpg

Para determinar cuál es router maestro, establece una prioridad en cada router. La prioridad por defecto es 100 y va desde 0 a 255. El router con mayor prioridad es el que será el active router. Ahora bien, una vez que el temporizador "Holdtime" expira (Holdtime por defecto definido a 10 segundos) lo cual equivale a 3 paquetes "Hello" (Timer Hello por defecto definido a 3 segundos) que no son enviados desde el active router. Este protocolo puede observarse en funcionamiento en el Capitulo 3. Practica No. 4 – Balanceo de Carga con HSRP.

Los comandos para configurar HSRP son los siguientes:

standby *<group#>* **ip** *<ip de la puerta de enlace virtual> //Activa el protocolo HSRP.*

standby *<group#>* **Preempt**[1]

standby *<group#>* **Priority** *<priority from 0-255> //con este comando se escoge el Active Router del grupo HSRP.*

standby *<group#>* **track** *<interface> //Para configurar una interface de modo que la Prioridad del protocolo cambie basándose en la disponibilidad de otras interfaces. En otras palabras, para rastrear el estado de una interface.*

Nota: La utilización de estos comandos depende del tipo de topología o red en la que se esté trabajando. Para más información referirse a la web www.cisco.com en el siguiente enlace:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml

[1] *Preempt: Es el acto de interrumpir temporalmente una tarea que esta llevándose a cabo por un sistema de computo, con la intención de resumir la tarea mas adelante. Es comúnmente conocido como switch de contexto.*

2.3.2 VRRP (Virtual Router Redundancy Protocol)

Es un estándar que surge como alternativa a HSRP que está definido por IETF en el *RFC2338*. Ambos protocolos son similares, aunque una diferencia es que VRRP puede ofrecer como IP virtual una virtual (al igual que HSRP) o la dirección IP del router activo.

Al igual que HSRP, tiene un router activo cuya prioridad es la mayor, el resto de routers están en estado “Backup”. El número del grupo va de 0 a 255 y la prioridad va de 1 a 255 (siendo 255 la más alta) por defecto es la 100 también. Ahora bien, la diferencia con HSRP es que no cuando el “active router” falla, anuncia una prioridad de 0 forzando a la elección del nuevo “active router” sin tener que esperar que el “Holdtime” expire. Otra diferencia es que los mensajes “Hello” son enviados cada 1 segundo, no cada 3 como en HSRP. A diferencia de HSRP, VRRP no tiene manera de monitorizar interfaces.

2.3.3 GLBP (Gateway Load Balancing Protocol)

Como se ha podido observar, HSRP y VRRP son muy parecidos, los dos balancean una o varias IPs virtuales y en base a sus prioridades cada router tiene un rol dentro del grupo. Este protocolo fue diseñado para ofrecer balanceo de carga sin las limitaciones de HSRP y VRRP. Debido a que al contrario de HSRP, todos los routers están activos por lo cual el balanceo de carga se cumple en todos los routers del grupo. *NOTA:* Este protocolo no está soportado por la familia Cisco 4500, 6500 y Nexus.

En este protocolo, el número de grupo GLBP va de 0 a 1023. La prioridad de 1 a 255 y por defecto es 100, los mensajes “Hello” se envían cada 3 Segundos. La dirección multicast para GLBP es 224.0.0.102 y el “Holdtime” por defecto es 10 segundos. Uno de los routers del grupo GLBP, el que tenga la mayor prioridad o

la IP más alta, es elegido como Puerta de Salida Virtual Activa (Active Virtual Gateway - AVG). Cuando un equipo quiere comunicarse con otro equipo que está fuera de su red, realizará un *"ARP Request"* de la ip de su *siguiente salto* a ese destino*, g*eneralmente la ruta por defecto. El objetivo de AVG es responder a todas las peticiones ARP de los servidores que llegan a la dirección del router virtual, luego dependiendo del algoritmo que se use este router AVG responderá con la MAC del router que corresponda al cual se enviarán los paquetes.

El router AVG asigna las direcciones MAC virtuales de cada router que participe en el grupo GLBP hasta un máximo de 4 direcciones MAC. Cada uno de estos 4 routers se llama *Active Virtual Forwarder* (AVF). En caso de que haya más routers en el grupo GLBP se mantienen en backup o secundarios por si algún AVF falla y tenga que sustituirlo.

2.3.3.1 Métodos de Balanceo de Carga

Para el balanceo de carga se puede configurar uno de estos tres métodos:

2.3.3.1.1 Round Robin: Cada nueva petición ARP se asigna la siguiente dirección de MAC disponible a modo circular, con esto se consigue distribuir la carga de igual forma a cada AVF asumiendo que los cliente envían y reciben la misma cantidad de tráfico. *Este método es usado por defecto.*

2.3.3.1.2 Weighted: El peso asignado a la interface del grupo GLBP determina la proporción de tráfico que se envía a cada AVF, cuanto mayor sea el peso más tráfico se envía a ese router. Si la comprobación de interface no se ha configurado, el valor máximo de peso se utiliza para establecer las proporciones relativas entre los AVFs.

2.3.3.1.3 Host Dependent: Cada petición ARP de los clientes se le asigna la misma dirección MAC con lo que cada cliente tiene la misma dirección MAC de salida (la del AVF asignado).

3. PRUEBAS DE LABORATORIO REALIZADAS UTILIZANDO LA FAMILIA DE SWITCHES CISCO CATALYST 3560 Y 2960.

Como se ha argumentado en los capítulos anteriores, los switches multicapa poseen muchas ventajas al momento de garantizar redundancia, seguridad, calidad en el servicio y alta disponibilidad en una red, ofreciendo minimizar las fallas al reducir los equipos de 2 (Switch + Router) a 1 solo equipo (Switch Multicapa), igualmente el proceso de enrutamiento se hace más rápido porque solo se revisa en una sola tabla y no dos ni tres (tantas tablas como routers). Adicional a todo eso, la seguridad en la infraestructura de red aumenta debido a que se aplican políticas de seguridad a un solo dispositivo.

Sabiendo esto, se procederá a realizar las siguientes configuraciones:

1- Configuracion de Enrutamiento entre VLAN's
2- Configuracion de MLS aplicando CEF (Cisco Express Forwarding)
3- Configuracion STP (Spanning Tree Protocol)
4- Configuracion de Balanceo de Carga (Esta práctica se realizará en el laboratorio de redes físicamente)

Se utilizará el simulador Packet Tracer Versión 5.3.2.0027, para realizar las 3 primeras pruebas, y los equipos en el laboratorio de redes para la última. Finalmente se anotarán todas las conclusiones de los resultados arrojados por las mismas.

NOTA: Todas las practicas se realizaron utilizando Vlan, esto no significa que sea obligación utilizarlas en la configuración que el lector desee realizar.

PRACTICA No. 1

3.1 CONFIGURANDO ENRUTAMIENTO ENTRE VLAN'S

3.1.1 Objetivo: Enrutar entre VLAN's utilizando un Switch Cisco Catalyst 3560-24PS.

3.1.2 Ventajas y Desventajas

Para analizar las ventajas del switch multicapa respecto a los switch convencionales, primero se debe conocer como es el enrutamiento convencional entre VLANs con 1 Switch Capa 2 y 1 Router. En la *Figura 5* se observa la topología convencional de enrutamiento entre Vlan.

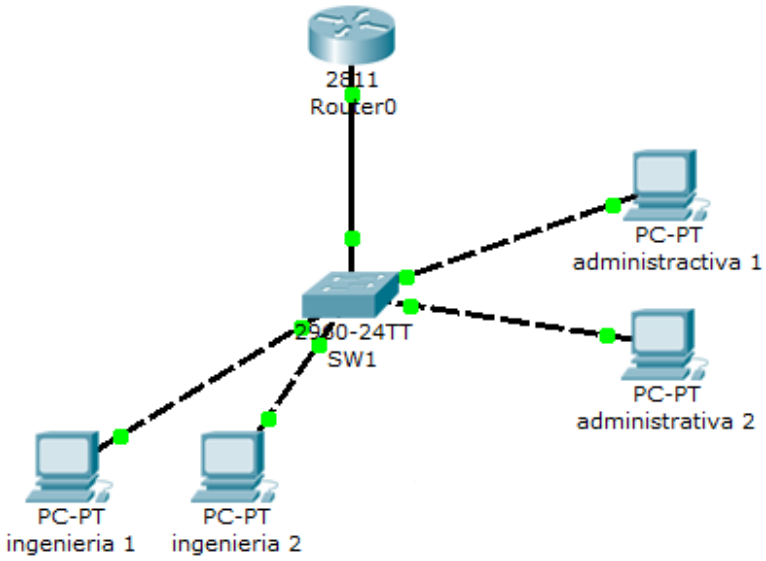


Figura 5. Topología convencional para enrutamiento entre VLANs

Para la configuración, en el switch capa 2 se configuran los puertos por donde tendrán acceso las VLANs con el comando ***Switchport Access Vlan [Vlan_Number]***. En este caso (*Fa0/1-9 -> Vlan 10 y Fa0/10-23 -> VLAN 20*) Cuando se agrega el router, se debe configurar la interfaz conectada al switch como troncal, adicionalmente se crean 2 interfaces virtuales en el router (En este

caso Fa0/0.1 y Fa0/0.2) con direcciones *IP 192.168.10.1 y 192.168.20.1* respectivamente las cuales son las puertas de enlace predeterminadas de cada VLAN. Una vez realizado esto, el enrutamiento queda habilitado entre las VLANs. Se utiliza el comando ***show running-config*** para ver la configuración.

```
!hostname router
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
```

Ahora bien, El enrutamiento es exitoso, pero esto implica que se utilizan un Switch y 1 Router lo cual representado en dinero es muy costoso. En cuanto a la configuración se necesita configurar 2 equipos lo cual implica tiempo y más dinero. Es por esa razón que el Switch Multicapa es la mejor opción para este tipo de interconexión debido a que reúne las capacidades de un switch convencional y de un router en un solo dispositivo lo cual genera reducción de costos de hardware y reducción de tiempo de configuración debido a que solo con un comando se habilita el enrutamiento entre las Vlan. En la práctica a continuación se observará como se configura el switch para lograr el enrutamiento entre VLANs. No se encontraron desventajas.

Para esta práctica se utilizara el simulador Packet Tracer Versión 5.3.2.0027 el cual trae en sus equipos el Switch Multicapa Cisco Catalyst 3560-24PS como se puede observar en la *Figura 6*.

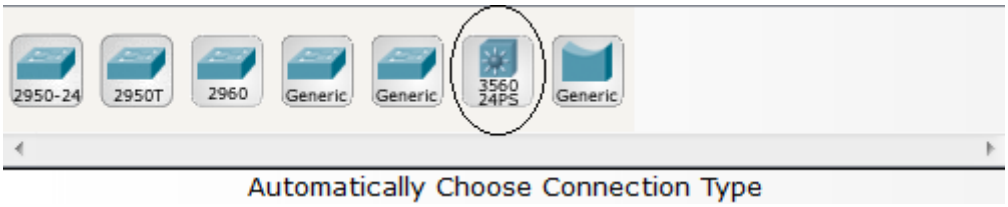


Figura 6. Switches Disponibles en el Simulador Packet Tracer Versión 5.3.2.0027

3.1.3 Escenario: Se Tendrá un Switch Multicapa con las VLAN 100 y 200. Se utilizarán los bloques IP ***192.168.10.0/24*** y ***192.168.20.0/24*** respectivamente. La topología utilizada para realizar esta prueba será la siguiente: (*Ver Figura 7*).

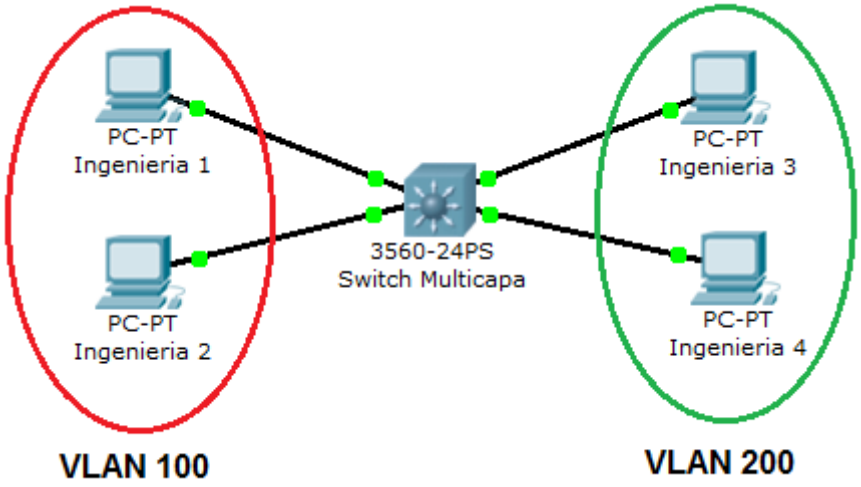


Figura 7: Topología para enrutamiento entre VLAN's con Switch Multicapa

3.1.4 Desarrollo:

Para comenzar se configurarán las VLAN. La configuración de las VLAN en estos switches no tiene nada distinto a la configuración que se hace en un switch de capa 2 como se puede observar a continuación:

Switch>ena

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range fastEthernet 0/1-fastEthernet 0/9
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
% Access VLAN does not exist. Creating vlan 100
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/10-fastEthernet 0/23
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 200
% Access VLAN does not exist. Creating vlan 200
Switch(config-if-range)#end

Con esto se han creado las VLAN. Ahora se procede a configurar el enrutamiento en el switch. Las puertas de enlace predeterminadas de cada host de las VLAN serán la IP de la interfaz VLAN del switch a la cual corresponde. Es decir, la Gateway de la VLAN 100 será 192.168.10.1 y la de la VLAN 200 será 192.168.20.1 respectivamente.

Switch(config)#interface vlan 100
%LINK-5-CHANGED: Interface Vlan100, changed state to up
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#exit

Switch(config)#interface vlan 200
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#exit
Switch(config)#

Ahora bien, realizado esto, aun no existe conectividad entre las VLAN, y esto se debe a que el switch multicapa aun se está comportando como un switch de capa 2. Para activar sus funciones de capa 3 debemos utilizar el comando ***ip routing***.

Switch(config)#ip routing

Con esto ya se ha habilitado el switch multicapa para enrutar. Se prueba el enrutamiento haciendo un ping de PC a PC.

En la *Figura 8* se puede observar que funciona correctamente el enrutamiento.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	Ingenieria 2	Ingenieria 1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Ingenieria 1	Ingenieria 2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Ingenieria 3	Ingenieria 2	ICMP		0.000	N	10	(edit)	(delete)
	Successful	Ingenieria 1	Ingenieria 3	ICMP		0.000	N	11	(edit)	(delete)
	Successful	Ingenieria 1	Ingenieria 4	ICMP		0.000	N	12	(edit)	(delete)
	Successful	Ingenieria 1	Ingenieria 3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Ingenieria 1	Ingenieria 4	ICMP		0.000	N	3	(edit)	(delete)
	Successful	Ingenieria 4	Ingenieria 3	ICMP		0.000	N	4	(edit)	(delete)
	Successful	Ingenieria 4	Ingenieria 1	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Ingenieria 4	Ingenieria 2	ICMP		0.000	N	6	(edit)	(delete)
	Successful	Ingenieria 4	Ingenieria 1	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Ingenieria 4	Ingenieria 2	ICMP		0.000	N	8	(edit)	(delete)
	Successful	Ingenieria 3	Ingenieria 1	ICMP		0.000	N	9	(edit)	(delete)

Figura 8. Pings de PC a PC entre equipos de la misma VLAN y de distintas VLAN.

3.1.5 Conclusiones

Como se observa en los resultados obtenidos por el simulador, el switch multicapa logra realizar el enrutamiento InterVLAN sin ningún tipo de inconvenientes gracias al comando ***ip-routing***. Esto nos demuestra una de las grandes ventajas que tiene este switch frente a switch convencionales de capa 2 brindando mejor rendimiento, reducción de costos y menos tiempo de configuración.

PRACTICA No. 2

3.2 ENRUTAMIENTO INTER-VLAN MEDIANTE EL PROCESO DE RUTEO INTERNO Y MONITOREANDO LAS FUNCIONES CEF (Cisco Express Forwarding)

3.2.1 Objetivo: Enrutar entre VLAN's utilizando un Switch Cisco Catalyst 3560-24PS mediante el proceso de ruteo interno utilizando CEF (Cisco Express Forwarding).

3.2.2 Ventajas del Protocolo CEF.

- Tiene mejor performance que el modo de conmutación por defecto de los dispositivos (Fast-Switching) y requiere menos ciclos de CPU para realizar la misma tarea.
- Cuando está habilitado este modo de conmutación, es posible utilizar otros "Features" avanzados, como NBAR**.**
- Permite Escalabilidad
- CEF es un modo de conmutación de tráfico más rápido que otros disponibles.

3.2.3 Escenario: Para esta práctica se creará una red jerárquica la cual incluye un equipo Cisco Catalyst 3560-24PS que actuará como capa de distribución, 2 Switches Cisco Catalyst 2960-24TT que actuarán como la capa de acceso. La red estará segmentada en 3 subredes funcionales utilizando VLAN para una mejor administración de red. Las VLAN's estarán distribuidas de la siguiente manera: el área administrativa VLAN 100, el área de ingeniería VLAN 200 y la administración de equipos tendrá la VLAN 1 que es la VLAN por defecto. Posteriormente se procederá a configurar VTP (Virtual Trunking Protocol) además del *Trunking*. Una

vez realizado esto, los SVI (Switched Virtual Interfaces) se usarán en la capa de distribución para enrutar las VLAN's dándole total conectividad a la red interna. Para esta práctica utilizaremos la topología mostrada en la *Figura 9*:

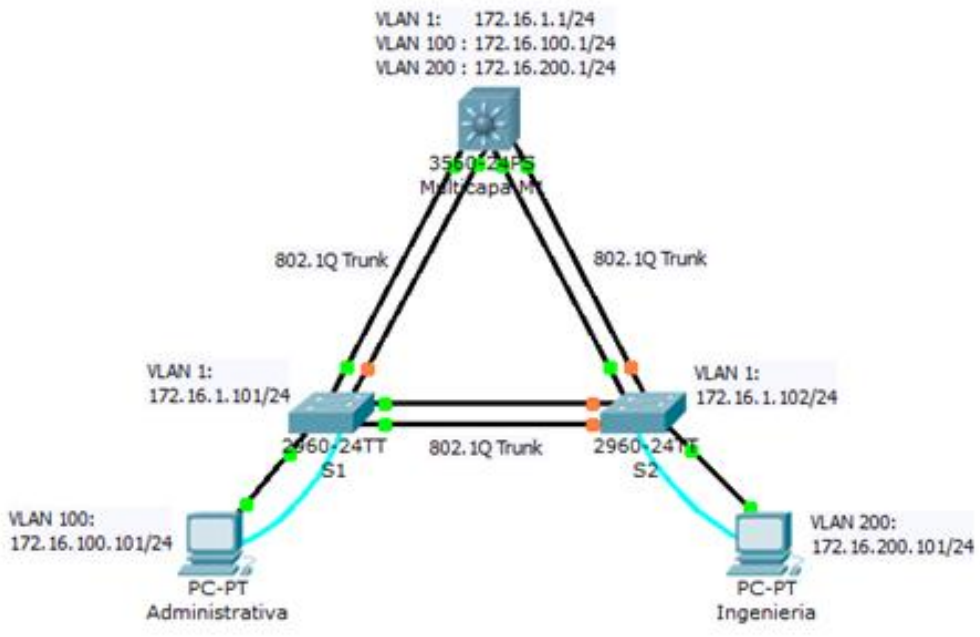


Figura 9. Topología utilizada para ruteo InterVLAN con monitoreo CEF (Cisco Forwarding Express)

3.2.4 Desarrollo:

Para empezar se debe configurar primero el hostname, la password y el acceso telnet en cada uno de los switches utilizando los siguientes comandos:

```
Switch>ena
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname MulticapaM1
MulticapaM1(config)#enable secret cisco
MulticapaM1(config)#line vty 0 15
MulticapaM1(config-line)#password cisco
MulticapaM1(config-line)#login
MulticapaM1(config-line)#end
MulticapaM1#
```

Para los demás switches se realizan las mismas operaciones solo cambia el nombre del *Hostname* de acuerdo al nombre que se le haya dado a cada equipo, en este caso para el switch S1 el hostname es *S1*, y para el Switch S2, el hostname es *S2*. Ahora se procede a configurar la administración de las direcciones IP de la VLAN 1 en cada uno de los switches de la siguiente manera:

Para el Switch S1:

```
S1>ena
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan1
S1(config-if)#ip address 172.16.1.101 255.255.255.0
S1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#exit
S1(config)#
```

Se aplican los mismos comandos en los demás switches, lo único que se cambia es la dirección IP que se le asigna a cada switch. Para el ***Switch S2*** es 172.16.1.102 255.255.255.0; y para el ***Switch MulticapaM1*** es 172.16.1.1 255.255.255.0.

Se configuran las puertas de enlace predeterminadas en los switches pertenecientes a la capa de acceso. En este caso los Switches S1 y S2 se le aplican los mismos comandos de la siguiente manera:

```
S1>ena
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 172.16.1.1
S1(config-if)#end
```

Se procede a configurar las troncales y los EtherChannel entre los switches. Se crearán 2 Port-Channel 1 y 2 respectivamente en cada uno de los switches. A continuación la configuración desde el Switch:

MulticapaM1 al Switch S1:

MulticapaM1>ena
Password:
MulticapaM1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MulticapaM1(config)#interface range fastethernet 0/7 - 8
MulticapaM1(config-if-range)#switchport trunk encapsulation dot1q
MulticapaM1(config-if-range)#switchport mode trunk
MulticapaM1(config-if-range)#channel-group 1 mode desirable
MulticapaM1(config-if-range)#

Del Switch MulticapaM1 al SwitchS2:

MulticapaM1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MulticapaM1(config)#interface range fastethernet 0/9 - 10
MulticapaM1(config-if-range)#switchport trunk encapsulation dot1q
MulticapaM1(config-if-range)#switchport mode trunk
MulticapaM1(config-if-range)#channel-group 2 mode desirable
MulticapaM1(config-if-range)#

Del SwitchS1 al MulticapaM1:

S1>ena
Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fastEthernet 0/11 - 12
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#channel-group 1 mode desirable
S1(config-if-range)#

Del Switch S1 al Switch S2:

S1(config-if-range)#exit
S1(config)#interface range fastEthernet 0/7 - 8
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#channel-group 2 mode desirable
S1(config-if-range)#

Del Switch S2 al MulticapaM1

S2>ena
Password:
S2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fastethernet 0/11 - 12
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#channel-group 1 mode desirable
S2(config-if-range)#

Del Switch S2 al Switch S1

S2(config-if-range)#exit
S2(config)#interface range fastethernet 0/11 - 12
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#channel-group 1 mode desirable
S2(config-if-range)#

Se procede a verificar las troncales entre los switches. Para eso, accedemos al switch multicapa y ejecutamos el siguiente comando:

MulticapaM1#show interfaces Trunk

Se puede observar la ejecución en la *Figura 10*:

```
MulticapaM1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/7       on           802.1q         trunking      1
Fa0/8       on           802.1q         trunking      1
Fa0/9       on           802.1q         trunking      1
Fa0/10      on           802.1q         trunking      1
Po1         on           802.1q         trunking      1
Po2         on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/7       1-1005
Fa0/8       1-1005
Fa0/9       1-1005
Fa0/10      1-1005
Po1         1-1005
Po2         1-1005

Port        Vlans allowed and active in management domain
Fa0/7       1
Fa0/8       1
Fa0/9       1
Fa0/10      1
Po1         1
Po2         1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/7       1
Fa0/8       1
Fa0/9       1
Fa0/10      1
Po1         1
Po2         1
MulticapaM1#
```

Figura 10: Ejecución del comando "Show Interface Trunk"

Para verificar los EtherChannel se utiliza el comando ***show etherchannel summary*** en cada uno de los switch. Lo ejecutamos en el switch multicapa para hacer la verificación así como se observa en la *Figura 11*:

```
MulticapaM1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           PAgP   Fa0/7(P) Fa0/8(P)
2      Po2(SU)           PAgP   Fa0/9(P) Fa0/10(P)
MulticapaM1#
```

Figura 11: Resumen de los EtherChannel en el Switch MulticapaM1

Ahora se procede a cambiar el modo del protocolo VTP (Virtual Trunking Protocol) en los switches de la capa de acceso. Se cambian de modo “Servidor” a modo “Cliente”. Primero verificamos el modo actual para verificar que en realidad están en modo “Servidor” ver *Figura 12*.

```
S1>ena
Password:
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.16.1.101 on interface Vl1 (lowest numbered VLAN interfac
e found)
S1#
```

Figura 12: Verificando modo del protocolo VTP en el Switch S1

Ejecutando el comando ***vtp mode client*** para cambiarlo a modo cliente. Ver *Figura 13.*

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vtp mode client
Setting device to VTP CLIENT mode.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
S1#
```

Figura 13: Cambiando el modo de operación del protocolo VTP a cliente en el Switch S1

En el switch multicapa, verificamos el estado del protocolo y se puede observar que se pueden soportar hasta 1005 VLANs localmente, tal como se ve en la *Figura 14.*

```
MulticapaM1>ena
Password:
MulticapaM1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 172.16.1.1 on interface Vl1 (lowest numbered VLAN interface
found)
MulticapaM1#
```

Figura 14: Estado del protocolo VTP en el switch multicapa

Ahora bien, en el switch multicapa se procede a crear el dominio VTP igualmente se crearan las VLAN 100 y 200 para el dominio.

De la siguiente manera:

```
MulticapaM1>ena
Password:
MulticapaM1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MulticapaM1(config)#vtp domain SWPOD
Changing VTP domain name from null to SWPOD
MulticapaM1(config)#vlan 100
MulticapaM1(config-vlan)#name administrativa
MulticapaM1(config-vlan)#exit
MulticapaM1(config)#vlan 200
MulticapaM1(config-vlan)#name ingenieria
MulticapaM1(config-vlan)#exit
```

Configuramos los puertos de los host para que estén en la VLAN correspondiente de acuerdo a la topología propuesta al inicio de este capitulo. Aplicamos la siguiente configuración en el Switch S1:

```
S1>ena
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface fastethernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 100
S1(config-if)#exit
S1(config)#
```

Y para el Switch S2:

```
S2>ena
Password:
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface fastethernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 200
S2(config-if)#exit
S2(config)#
```

En este punto aun no hay enrutamiento entre las VLANs. Para lograrlo se debe recordar la práctica anterior. Se accede al switch multicapa y se crean las interfaces VLAN de capa 3. Adicional a eso se usará el comando ***ip-routing*** como se hizo en la práctica anterior para habilitar el enrutamiento de la siguiente manera:

MulticapaM1>ena
Password:
MulticapaM1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MulticapaM1(config)#interface vlan 100
MulticapaM1(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up
MulticapaM1(config-if)#ip add 172.16.100.1 255.255.255.0
MulticapaM1(config-if)#no shutdown
MulticapaM1(config-if)#interface vlan 200
MulticapaM1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up
MulticapaM1(config-if)#ip address 172.16.200.1 255.255.255.0
MulticapaM1(config-if)#no shutdown
MulticapaM1(config-if)#exit
MulticapaM1(config)#ip routing
MulticapaM1(config)#exit
MulticapaM1#

Verificamos la configuración con el comando ***show ip route***. Ver *Figura 15.*

```
MulticapaM1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, Vlan1
C       172.16.100.0 is directly connected, Vlan100
C       172.16.200.0 is directly connected, Vlan200
MulticapaM1#
```

Figura 15: IP Route en el Switch Multicapa

Se puede observar que las VLAN quedaron asignadas a las redes correspondientes como se había propuesto en la topología inicial. Realizamos un ping para ver si la configuración hasta el momento esta correcta. Ver *Figura 16*.

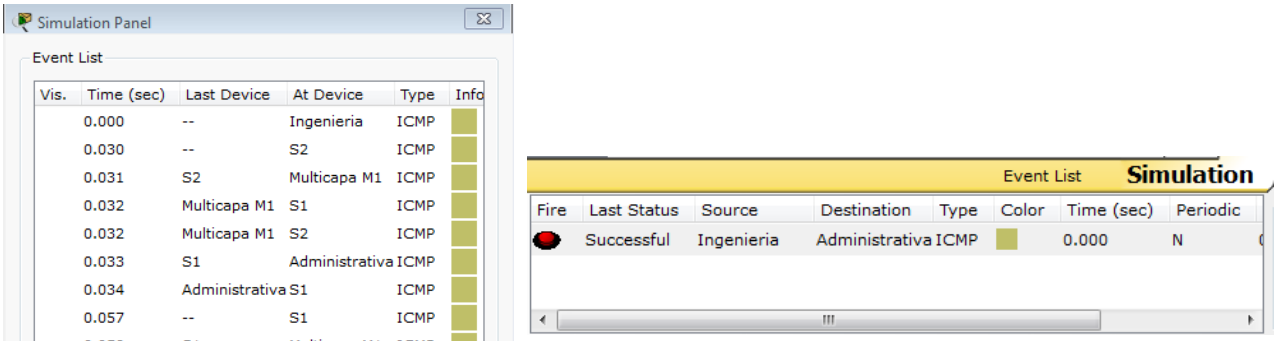


Figura 16: Resultados Simulación Ping de un departamento a otro.

Igualmente se intenta acceder remotamente al switch multicapa por telnet. Se toma el host de ingeniería para acceder al switch. Ver *Figura 17*.

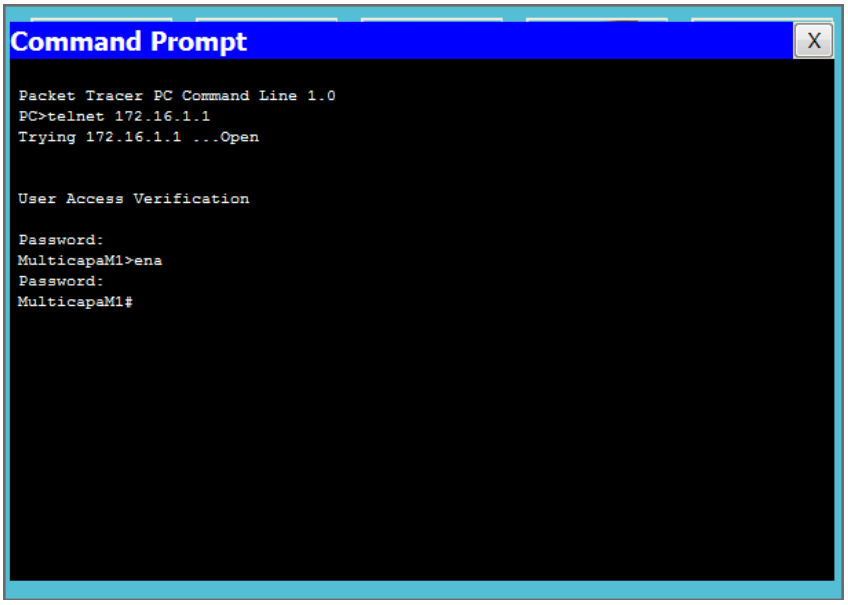


Figura 17: Acceso mediante telnet al switch multicapa

Se puede observar en la figura anterior que es posible acceder remotamente al switch multicapa desde un host en el departamento de ingeniería. Igualmente se puede acceder a él, desde el otro departamento.

Ahora bien, CEF (Cisco Express Forwarding) implementa un avanzado algoritmo de seguimiento y búsqueda para entregar el máximo rendimiento en la capa 3. El protocolo CEF está habilitado por defecto en los Switches 3560. Para ver el estado del protocolo simplemente ejecutamos el comando ***show ip cef.*** Ver *Figura 18.*

```
MulticapaM1>ena
Password:
MulticapaM1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           no route
0.0.0.0/32          receive
172.16.1.0/24       attached            Vlan1
172.16.1.0/32       receive             Vlan1
172.16.1.1/32       receive             Vlan1
172.16.1.255/32     receive             Vlan1
172.16.100.0/24     attached            Vlan100
172.16.100.0/32     receive             Vlan100
172.16.100.1/32     receive             Vlan100
172.16.100.101/32   172.16.100.101      Vlan100
172.16.100.255/32   receive             Vlan100
172.16.200.0/24     attached            Vlan200
172.16.200.0/32     receive             Vlan200
172.16.200.1/32     receive             Vlan200
172.16.200.101/32   172.16.200.101      Vlan200
172.16.200.255/32   receive             Vlan200
224.0.0.0/4         drop
224.0.0.0/24        receive
255.255.255.255/32  receive
MulticapaM1#
```

Figura 18: Estado del Protocolo CEF (Cisco Express Forwarding) en el Switch Multicapa

Para ver un resumen de la tabla CEF se utiliza el comando ***show ip cef summary***. Ver *Figura 19.*

```
MulticapaM1#show ip cef summary
IPv4 CEF is enabled for distributed and running
VRF Default:
 19 prefixes (19/0 fwd/non-fwd)
 Table id 0
 Database epoch:        4 (19 entries at this epoch)

MulticapaM1#
```

Figura 19: Resumen de las entradas contenidas en la Tabla FIB del protocolo CEF

Para ver la operación detalla del protocolo para el switch multicapa se utiliza el comando ***show ip cef detail***. Ver *Figura 20*.

```
MulticapaM1#show ip cef detail
IPv4 CEF is enabled for distributed and running
VRF Default:
 19 prefixes (19/0 fwd/non-fwd)
 Table id 0
 Database epoch:        4 (19 entries at this epoch)

0.0.0.0/0, epoch 4, flags default route handler
  no route
0.0.0.0/32, epoch 4, flags receive
  Special source: receive
  receive
172.16.1.0/24, epoch 4, flags attached
  attached to Vlan1
172.16.1.0/32, epoch 4, flags receive
  Interface source: Vlan1
  receive for Vlan1
172.16.1.1/32, epoch 4, flags receive
  Interface source: Vlan1
  receive for Vlan1
172.16.1.255/32, epoch 4, flags receive
  Interface source: Vlan1
  receive for Vlan1
172.16.100.0/24, epoch 4, flags attached
  attached to Vlan100
172.16.100.0/32, epoch 4, flags receive
  Interface source: Vlan100
  receive for Vlan100
172.16.100.1/32, epoch 4, flags receive
  Interface source: Vlan100
  receive for Vlan100
172.16.100.101/32, epoch 4
  Adj source: IP adj out of Vlan100, addr 172.16.100.101
  attached to Vlan100
172.16.100.255/32, epoch 4, flags receive
  Interface source: Vlan100
  receive for Vlan100
172.16.200.0/24, epoch 4, flags attached
  attached to Vlan200
172.16.200.0/32, epoch 4, flags receive
  Interface source: Vlan200
  receive for Vlan200
172.16.200.1/32, epoch 4, flags receive
  Interface source: Vlan200
  receive for Vlan200
172.16.200.101/32, epoch 4
  Adj source: IP adj out of Vlan200, addr 172.16.200.101
  attached to Vlan200
172.16.200.255/32, epoch 4, flags receive
  Interface source: Vlan200
  receive for Vlan200
224.0.0.0/4, epoch 4
  Special source: drop
  drop
224.0.0.0/24, epoch 4, flags receive
  Special source: receive
  receive
255.255.255.255/32, epoch 4, flags receive
  Special source: receive
  receive
```

Figura 20: Operación detallada sobre cada entrada en la tabla FIB del protocolo CEF

3.2.5 Conclusiones: Los switches cisco poseen 2 generaciones de conmutación multicapa o más conocida como MLS (Multilayer Switching) que son la "*Route Catching"* y la *"Basada en Topología"* esta generación basada en topología es la que se utiliza en la actualidad debido a que utiliza circuitos integrados especializados para construir una base de datos única con toda la topología de red. A esto es a lo que se le conoce como CEF (Cisco Express Forwarding) el cual

hemos puesto en práctica en esta segunda prueba. Cabe anotar que en esta prueba se ha utilizado un Switch Cisco Catalyst 3560-24PS y la funcion CEF está habilitada por defecto. Existen dispositivos en los cuales CEF no viene habilitado por defecto y se debe habilitar con el comando ***ip cef*** en modo de configuración global. Igualmente para deshabilitarlo se utiliza el comando ***no ip cef***.

Con esta prueba se recalcan las ventajas de los switches multicapa frente a los switches convencionales, igualmente resalta la eficiencia que estos brindan al momento de conmutar grandes cantidades de paquetes garantizando seguridad, eficiencia, redundancia y disponibilidad del servicio siempre.

PRACTICA No. 3

3.3 CONFIGURANDO EL PROTOCOLO SPANNING TREE – STP

3.3.1 Objetivo: Esta práctica se dividirá en 2 partes. En la primera parte se observará que sucede cuando el comportamiento por defecto del protocolo STP es modificado. En la segunda parte se observará lo que sucede cuando existe una instancia separada del protocolo STP por Vlan. Por último se cambiará de modo Spanning-Tree Regular (PVST) a modo Rapid Spanning-Tree (RSTP).

3.3.2 Ventajas y Desventajas del Protocolo STP

Las *ventajas* del protocolo STP son las siguientes:

- Se encarga de eliminar y evitar bucles en la red
- Evita tormentas de broadcast o multicast
- Evita copias múltiples de una misma trama
- Evita la inestabilidad de las tablas de direcciones MAC

Igualmente, existen algunas *desventajas* del protocolo STP, un Spanning Tree Simple impide el balanceo de carga, y puede llevar a que la conectividad en ciertas VLANs este incompleta (un simple STP de una Vlan podría seleccionar un enlace que no esté incluido en otra VLAN). Pero para solucionar estas desventajas existe una mejora del protocolo el RSTP.

3.3.3 Escenario: Para esta práctica se utilizará el simulador Packet Tracer 5.3.2.0027 en el cual crearemos una topología con 4 Switches. Se tendrán 2 capas, la de distribución y la de acceso. Para la capa de distribución se utilizarán 2 Switches Cisco Catalyst 3560, y para la capa de acceso 2 Switches Cisco Catalyst 2960. Se tendrán enlaces redundantes entre la capa de distribución, y la capa de acceso debido a la posibilidad de que aparezcan los llamados "Bridging Loops".
La topología se muestra en la *Figura 21*.

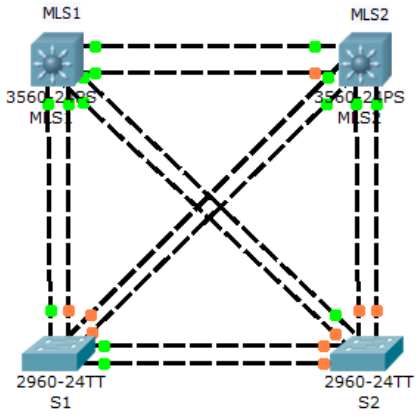


Figura 21. Topología utilizada para la práctica de STP

3.3.4 Desarrollo 1° Parte:

En los switches cisco, el protocolo STP viene activado por defecto. Es decir, sin necesidad de configurar los switches, automáticamente habilitan el protocolo. Para ver el Spanning-tree por defecto se utiliza el comando ***show Spanning-tree*** en modo de configuración global. Se ejecuta en cada uno de los switches, para saber cuál de ellos es el switch raíz. Así:

Switch MLS1:

```
MLS1#show sp
MLS1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.43C7.0480
              Cost        19
              Port        11(FastEthernet0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Altn BLK 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

Ilustración 1. Show Spanning Tree en MLS1

Switch MLS2:

```
MLS2#show spa
MLS2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.43C7.0480
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.43C7.0480
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
```

Ilustración 2. Show Spanning Tree (Bridge Root en MLS2)

Switch S1:

```
S1#show spa
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.43C7.0480
              Cost        19
              Port        9(FastEthernet0/9)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.639B.E212
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Root FWD 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
```

Ilustración 3. Show Spanning Tree (Non Root Bridge en S1)

Switch S2:

```
S2#show spa
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.43C7.0480
              Cost        19
              Port        7(FastEthernet0/7)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00E0.B088.E835
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Root FWD 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Altn BLK 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p
Fa0/11           Altn BLK 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

Ilustración 4. Show Spanning Tree (Non Root Bridge en S2)

Ahora bien, MLS2 es el switch raíz principal. Lo que se hará a continuación es cambiar el switch raíz principal y crear un switch raíz secundario. El nuevo switch raíz principal será MLS1 y el switch raíz secundario será S1. Para hacerlo se utilizan los comandos ***Spanning-tree Vlan [Vlan_number] root primary*** y ***Spanning-tree Vlan [Vlan_number] root secondary***. Para monitorear los cambios en la topología se utilizará el comando ***debug Spanning-tree events.*** Este comando se ejecuta en el switch que no va hacer modificado. En este caso, en el switch MLS2. *(Packet Tracer no soporta este comando por ese motivo no se monitorearan los cambios de la topología en este caso).*

Para cambiar el switch raíz se accede al switch que se quiere colocar como el nuevo switch raíz. En este caso, el nuevo switch raíz será MLS1, y el nuevo switch secundario será el S1.

Switch MLS1:

```
MLS1>ena
MLS1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
MLS1(config)#spanning-tree vlan 1 root primary
MLS1(config)#exit
MLS1#
```

Switch S1:

```
S1>ena
S1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#spanning-tree vlan 1 root secondary
S1(config)#exit
S1#
```

Como se pudo observar en la configuración por defecto del Spanning-tree, la prioridad por defecto es (*32769)*. Al ejecutar los comandos anteriores se observa

que la prioridad cambia. Escribimos tanto en el switch MLS1 como el switch S1 el comando ***show Spanning-tree*** para ver los cambios en la prioridad.

Switch MLS1:

```
MLS1#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
```

Ilustración 5. Show Spanning Tree (Root Bridge Prioridad)

Switch S1:

```
S1#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              Cost        19
              Port        7(FastEthernet0/7)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28673  (priority 28672 sys-id-ext 1)
              Address     0001.639B.E212
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Root FWD 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
```

Ilustración 6. Show Spanning Tree (Non Root Bridge Prioridad

Con Spanning-tree, también se puede modificar la prioridad de los puertos para determinar que puertos están en modo *Forward (FWD)* y cuales están en modo *Blocking (BLK)*. Para escoger que puerto se vuelve la raíz en un switch no-raiz cuando enfrenta rutas raíces redundantes, el switch mira la prioridad de los puertos primero, es decir, el switch escoge el puerto con el menor número de puerto. Por ejemplo, en el enlace entre MLS1 y MLS2, el puerto *forward* por defecto es Fa0/11 porque es el más bajo. Y el puerto *blocking* por defecto es Fa0/12 porque es el más alto. Los dos puertos tienen el mismo costo porque van a la misma velocidad. Más adelante se explicará como modificar esto. Se ejecuta nuevamente show Spanning-tree en el switch que no es raíz, en este caso el MLS2, se observa que los puertos Fa0/11 y Fa0/12 tienen el mismo costo (19) y el estado de Fa0/11 es FWD y el de Fa0/12 es BLK. (En el switch raíz todos los puertos están en modo FWD).

```
MLS2#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              Cost        19
              Port        11(FastEthernet0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.43C7.0480
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/9            Altn BLK 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p

MLS2#
```

Ilustración 7. Show Spanning Tree (Estado de los Puertos)

El rango de prioridad de los puertos va de 0 a 240, en incrementos de 16. La prioridad por defecto es 128 (como se pudo observar en las ejecuciones anteriores) y una prioridad más baja es requerida. Para cambiarle la prioridad a un

puerto, se hace en el switch más cercano a la raíz. Si se quiere que el puerto Fa0/12 sea el puerto raíz en el MLS2, y bloquear el puerto Fa0/11 se ejecuta en el switch MLS1 de la siguiente manera:

```
MLS1>ena
MLS1#conf ter
MLS1(config)#interface f0/12
MLS1(config-if)#spanning-tree port-priority 112
                        ^
% Invalid input detected at '^' marker.
MLS1(config-if)#spanning-tree vlan 1 port-priority 112
MLS1(config-if)#
```

NOTA:

En Switches reales se utiliza: **Spanning-tree port-priority *prioridad.***

Pero para que funcione en Packet Tracer se debe especificar la Vlan a la que pertenece el puerto de la siguiente manera:

Spanning-tree Vlan *numero* port-priority *prioridad*

Ahora se puede mirar que puerto esta en modo *blocking* en MLS2.

```
MLS2#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              Cost        19
              Port        12(FastEthernet0/12)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.43C7.0480
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Altn BLK 19        128.11   P2p
Fa0/12           Root FWD 19        128.12   P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/9            Altn BLK 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p

MLS2#
```

Ilustración 8. Show Spanning Tree (Estado de los Puertos en MLS2)

Como se puede observar, el puerto raíz ha cambiado, pero las prioridades siguen iguales. Se puede ver el cambio de prioridad en MLS1.

```
MLS1#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     0050.0FB6.2A30
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0050.0FB6.2A30
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        112.12   P2p
```

Ilustración 9. Show Spanning Tree (Cambio de Prioridad en MLS1)

Otra manera de cambiar el puerto raíz es modificando el costo del puerto utilizando el comando **Spanning-tree cost *costo*** en la interface en la cual se quiere cambiar el costo. Los costos por defecto para Gigabit Ethernet (4), para Fast Ethernet (19), y para 10BaseT Ethernet (100). Packet Tracer no soporta este comando por lo cual no se utilizará en esta práctica. Si se tiene un switch real se puede usar perfectamente este comando.

3.3.5 Desarrollo 2° Parte:

Para la segunda parte lo primero que se debe hacer es configurar los puertos Fa0/7 hasta Fa0/12 para que sean troncales. De la siguiente manera:

Switch MLS1:

```
MLS1>ena
MLS1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
MLS1(config)#interface range fastEthernet 0/7 - 12
MLS1(config-if-range)#switchport trunk encapsulation dot1q
MLS1(config-if-range)#switchport mode trunk
```

Switch MLS2:

```
MLS2>ena
MLS2#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
```

MLS2(config)#interface range fastethernet 0/7 - 12
MLS2(config-if-range)#switchport trunk encapsulation dot1q
MLS2(config-if-range)#switchport mode trunk

Switch S1:

S1>ena
S1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range fastEthernet 0/7 - 12
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#

Switch S2:

S2>ena
S2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fastEthernet 0/7 - 12
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#

A continuación, se creará un dominio VTP (como se hizo en la práctica No. 2, le colocaremos de nombre “cisco”) se cambiara el modo VTP a *transparent* y se crearán 2 Vlan, la 10 y la 20 respectivamente. De la siguiente manera:

Switch MLS1:

MLS1>ena
MLS1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
MLS1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
MLS1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
MLS1(config)#vlan 10
MLS1(config-vlan)#name ingenieria
MLS1(config-vlan)#exit
MLS1(config)#vlan 20
MLS1(config-vlan)#name administrativa
MLS1(config-vlan)#exit

Switch MLS2:

MLS2>ena
MLS2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
MLS2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
MLS2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
MLS2(config)#vlan 10
MLS2(config-vlan)#name ingenieria
MLS2(config-vlan)#exit
MLS2(config)#vlan 20
MLS2(config-vlan)#name administrativa
MLS2(config-vlan)#exit
MLS2(config)#

Switch S1:

S1>ena
S1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
S1(config)#vlan 10
S1(config-vlan)#name ingenieria
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name administrativa
S1(config-vlan)#exit
S1(config)#

Switch S1:

S2>ena
S2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
S2(config)#vlan 10

S2(config-vlan)#name ingenieria
S2(config-vlan)#exit
S2(config)#vlan 20
S2(config-vlan)#name administrativa
S2(config-vlan)#exit

Si se utiliza el comando show spanning-tree en cualquiera de los 4 switches, se puede notar que en vez de una sola Vlan, hay múltiples Vlan.

```
MLS1#
MLS1#show sp
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        112.12   P2p
```

Ilustración 10. Show Spanning Tree (Mostrando la Vlan - 1)

```
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0001.43C7.0480
              Cost        19
              Port        11(FastEthernet0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Altn BLK 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

Ilustración 11. Show Spanning Tree (Mostrando la Vlan - 10)

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    32788
              Address     0001.43C7.0480
              Cost        19
              Port        11(FastEthernet0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Altn BLK 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

Ilustración 12. Show Spanning Tree (Mostrando las Vlan - 20)

Se puede notar que todos los puertos poseen un comportamiento de Spanning-tree idéntico. Esto es debido a que todas las Vlan están ejecutando el protocolo con el comportamiento por defecto. Sin embargo, se puede modificar este comportamiento por defecto por una base per-Vlan. Recordando la primera parte de esta práctica, MLS1 es el switch raíz. Entonces, se asignará en MLS1 la Vlan 10 como la raíz y en MLS2 la Vlan 20 como la raíz.

Switch MLS1:

```
MLS1>ena
MLS1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
MLS1(config)#spanning-tree vlan 10 priority 4096
MLS1(config)#exit
MLS1#
```

Switch MLS2:

```
MLS2>ena
MLS2#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
MLS2(config)#spanning-tree vlan 20 priority 4096
MLS2(config)#
```

Si se ejecuta el comando ***show Spanning-tree*** en los 4 switches se puede observar que el estado de los puertos y los switches raíz varían con base a las Vlan. Como ejemplo se observará el comportamiento de la Vlan 20.

MLS1:

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     0001.43C7.0480
              Cost        19
              Port        11(FastEthernet0/11)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Altn BLK 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p

MLS1#
```

Ilustración 13. Show Spanning Tree (Comportamiento de los puertos Vlan 20 en MLS1)

MLS2:

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     0001.43C7.0480
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4116  (priority 4096 sys-id-ext 20)
              Address     0001.43C7.0480
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p

MLS2#
```

Ilustración 14. Show Spanning Tree (Comportamiento de los puertos Vlan 20 en MLS2)

S1:

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     0001.43C7.0480
              Cost        19
              Port        9(FastEthernet0/9)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     0001.639B.E212
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Root FWD 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        128.12   P2p

S1#
```

Ilustración 15. Show Spanning Tree (Comportamiento de los puertos Vlan 20 en S1)

S2:

```
VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    4116
              Address     0001.43C7.0480
              Cost        19
              Port        7(FastEthernet0/7)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     00E0.B088.E835
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/7            Root FWD 19        128.7    P2p
Fa0/8            Altn BLK 19        128.8    P2p
Fa0/9            Altn BLK 19        128.9    P2p
Fa0/10           Altn BLK 19        128.10   P2p
Fa0/11           Altn BLK 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p

S2#
```

Ilustración 16. Show Spanning Tree (Comportamiento de los puertos Vlan 20 en S2)

Como se puede observar debajo del nombre de la Vlan dice: *"Spanning tree enabled protocol ieee"* eso quiere decir que el protocolo está habilitado en modo básico o regular. Pero existen otros modos de Spanning-tree como el RSTP

(Rapid Spanning Tree Protocol) el cual reduce en gran cantidad el tiempo entre la subida y el cambio a modo FWD del puerto mientras previene los posibles "Bridgning Loops" que se puedan presentar. Para cambiar a este modo se utiliza el comando ***Spanning-tree mode rapid-pvst.*** Se configura en los 4 switches y luego se observa con el comando ***show Spanning-tree*** si se habilita o no.

Switches MLS1, MLS2, S1 y S2:

Switch>ena
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#exit

```
MLS1(config)#spanning-tree mode rapid-pvst
MLS1(config)#exit
MLS1#
%SYS-5-CONFIG_I: Configured from console by console
show sp
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     0050.0FB6.2A30
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/7            Desg FWD 19        128.7    P2p
Fa0/8            Desg FWD 19        128.8    P2p
Fa0/9            Desg FWD 19        128.9    P2p
Fa0/10           Desg FWD 19        128.10   P2p
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/12           Desg FWD 19        112.12   P2p

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    4106
              Address     0050.0FB6.2A30
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
              Address     0050.0FB6.2A30
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
 --More--
```

Ilustración 17. Show Spanning Tree (Habilitando el protocolo RSTP)

3.3.6 Conclusiones: En esta práctica se puedo observar la importancia del protocolo Spanning-tree para garantizar eficiencia y redundancia en una red. Se trataron las características más utilizadas por el protocolo, debido a que el simulador no permite utilizar algunos comandos asociados al protocolo que si se pueden usar en los switches físicos. Pero se podría decir que Spanning-tree va mucho más allá de lo que se hizo en esta práctica, ya queda al interés del lector un mayor estudio sobre el protocolo y todos sus alcances.

Practica No. 4

3.4 CONFIGURANDO HSRP (HOST STANDBY ROUTER PROTOCOL) y MHSRP EN UNA RED INTERNA PARA GARANTIZAR REDUNDANCIA Y BALANCEO DE CARGA.

3.4.1 Objetivo: Configurar el enrutamiento entre Vlan con HSRP (Host Standby Router Protocol) para garantizar redundancia, y tolerancias a fallas de enrutamiento en la red interna.

3.4.2 Ventajas y Desventajas del Protocolo HSRP

Ventajas.

- Es muy flexible. El administrador de red puede controlar todo el comportamiento de los router de un grupo.
- La configuración básica requiere solamente el subcomando de configuración de interfaz de IOS *standby ip.*
- Ofrece un nivel de escalabilidad bastante bueno ya que además, es posible adaptar el modelo de redundancia hasta por ejemplo, conexión de VPN’s redundantes.

Desventajas

Una de las desventajas del HSRP original era que no permitía al administrador de red compartir la carga del tráfico que cruza ambos routers del grupo de reserva. Básicamente, el router de reserva estaría inactivo a menos que fallará el router de reenvío activo. Para solucionar este problema, se añadió al software IOS la capacidad para admitir varios grupos HSRP en la misma interfaz (MHSRP). En la misma interfaz se pueden crear varios grupos HSRP, cada uno de ellos con una dirección IP virtual distinta, para respaldarse unos a otros. Con dos grupos HSRP y dos direcciones IP virtuales definidas, el administrador de red puede configurar el Gateway predeterminado en algunos de los host con una de las direcciones virtuales de HSRP, y en los host restantes, con la otra. Aunque no consigue un equilibrado de la carga exactamente igual, esta configuración *comparte la carga* entre los dos routers en lugar de sobrecargar sustancialmente uno de ellos mientras el otro se queda completamente inactivo.

3.4.3 Escenario: Esta práctica se realizará en el laboratorio de redes de la Universidad Tecnológica de Bolívar. Para esta práctica se utilizará la misma topología de la práctica anterior, con la diferencia que ahora se agregarán 2 host (1 para la Vlan 10, y el otro para la Vlan 20) y 2 servidores (un servidor financiero que estará en la Vlan 30 y un servidor SQL que estará en la Vlan 40). Las puertas de enlace HSRP serán: Para la VLAN1, 172.16.1.1/24, Para la VLAN10, 172.16.10.1/24, Para la VLAN20, 172.16.20.1/24, Para la VLAN30, 172.16.30.1/24, y Para la VLAN40, 172.16.40.1/24. HSRP proveerá un mecanismo de fallos transparente para las estaciones finales en la red. Esto provee a los usuarios de “Servicio Ininterrumpido” en el momento de que algún router falle.

Materiales Necesarios para la Practica: 2 Switches Cisco Catalyst 3560 de 12 puertos o mas, 2 Switches Cisco Catalyst 2960 de 12 puertos o más, 12 cables UTP Cat.5e o superior preferiblemente ponchados en sus extremos, 2 equipos que

serán servidores, y 2 Hosts. En la *Figura 22* se puede observar la topología que se utilizará.

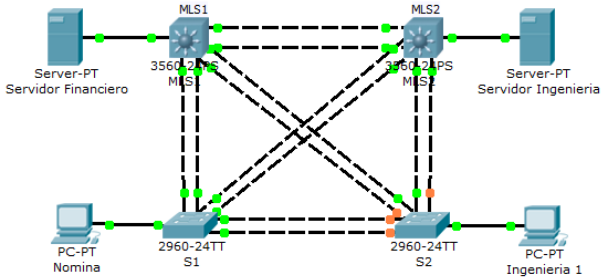


Figura 22. Topología utilizada para la práctica de HSRP

3.4.4 Desarrollo:

Primero se procede a configurar en cada uno de los Switches el nombre del equipo, su contraseña, y su acceso telnet, igualmente en la vlan1 las direcciones IP para administración. De la siguiente manera:

```
Switch#
Switch#confi ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname MLS1
MLS1(config)#enable secret cisco
MLS1(config)#line vty 0 15
MLS1(config-line)#password cisco
MLS1(config-line)#login
MLS1(config-line)#exit
MLS1(config)#interface vlan 1
MLS1(config-if)#ip address 172.16.1.3 255.255.255.0
MLS1(config-if)#no shutdown
MLS1(config-if)#end
MLS1#
```

De igual manera en el resto de los Switches se aplican los mismos comandos, y solo cambia el hostname y la dirección IP de la vlan1. El segundo switch multicapa se llamará MLS2, y los Switches de la capa de acceso (Catalyst 2960) serán S1 y S2 respectivamente. La Vlan1 de MLS2 tendrá la IP 172.16.1.4 y mascara de subred 255.255.255.0. La IP de la Vlan1 en los Switches S1 y S2 serán

172.16.1.101 con mascara 255.255.255.0 y 172.16.1.102 con mascara 255.255.255.0 respectivamente.

Posteriormente se procede a configurar las puertas de enlace predeterminada en los Switches de la capa de acceso (S1 y S2). En los Switches de la capa de distribución no necesitan configurarse puertas de enlace predeterminadas porque actúan como dispositivos de capa 3

```
S1#conf ter
S1(config)#ip default-gateway 172.16.1.1
S1(config)#end
S1#
```

A continuación se procede a configurar las troncales y el EtherChannel entre los Switches. El EtherChannel se utiliza para estas troncales y permite utilizar ambas interfaces FastEthernet disponibles en cada dispositivo por lo cual la banda se duplica. Así:

En MLS1:

```
MLS1>
MLS1#conf ter
MLS1(config)#interface range fastethernet 0/7 - 8
MLS1(config-if-range)#switchport trunk encapsulation dot1q
MLS1(config-if-range)#switchport mode trunk
MLS1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
MLS1(config-if-range)#end

MLS1#conf ter
MLS1(config)#interface range fastethernet 0/9 - 10
MLS1(config-if-range)#switchport trunk encapsulation dot1q
MLS1(config-if-range)#switchport mode trunk
MLS1(config-if-range)#channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2
MLS1(config-if-range)#end

MLS1#conf ter
MLS1(config)#interface range fastethernet 0/11 - 12
MLS1(config-if-range)#switchport trunk encapsulation dot1q
MLS1(config-if-range)#switchport mode trunk
MLS1(config-if-range)#channel-group 3 mode desirable
```

Creating a port-channel interface Port-channel 3
MLS1(config-if-range)#end

Nota: Para verificar si todo está bien ejecutar el comando show running-config en modo de configuración global

En MLS2:

MLS2>
MLS2#conf ter
MLS2(config)#interface range fastethernet 0/7 - 8
MLS2(config-if-range)#switchport trunk encapsulation dot1q
MLS2(config-if-range)#switchport mode trunk
MLS2(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
MLS2(config-if-range)#end

MLS2#conf ter
MLS2(config)#interface range fastethernet 0/9 - 10
MLS2(config-if-range)#switchport trunk encapsulation dot1q
MLS2(config-if-range)#switchport mode trunk
MLS2(config-if-range)#channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2
MLS2(config-if-range)#end

MLS2#conf ter
MLS2(config)#interface range fastethernet 0/11 - 12
MLS2(config-if-range)#switchport trunk encapsulation dot1q
MLS2(config-if-range)#switchport mode trunk
MLS2(config-if-range)#channel-group 3 mode desirable
Creating a port-channel interface Port-channel 3
MLS2(config-if-range)#end

Nota: Para verificar si todo está bien ejecutar el comando show running-config en modo de configuración global

En S1:

S1>
S1#conf ter
S1(config)#interface range fastEthernet 0/7 - 8
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)#exit

S1(config)#interface range fastEthernet 0/9 - 10
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#channel-group 2 mode desirable
Creating a port-channel interface Port-channel 2
S1(config-if-range)#exit

S1(config)#interface range fastEthernet 0/11 - 12
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#channel-group 3 mode desirable
Creating a port-channel interface Port-channel 3
S1(config-if-range)#exit

Nota: Se puede notar que no es necesario ningún tipo de encapsulación en los Switches 2960 debido a que estos Switches solo soportan troncales 802.1q.

Se Verifican las troncales entre MLS1, S1 y S2 utilizando el comando ***show interface trunk*** en todos los Switches. Por ejemplo en MLS1:

MLS1>ena
Password:
MLS1#show interface trunk

Port	*Mode*	*Encapsulation*	*Status*	*Native vlan*
Po1	*on*	*802.1q*	*trunking*	*1*
Po2	*on*	*802.1q*	*trunking*	*1*
Po3	*on*	*802.1q*	*trunking*	*1*

Port	*Vlans allowed on trunk*
Po1	*1-4094*
Po2	*1-4094*
Po3	*1-4094*

Port	*Vlans allowed and active in management domain*
Po1	*1*
Po2	*1*
Po3	*1*

Port	*Vlans in spanning tree forwarding state and not pruned*
Po1	*1*
Po2	*1*
Po3	*1*

Nota: En todos los Switches debe mostrar lo anterior.

Ahora se cambia el modo del VTP de *"Server"* a *"Cliente"* en los Switches de la capa de acceso, en este caso los Switches S1y S2. En modo de configuración privilegiado utilizando el comando ***vtp mode client***. Luego se crea el dominio VTP en MLS1 y se crean las Vlans 10, 20, 30 y 40.

En S1 y S2:

S1>
S1#conf ter
S1(config)#vtp mode client
Setting device to VTP CLIENT mode

S2>
S2#conf ter
S2(config)#vtp mode client
Setting device to VTP CLIENT mode

Nota: Para verificar el estado del protocolo vtp en los Switches utilizar el comando "show vtp status" en modo de configuración global.

En MLS1:

MLS1>ena
Password:
MLS1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
MLS1(config)#vtp domain HSRP
Changing VTP domain name from NULL to HSRP
MLS1(config)#inter
MLS1(config)#vlan 10
MLS1(config-vlan)#name financiera
MLS1(config-vlan)#exit
MLS1(config)#vlan 20
MLS1(config-vlan)#name ingenieria
MLS1(config-vlan)#exit
MLS1(config)#vlan 30
MLS1(config-vlan)#name servidor-1
MLS1(config-vlan)#exit
MLS1(config)#vlan 40
MLS1(config-vlan)#name servidor-2

MLS1(config-vlan)#exit
Nota: Verificar el estado VTP y las VLAN con los comandos "show vtp status" y "show vlan" respectivamente.

Se procede a configurar los hosts con las direcciones IP y sus puertas de enlace predeterminadas. Luego se configuran los puertos de los hosts en los 4 Switches (Todos los host estarán conectados a la Interface Fa0/6). Se colocan los puertos en sus Vlan correspondientes y se activa el "Spanning-tree Port Fast" para los puertos. Ejemplo de asignación de IP en el host de ingeniería (*Ver Figura 23*):

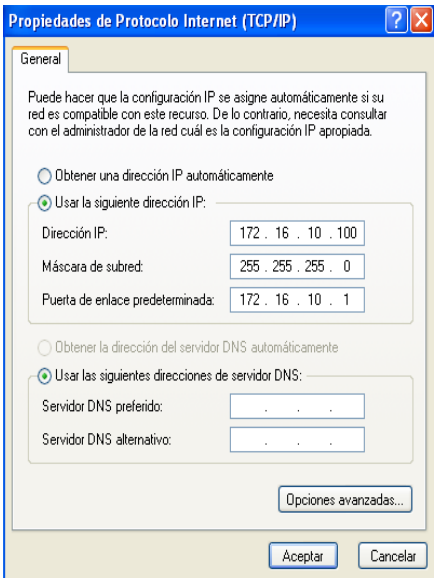


Figura 23.Asignando Dirección IP a uno de los Hosts

Configuración en MLS1:

MLS1#conf ter
MLS1(config)#interface fastEthernet 0/6
MLS1(config-if)#switchport mode access
MLS1(config-if)#switchport access vlan 30
MLS1(config-if)#spanning-tree portfast
MLS1(config-if)#exit
MLS1(config)#

Configuración en MLS2:

MLS2#conf ter

MLS2(config)#interface fastEthernet 0/6
MLS2(config-if)#switchport mode access
MLS2(config-if)#switchport access vlan 40
MLS2(config-if)#spanning-tree portfast
MLS2(config-if)#exit
MLS2(config)#

Configuración en S1:

S1#conf ter
S1(config)#interface fastEthernet 0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#spanning-tree portfast
S1(config-if)#exit
S1(config)#

Configuración en S2:

S2#conf ter
S2(config)#interface fastEthernet 0/6
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#spanning-tree portfast
S2(config-if)#exit
S2(config)#

A esta altura del proceso, si se realiza un ping de la Vlan 10 al host de la Vlan 40, no se obtendrá ningún resultado debido a que aun no se le ha dicho a los Switches multicapa que enruten entre sí. Para esto se utiliza el comando *"ip-routing"* (utilizado en la primera práctica de este trabajo). Ahora bien, una vez realizado esto, se procede a configurar el protocolo HSRP. (En este punto se deben tener claros los conceptos adquiridos en el capítulo 2 sobre este protocolo) Cada procesador de ruta puede enrutar entre varias interfaces virtuales (SVIs) configuradas en los Switches. Se asignará una tercera dirección IP en cada subred y se usará como puerta de enlace predeterminada virtual. HSRP negociará cual de los Switches acepta la información que viaja a la dirección IP de puerta de enlace virtual.

El comando ***standby*** configura la dirección IP de la puerta de enlace virtual, establece la prioridad para cada Vlan, y configura el router para ***Preempt***. Esto permite al router con la prioridad más alta convertirse en el "Active Router" después de que un fallo de red haya sido resuelto. A continuación se establecerán prioridades: Para la Vlan1, 10 y 20, la prioridad será de 150 en MLS1, convirtiéndolo en el "Active Router" para esas Vlans. Las Vlan 30 y 40 tendrán una prioridad de 100 en MLS1, convirtiéndolo en el "standby" router para esas Vlans. MLS2 se configurará para ser el "Active Router" de las Vlans 30 y 40 y el "standby" router para las Vlans 1, 10, y 20.

Configuración HSRP en MLS1:

```
MLS1>ena
Password:
MLS1#conf ter
MLS1(config)#ip routing
MLS1(config)#interface vlan 1
MLS1(config-if)#standby 1 ip 172.16.1.1
MLS1(config-if)#standby 1 preempt
MLS1(config-if)#standby 1 priority 150
MLS1(config-if)#exit
05:02:51: %HSRP-6-STATECHANGE: Vlan1 Grp 1 state Standby -> Active
MLS1(config)#interface vlan 10
MLS1(config-if)#ip address 172.16.10.3 255.255.255.0
MLS1(config-if)#standby 1 ip 172.16.10.1
MLS1(config-if)#standby 1 preempt
MLS1(config-if)#standby 1 priority 150
MLS1(config-if)#no shutdown
MLS1(config-if)#exit
05:04:11: %HSRP-6-STATECHANGE: Vlan10 Grp 1 state Standby -> Active
MLS1(config)#interface vlan 20
MLS1(config-if)#ip address 172.16.20.3 255.255.255.0
MLS1(config-if)#standby 1 ip 172.16.20.1
MLS1(config-if)#standby 1 preempt
MLS1(config-if)#standby 1 priority 150
MLS1(config-if)#exit
MLS1(config)#interface vlan 30
MLS1(config-if)#ip address 172.16.30.3 255.255.255.0
```

MLS1(config-if)#standby 1 ip 172.16.30.1
MLS1(config-if)#standby 1 preempt
05:08:21: %HSRP-6-STATECHANGE: Vlan30 Grp 1 state Speak -> Standby
MLS1(config-if)#standby 1 priority 100
MLS1(config-if)#exit
MLS1(config)#interface vlan 40
MLS1(config-if)#ip address 172.16.40.3 255.255.255.0
MLS1(config-if)#standby 1 ip 172.16.40.1
MLS1(config-if)#standby 1 preempt
MLS1(config-if)#standby 1 priority 100
MLS1(config-if)#end
MLS1#
05:10:45: %SYS-5-CONFIG_I: Configured from console by console
05:10:56: %HSRP-6-STATECHANGE: Vlan40 Grp 1 state Speak -> Stanby

Configuración HSRP en MLS2:

MLS2>ena
Password:
MLS2#conf ter
MLS2(config)#ip routing
MLS2(config)#interface vlan 1
MLS2(config-if)#standby 1 ip 172.16.1.1
MLS2(config-if)#standby 1 preempt
MLS2(config-if)#standby 1 priority 150
MLS2(config-if)#exit
**Mar 1 04:25:43.077: %HSRP-5-STATECHANGE: Vlan1 Grp 1 state Speak -> Standby*
MLS2(config)#interface vlan 10
MLS2(config-if)#ip address 172.16.10.4 255.255.255.0
MLS2(config-if)#standby 1 ip 172.16.10.1
MLS2(config-if)#standby 1 preempt
MLS2(config-if)#standby 1 priority 150
MLS2(config-if)#
**Mar 1 04:27:10.562: %HSRP-5-STATECHANGE: Vlan10 Grp 1 state Speak -> Standby*
MLS2(config-if)#no shutdown
MLS2(config-if)#exit
MLS2(config)#interface vlan 20
MLS2(config-if)#ip address 172.16.20.4 255.255.255.0
MLS2(config-if)#standby 1 ip 172.16.20.1
MLS2(config-if)#standby 1 preempt
MLS2(config-if)#standby 1 priority 150
MLS2(config-if)#exit
**Mar 1 04:30:47.005: %HSRP-5-STATECHANGE: Vlan20 Grp 1 state Speak -> Standby*

MLS2(config)#interface vlan 30
MLS2(config-if)#ip address 172.16.30.4 255.255.255.0
MLS2(config-if)#standby 1 ip 172.16.30.1
MLS2(config-if)#standby 1 preempt
MLS2(config-if)#standby 1 priority 100
MLS2(config-if)#exit
MLS2(config)#
**Mar 1 04:33:30.079: %HSRP-5-STATECHANGE: Vlan30 Grp 1 state Speak -> Active*
MLS2(config)#interface vlan 40
MLS2(config-if)#ip address 172.16.40.4 255.255.255.0
MLS2(config-if)#standby 1 ip 172.16.40.1
MLS2(config-if)#standby 1 preempt
MLS2(config-if)#standby 1 priority 100
MLS2(config-if)#exit
MLS2(config)#
**Mar 1 04:35:48.508: %HSRP-5-STATECHANGE: Vlan40 Grp 1 state Speak -> Active*

Para observar el estado del protocolo en las Vlan se utiliza el comando ***show standby*** en MLS1 y MLS2. Se obtiene lo siguiente:

En MLS1:

```
MLS1>
MLS1>ena
Password:
MLS1#show standby
Vlan1 - Group 1
  State is Active
    2 state changes, last state change 01:26:02
  Virtual IP address is 172.16.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)

  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.463 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.1.4, priority 150 (expires in 9.152 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl1-1" (default)

Vlan10 - Group 1
  State is Active
```

```
  2 state changes, last state change 01:24:43
 Virtual IP address is 172.16.10.1
 Active virtual MAC address is 0000.0c07.ac01
   Local virtual MAC address is 0000.0c07.ac01 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 0.945 secs
 Preemption enabled
 Active router is local
 Standby router is 172.16.10.4, priority 150 (expires in 9.874 sec)
 Priority 150 (configured 150)
 IP redundancy name is "hsrp-Vl10-1" (default)
Vlan20 - Group 1
 State is Active
   2 state changes, last state change 01:23:34
 Virtual IP address is 172.16.20.1
 Active virtual MAC address is 0000.0c07.ac01
   Local virtual MAC address is 0000.0c07.ac01 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 2.555 secs
 Preemption enabled
 Active router is local
 Standby router is 172.16.20.4, priority 150 (expires in 9.740 sec)
 Priority 150 (configured 150)
 IP redundancy name is "hsrp-Vl20-1" (default)
Vlan30 - Group 1
 State is Standby
   2 state changes, last state change 01:20:42
 Virtual IP address is 172.16.30.1
 Active virtual MAC address is 0000.0c07.ac01
   Local virtual MAC address is 0000.0c07.ac01 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 0.156 secs
 Preemption enabled
 Active router is 172.16.30.4, priority 150 (expires in 7.366 sec)
 Standby router is local
 Priority 100 (default 100)
 IP redundancy name is "hsrp-Vl30-1" (default)

Vlan40 - Group 1
 State is Standby
   2 state changes, last state change 01:18:10
 Virtual IP address is 172.16.40.1
 Active virtual MAC address is 0000.0c07.ac01
```

Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.952 secs
Preemption enabled
Active router is 172.16.40.4, priority 150 (expires in 7.777 sec)
standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Vl40-1" (default)

En MLS2:

MLS2#show standby
Vlan1 - Group 1
State is Standby
1 state change, last state change 01:11:24
Virtual IP address is 172.16.1.1
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.197 secs
Preemption enabled
Active router is 172.16.1.3, priority 150 (expires in 8.507 sec)
Standby router is local
Priority 150 (configured 150)
IP redundancy name is "hsrp-Vl1-1" (default)
Vlan10 - Group 1
State is Standby
1 state change, last state change 01:09:57
Virtual IP address is 172.16.10.1
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.777 secs
Preemption enabled
Active router is 172.16.10.3, priority 150 (expires in 9.991 sec)
Standby router is local
Priority 150 (configured 150)
IP redundancy name is "hsrp-Vl10-1" (default)
Vlan20 - Group 1
State is Standby
1 state change, last state change 01:06:25
Virtual IP address is 172.16.20.1
Active virtual MAC address is 0000.0c07.ac01
Local virtual MAC address is 0000.0c07.ac01 (v1 default)

```
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.574 secs
  Preemption enabled
  Active router is 172.16.20.3, priority 150 (expires in 7.374 sec)
  Standby router is local
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl20-1" (default)
Vlan30 - Group 1
  State is Active
    1 state change, last state change 01:03:45
  Virtual IP address is 172.16.30.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.291 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.30.3, priority 100 (expires in 9.211 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl30-1" (default)
Vlan40 - Group 1
  State is Active
    1 state change, last state change 01:01:28
  Virtual IP address is 172.16.40.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.320 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.40.3, priority 100 (expires in 9.824 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl40-1" (default)
MLS2#
```

Se verifica ahora el enrutamiento en ambos Switches con el comando ***show ip route***.

```
MLS1>ena
Password:
MLS1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.40.0 is directly connected, Vlan40
C       172.16.30.0 is directly connected, Vlan30
C       172.16.20.0 is directly connected, Vlan20
C       172.16.10.0 is directly connected, Vlan10
C       172.16.1.0 is directly connected, Vlan1
MLS1#
```

Ahora se procede a verificar el protocolo HSRP desconectando las troncales de MLS1 que es el "Active Router" para las Vlans 1, 10 y 20 y el "Standby Router" para las Vlans 30 y 40. Se observará como MLS2 se convierte en "Active Router" para las Vlans 30 y 40 al momento que MLS1 falla. Para no desconectar los cables físicamente en MLS1, utilizo el comando ***shutdown*** para apagar el rango de interfaces Fa0/7 – 12. Esto equivale a desconectar físicamente los cables del Switch. Así:

```
MLS1#
MLS1#conf ter
MLS1(config)#interface range fastEthernet 0/7 - 12
MLS1(config-if-range)#shutdown
MLS1(config-if-range)#
```

Una vez ejecutado el comando se observa lo siguiente en MLS1:

```
MLS1#
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to
down
```

06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to down
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to down
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
06:30:09: %HSRP-6-STATECHANGE: Vlan1 Grp 1 state Active -> Init
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
06:30:09: %HSRP-6-STATECHANGE: Vlan10 Grp 1 state Active -> Init
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
06:30:09: %HSRP-6-STATECHANGE: Vlan20 Grp 1 state Active -> Init
06:30:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
06:30:10: %LINK-3-UPDOWN: Interface Port-channel1, changed state to down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
06:30:10: %LINK-3-UPDOWN: Interface Port-channel2, changed state to down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
06:30:10: %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
06:30:10: %LINK-3-UPDOWN: Interface Port-channel3, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/7, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
06:30:11: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to down

Una vez se cae la conexión en MLS1, en MLS2 sucede lo siguiente:

MLS2#
*Mar 1 05:37:52.328: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
*Mar 1 05:37:52.337: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to down
*Mar 1 05:37:52.345: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to down
*Mar 1 05:37:53.327: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to down

*Mar 1 05:37:53.352: %LINK-3-UPDOWN: Interface Port-channel3, changed state to down
*Mar 1 05:37:53.352: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to down
*Mar 1 05:37:59.987: %HSRP-5-STATECHANGE: Vlan40 Grp 1 state Standby -> Active
*Mar 1 05:38:01.153: %HSRP-5-STATECHANGE: Vlan30 Grp 1 state Standby -> Active
*Mar 1 05:40:36.846: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to up
*Mar 1 05:40:36.846: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to up
*Mar 1 05:40:40.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up
*Mar 1 05:40:40.788: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up
*Mar 1 05:40:41.728: %LINK-3-UPDOWN: Interface Port-channel3, changed state to up
*Mar 1 05:40:42.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up

Como se puede observar, MLS2 se convierte en el “Active Router” para las Vlans 30 y 40, asumiendo la responsabilidad de toda la carga que pasaba por allí. En MLS1 se encienden nuevamente las troncales y una vez estén operativas, se ejecuta nuevamente el comando ***show standby*** y se observa que MLS1 ahora es el “Standby Router” para las Vlans 1, 10, y 20.

```
MLS1(config-if-range)#exit
MLS1(config)#exit
MLS1#show standby

Vlan1 - Group 1
  State is Standby
    4 state changes, last state change 00:01:08
  Virtual IP address is 172.16.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.961 secs
  Preemption enabled
  Active router is 172.16.1.4, priority 150 (expires in 7.559 sec)
  Standby router is local
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl1-1" (default)
Vlan10 - Group 1
  State is Standby
    4 state changes, last state change 00:01:08
  Virtual IP address is 172.16.10.1
```

```
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.374 secs
  Preemption enabled
  Active router is 172.16.10.4, priority 150 (expires in 9.044 sec)
  Standby router is local
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl10-1" (default)
Vlan20 - Group 1
  State is Standby
    4 state changes, last state change 00:01:12
  Virtual IP address is 172.16.20.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.256 secs
  Preemption enabled
  Active router is 172.16.20.4, priority 150 (expires in 7.215 sec)
  Standby router is local
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Vl20-1" (default)
```

Se nota como automáticamente MLS2 asume la responsabilidad de seguir con el servicio en la red por el fallo ocasionado en las Vlans de MLS1. Dado el caso en el cual las Vlans de MLS2 fallen, MLS1 volverá a ser el “Active Router” para esas Vlans. Para observar las configuración general en cada uno de los Switches utilicen el comando ***show running-config***. Con esto se concluye la práctica del protocolo de redundancia HSRP en una red interna.

Hasta este punto solo se ha demostrado la importancia del protocolo basándose en la redundancia para hacer frente a cualquier tipo de falla de un dispositivo. Con esta configuración toda la carga de la red siempre pasará por el router activo, quedando el otro en Standby sin que ningún paquete pase por él, solo si ocurre una falla en la red se convertirá en router activo y empezará a recibir los paquetes.

Para lograr un balanceo de carga, se procede a configurar el protocolo de manera que ambos router estén activos y en Standby al mismo tiempo, y eso se logra con MHSRP (Multi Hot Standby Protocol). MHSRP es simplemente configurar más grupos dentro del protocolo HSRP con el objetivo de lograr que el router en Standby se convierta en un router activo. Lo que se hace es crear otra puerta de enlace virtual y hacer que sea la opción preferida del router en Standby, convirtiéndolo en active router y creando así un balanceo de los paquetes que ingresan a la red. Ahora bien, se crean 2 caminos (Por decirlo así) como se está enrutando por Vlan, se configuran las nuevas puertas de enlace para cada Vlan. Por ejemplo, el primer router en la Vlan 10, tendrá la puerta de enlace 172.16.10.1 en el Standby Group #1 con una prioridad de 150 y en el Standby Group #2, tendrá la puerta de enlace 172.16.10.2 con una prioridad por defecto (100) siendo para la Vlan 10 el active router del grupo #1 por tener la prioridad más alta y el Standby router para el grupo #2. Un paquete que ingrese por la Vlan 10 tendrá la opción de pasar por los 2 “Caminos” 172.16.10.1 ó 172.16.10.2. El camino que siga el paquete dependerá del protocolo de enrutamiento del dispositivo. Para esta parte se supondrá que existe un router que comunica al servidor de ingeniería. Se puede observar en la *Figura 24*.

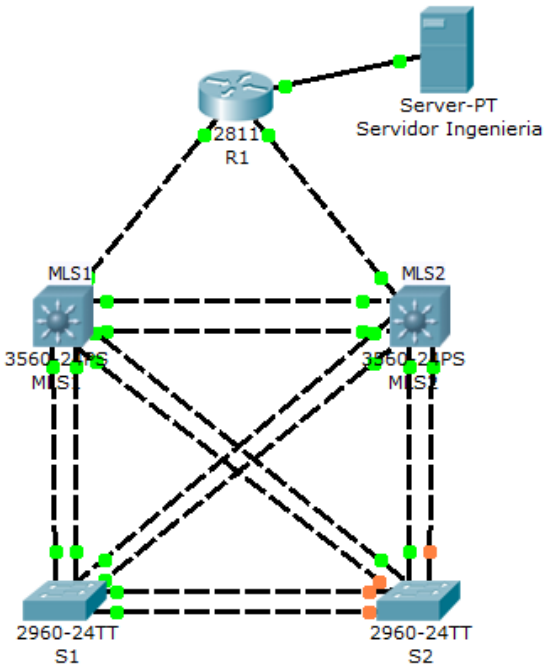


Figura 24. Topología para Balanceo de Carga con MHSRP

A continuación se observa cómo se configura MHSRP:

En MLS1:

```
interface Vlan1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.1                 //Puerta de enlace virtual para el grupo 1 de la Vlan 1
 standby 1 preempt
 standby 1 track Vlan1
 standby 2 ip 172.16.1.2                 //Puerta de enlace virtual para el grupo 2 de la Vlan 1
 standby 2 priority 150
 standby 2 preempt
 standby 2 track Vlan1
!                                        //es igual para el resto de las Vlan.
interface Vlan10
 ip address 172.16.10.3 255.255.255.0
 standby 1 ip 172.16.10.1
 standby 1 preempt
 standby 1 track Vlan10
 standby 2 ip 172.16.10.2
 standby 2 priority 150
 standby 2 preempt
 standby 2 track Vlan10
```

```
!
interface Vlan20
 ip address 172.16.20.3 255.255.255.0
 standby 1 ip 172.16.20.1
 standby 1 preempt
 standby 1 track Vlan20
 standby 2 ip 172.16.20.2
 standby 2 priority 150
 standby 2 preempt
 standby 2 track Vlan20
!
interface Vlan30
 ip address 172.16.30.3 255.255.255.0
 standby 1 ip 172.16.30.1
 standby 1 preempt
 standby 1 track Vlan30
 standby 2 ip 172.16.30.2
 standby 2 preempt
 standby 2 track Vlan30
!

interface Vlan40
 ip address 172.16.40.3 255.255.255.0
 standby 1 ip 172.16.40.1
 standby 1 preempt
 standby 1 track Vlan40
 standby 2 ip 172.16.40.2
 standby 2 preempt
 standby 2 track Vlan40
!
```

En MLS2:

```
interface Vlan1
 ip address 172.16.1.4 255.255.255.0
 standby 1 ip 172.16.1.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Vlan1
 standby 2 ip 172.16.1.2
 standby 2 preempt
 standby 2 track Vlan1
!
```

```
interface Vlan10
 ip address 172.16.10.4 255.255.255.0
 standby 1 ip 172.16.10.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Vlan10
 standby 2 ip 172.16.10.2
 standby 2 preempt
 standby 2 track Vlan10
!
interface Vlan20
 ip address 172.16.20.4 255.255.255.0
 standby 1 ip 172.16.20.1
 standby 1 priority 150
 standby 1 preempt
 standby 1 track Vlan20
 standby 2 ip 172.16.20.2
 standby 2 preempt
 standby 2 track Vlan20
!
interface Vlan30
 ip address 172.16.30.4 255.255.255.0
 standby 1 ip 172.16.30.1
 standby 1 preempt
 standby 1 track Vlan30
 standby 2 ip 172.16.30.2
 standby 2 preempt
 standby 2 track Vlan30
!
interface Vlan40
 ip address 172.16.40.4 255.255.255.0
 standby 1 ip 172.16.40.1
 standby 1 preempt
 standby 1 track Vlan40
 standby 2 ip 172.16.40.2
 standby 2 preempt
 standby 2 track Vlan40
```

Una vez realizado esto, el trafico de paquetes enviados por los usuarios pasarán algunos por MLS1 y otros MLS2 estadísticamente se tendrá un buen chance de tener una distribución equitativa del trafico a través de nuestra red.

El servidor tiene la dirección IP 172.16.40.100, se le hará un ping constante para verificar que están llegando los paquetes desde el host al servidor. Ver figura 25.

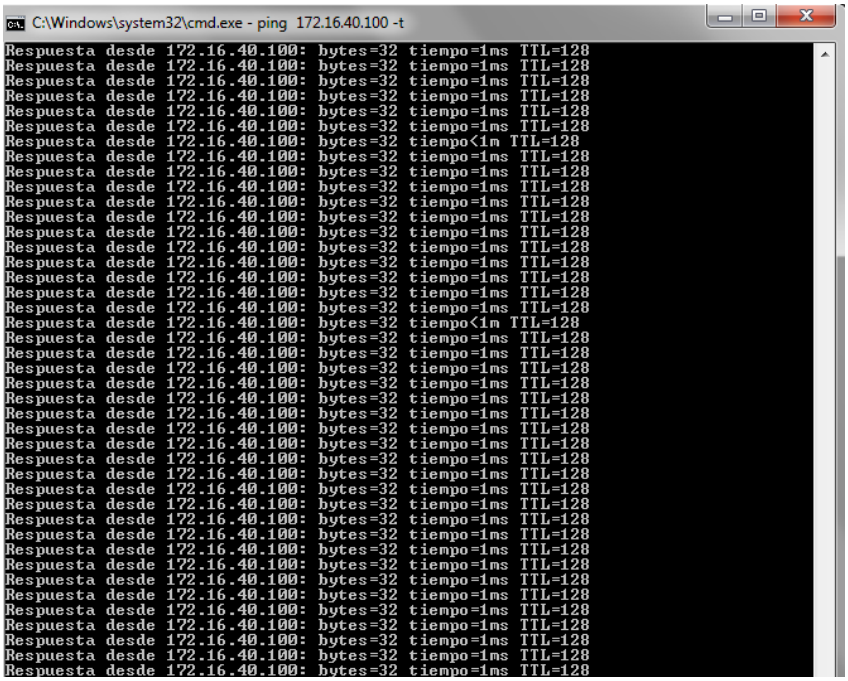


Figura 25. Ping Continuo al Servidor 172.16.40.100

Implícitamente ahí balanceo de carga en el flujo de paquetes que llegan al servidor, Como se dijo anteriormente los paquetes llegan por cualquiera de los 2 switches multicapa dependiendo del protocolo de enrutamiento y la prioridad que se tenga en el protocolo. De repente el Switch MLS1 falla, y como se observa en la *Figura 26*, la conexión no se ve afectada.

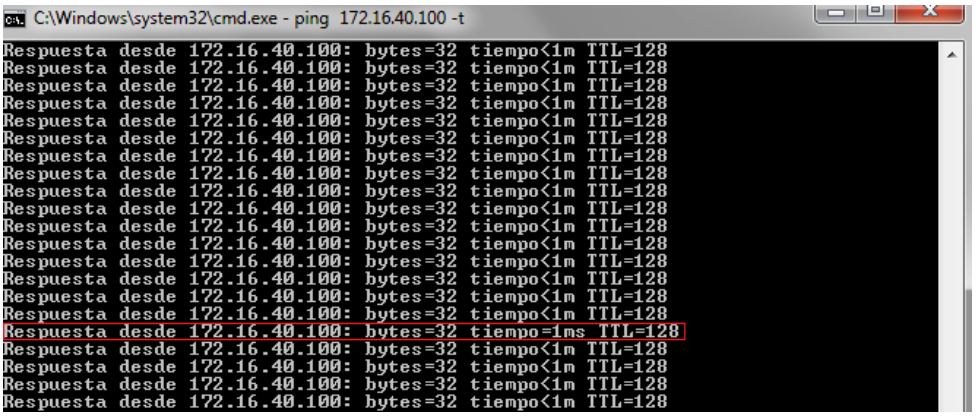


Figura 26. Ping Continuo después de una Falla en MLS1

En el switch MLS2, el grupo 2 de HSRP pasa de estado “Standby” a “Active” en las Vlan 1, 10, 20, 30. *Ver Figura 27*.

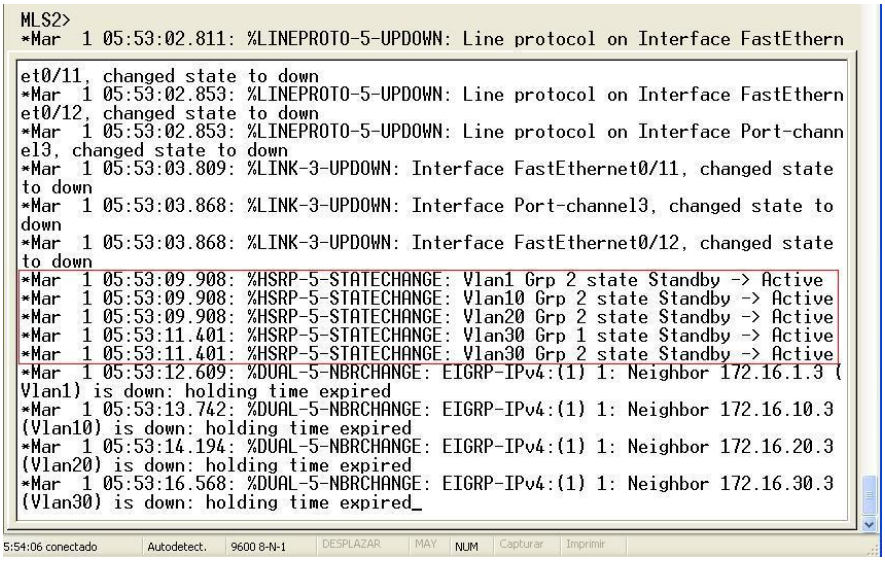


Figura 27. Estado de los Grupos HSRP en MLS2 cuando MLS1 Presenta una Falla

Una vez es solucionada la falla en MLS1, los grupos vuelven a cambiar su estado basándose en la prioridad que tiene cada uno. Se puede observar cuando MLS1 se vuelve operativo en la *Figura 28*.

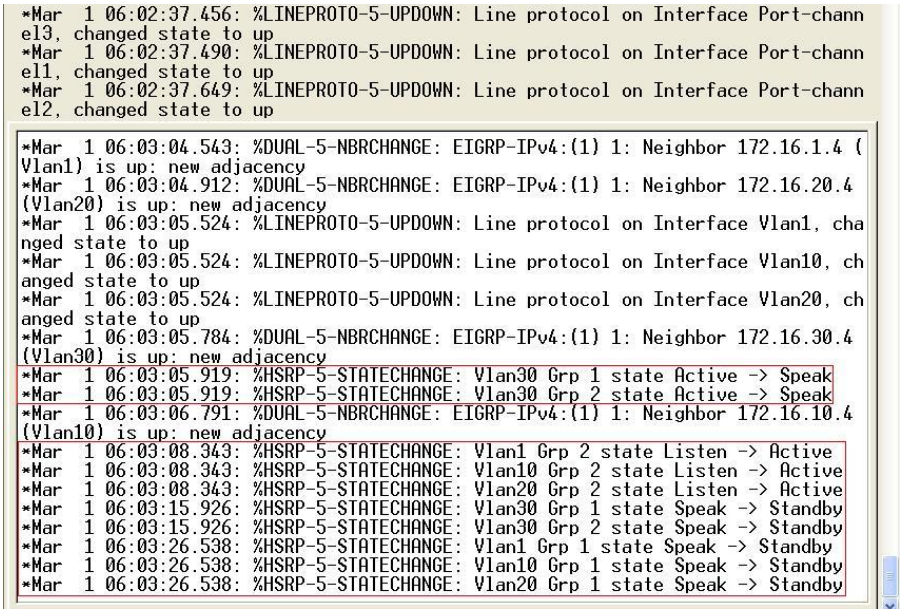


Figura 28. MLS1 Operando Nuevamente Después de la Falla

En MLS2 se modifican los estados de los grupos nuevamente. *Ver Figura 29*.

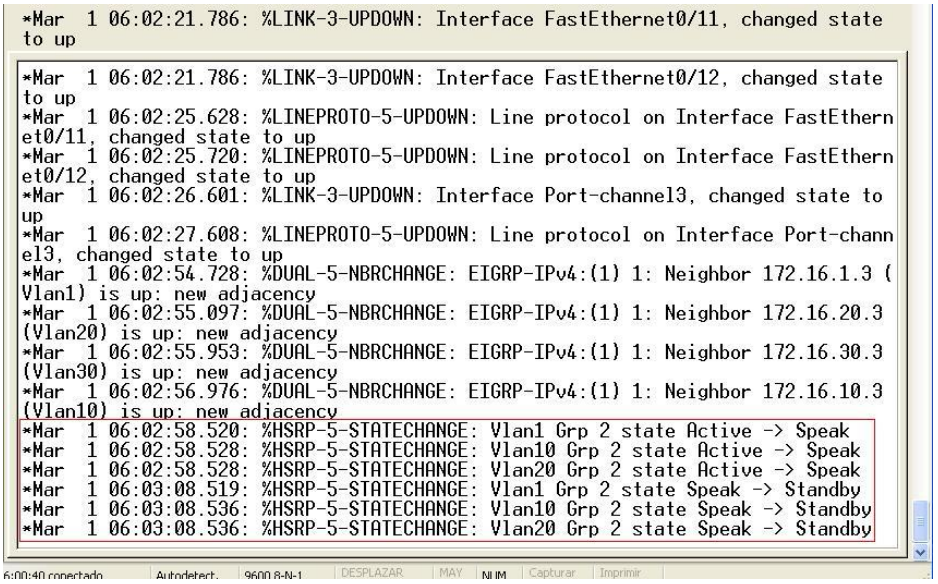


Figura 29. Estado de los Grupos en MLS2 cuando MLS1 se vuelve operativo

Como se pudo observar en las imágenes, no todas las Vlan cambian de estado, todo depende de la prioridad de las mismas. Para observar la configuración final, ejecutar el comando ***show running-config*** en cada uno de los dispositivos.

3.4.5 Conclusiones

Como se pudo observar en esta práctica es muy importante la redundancia en la red, pero en algunas ocasiones es muy costosa. Igualmente, el balanceo de carga es fundamental para evitar congestión de red y esta práctica es una de las tantas maneras de realizar balanceo en una red. Lo que se quería era sentar las bases para entender el verdadero significado del balanceo de carga. Queda a disposición del lector investigar más sobre el protocolo VRRP y GLBP. Adicionalmente, como se realiza el balanceo de carga por EIGRP, EtherChannel, entre otros.

CONCLUSIONES

Al analizar la actualidad de las comunicaciones, se nota que existe una necesidad, y es la d*e "Calidad y Velocidad"* en cuanto a los servicios de transmisión y flujo de datos de las redes. Larry Roberts, fundador del embrión de la red afirma que: *"El estado actual de Internet es "Insostenible y Peligroso".* Debido a que el internet está creciendo demasiado rápido para la infraestructura de red de hoy día y se observa en los malos servicios que ofrecen los proveedores del servicio de internet.

Cada vez son más los usuarios, clientes, empresas, que se quejan porque no se logra llegar a un servicio óptimo como se espera que suceda con tanta evolución tecnológica que existe actualmente; desde este enfoque, la infraestructura de redes actual implementada posee muchas fallas, una de ellas es la de no soportar la cantidad de usuarios nuevos que aparecen día a día en la red y esto ocasiona muchas caídas en los distintos servicios ofrecidos, además de tiempos de respuesta muy largos, y velocidad de transferencia ineficiente.

En este documento se pudo observar cómo es posible resolver la mayoría de las fallas que comúnmente se tienen dentro de un diseño de red gracias a las bondades que nos ofrecen los switches multicapa. Esta es la actualidad de los dispositivos de enrutamiento lo cual genera beneficios en cuanto a costos de hardware, eficiencia de red, escalabilidad, tiempo de configuración e incluso disponibilidad del servicio hasta de un 99.99%.

REFERENCIAS BIBLIOGRAFICAS

[1] *Enrutadores Inalámbricos* [en línea]. Subido por Katherine de Peña Davis. <http://www.monografias.com/trabajos72/enrutadores-inalambricos/enrutadores-inalambricos2.shtml> [Consulta: 2 mayo 2011].

[2] Larry L. Paterson and Bruce S. Davie (2007). Computers Networks, A System Approach. 4th Edition (168-170), EE.UU: San Francisco

[3] *Clasificación de los Switches* [en línea]. Info-IP.net <http://www.info-ip.net/dispositivos-ip/Clasificacion-de-los-Switches.php> [Consulta: 2 mayo 2011].

[4] McGraw-Hill Interamericana de España, SL. Ciclos Formativos Informática. Archivos. Unidad 9. Recurso 1. Configuracion de Switch-Router. Disponible en: http://www.mhe.es/cf/ciclos_informatica/844819974X/archivos/unidad9_recurso1.pdf

[5] "Multi-Layer Switching". Cisco Systems. Consultado el 24 Julio de 2011. Disponible en: http://www.cisco.com/en/US/tech/tk389/tk815/tk850/tsd_technology_support_sub-protocol_home.html

[6] TECNOLOGIA INNOVADORA. Ing. Marc Anthony. Unidad V – Switches Multicapa. Por Marc2233. Consultado el 24 Julio de 2011 en: http://marc22331.wordpress.com/unidad-v-switches-multicapa/

[7] REDES CONVERGENTES – Antología. Universidad Tecnológica de Izúcar de Matamoros. Maestro. Sergio Valera Orea. 22 Abril de 2010.
Consultado el 18 Agosto de 2011 en:
http://www.utim.edu.mx/~svalero/docs/Antologia%20Redes%20Convergentes.pdf

[8] CCNP SWITCH 642-813 Guia Oficial de Certificacion (Parte II – Capitulo 2.2 Multilayer Switch Operation)

[9] CCNA Semestre 3. Spanning Tree Protocol. Disponible en:
http://www.ciscoredes.com/ccna3/101-stp-spanning-tree-protocol.html

[10] Curriculum Cisco CCNP3 BCMSN_v50. Capitulo 3. Spanning Tree Protocol. Disponible en la Cisco Networking Academy.
http://www.cisco.com/web/learning/netacad/index.html