UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

Facultad de Educación Técnica para el Desarrollo

TESIS DE GRADO

Previo a la obtención del título:

Ingeniero en Telecomunicaciones

con Mención en Gestión Empresarial

TEMA:

Estudio de la factibilidad de un *BACKBONE MPLS* para brindar servicio de *VPN*, para acceder a un *FILE SERVER* desde un punto remoto.

REALIZADO POR:

Leyla Esther Matías Rodríguez

Manuel Eduardo Millán Rodríguez

DIRECTOR:

Ing. Efraín Vélez Tacuri

Guayaquil – Ecuador

2009 - 2010

TESIS DE GRADO

TEMA:

Estudio de la factibilidad de un *BACKBONE MPLS* para brindar servicio de *VPN*, para acceder a un *FILE SERVER* desde un punto remoto.

Presentada a la Facultad de Educación Técnica para el Desarrollo,

Carrera de Ingeniería en Telecomunicaciones de la

Universidad Católica de Santiago de Guayaquil.

REALIZADO POR:

Leyla Esther Matías Rodríguez

Manuel Eduardo Millán Rodríguez

Para dar cumplimiento con uno de los requisitos para optar por el Título de:

Ingeniero en Telecomunicaciones con Mención en Gestión Empresarial

_____	_____
Ing. Héctor Cedeño	Ing. Pedro Tutiven
Decano	Director de Carrera

_____

Ing. Efraín Vélez

Director de Tesis

DEDICATORIA

Durante la niñez, mi madre me brindo todo su amor y sembró en mí la semilla de la honestidad y el respeto. Por otro lado mi padre me demostró que con sencillez y esfuerzo todo se puede alcanzar.

Dedico este título al Sr. Homero Manuel Millán Rosero y a la Sra. Flor María Rodríguez Caivinagua y a mi querido hermano Jonathan Daniel Millán Rodríguez, en agradecimiento ha su apoyo moral y espiritual que me brindaron en cada ciclo de mi vida. Ellos son los pilares de mi existencia y la razón que me incentiva a mejorar cada día.

A Mama Miche y a Taita José que me enseñaron amar la creación del Señor, Doña María y a la memoria del abuelo Olmedo ejemplo de lucha incansable. Tío Orlando, tía Katty, tía Adela, Dalton ustedes me ayudaron durante diferentes etapas como estudiante, mil gracias.

Carol mi amor, colocaste tu granito de arena. Me incentivaste a mejorar por el bien de los dos, por nuestro futuro.

Manuel Eduardo Millán Rodríguez

Una vez escuche que cada uno de nosotros fuimos alguna vez un pensamiento de Dios, el hecho está en que no sólo nos quedamos en su mente si no en su corazón por algo él nos creo, y enseñó que a su lado no existe imposibles, doy Gracias a “Papito Dios” como le digo siempre, porque ha sido la roca en la que edifiqué mi vida, mi refugio en tiempo de pruebas, y mi amigo eterno en todo momento.

Gracias a mi mamita Ruth y a mi papito Wilson por enseñarme que un papá no es el que está pendiente de tus calificaciones en todo tiempo, si no es aquel que lo entrega todo porque es conciente de que sus hijos pueden lograr lo que se proponen.

Dedico este logro a mis abuelitos por que se que va a ser una alegría muy grande para ellos que su nieta sea una de las primeras ingenieras de su descendencia, a mis hermanos Josué y Chochito, a mis tías Eli, Chelita, Jovita, Inés por su preocupación y apoyo ya que son como mis otras mamás a mis tíos. A mis primas y primos los amo mucho.

Gracias a los amigos que se portaron como hermanos cada vez que los necesité, se que son pocos pero los quiero mucho, Roberta, Juan Carlos, Katherine, Dulce, Susana, Sandrita, Sarita y el Guado.

Leyla Esther Matías Rodríguez

PRÓLOGO

El desarrollo de este tema de investigación se fundamenta en la necesidad de comprender el crecimiento y la convergencia de las redes IP con las infraestructuras heredadas. El aumento exponencial del Internet, así como la demanda acelerada de nuevos y más sofisticados servicios, propone cambios tecnológicos avanzados respecto a las prácticas habituales que se desarrollaron a mitad de los años 90. MPLS (por sus siglas en inglés Multiprotocol Label Switching) surge como solución para satisfacer las necesidades de transmitir grandes volúmenes de información sobre una arquitectura que soporta diferentes protocolos de transporte. En la actualidad las instituciones académicas, empresas privadas o gubernamentales cuentan con agencias o sucursales para expandir su cobertura y ofrecer sus servicios, provocando la necesidad de comunicar las agencias con la matriz a través de enlaces dedicados pero con un alto valor monetario. Virtual Private Network es una alternativa que utiliza una red pública o internet para comunicar dos puntos ofreciendo los mismos servicios que un enlace dedicado.

El objetivo que se desea alcanzar al finalizar esta investigación es simular una Backbone MPLS y configurar una Red Privada Virtual, además analizar los mecanismos utilizados para encaminar los datos desde su origen hacia su destino y conocer las políticas de seguridad para garantizar la autenticación de los paquetes que viajan a través del túnel VPN.

Para lograr el alcance del objetivo planteado es necesario cumplir con los siguientes requisitos:

- **Analizar los mecanismos que utiliza MPLS para conmutar y encaminar el paquete IP.**

- **Configurar una VPN sobre el Backbone MPLS, además de entender la encriptación de seguridad.**

- **Explicar el funcionamiento del simulador de IOS de Cisco Dynamips, que se utiliza para el diseño de nuestra red.**

Al finalizar nuestro tema de tesis se demostrará a la comunidad estudiantil, catedráticos de la Facultad Técnica para el Desarrollo Humano y público en general una nueva alternativa de transporte de datos (sean estas voz, información o video), que permitirá reemplazar los métodos tradicionales de enlaces WAN o MAN; por otra parte comprender los motivos por el cual los diseñadores de red implementen la arquitectura MPLS.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

1.1 PRE MPLS

En la última década, el número de usuarios con acceso a internet ha crecido descontroladamente. Las empresas han desarrollado aplicaciones cada vez más complejas y con mayor consumo de ancho de banda, dichas aplicaciones han captado la atención de los usuarios provocando la transmisión de grandes volúmenes de datos. La infraestructura existente, para ese entonces ATM, necesitaba transportar cualquier paquete basado en IP, poco a poco aparecieron soluciones momentáneas para la convergencia IPoATM. Sin embargo las limitaciones de ATM provocaron que un grupo de investigadores de IBM, Cisco y Ascend recopilaran las mejores características de ATM y de las soluciones para IPoATM con el fin de creer una nueva arquitectura de transporte llamada *Multiprotocol Label Switching MPLS*.

1.1.1 PROTOCOLO DE INTERNET IP

El Protocolo Internet está diseñado para sistemas interconectados de redes de ordenadores por intercambio de paquetes. Es un sistema no orientado a conexión, trabaja en la capa de red del modelo OSI, proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet también se encarga, si es necesario, de la fragmentación y el re-ensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

Las principales características de este protocolo son:

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.
- Tamaño máximo del paquete de 65635 bytes.

ESTRUCTURA DEL PAQUETE IP

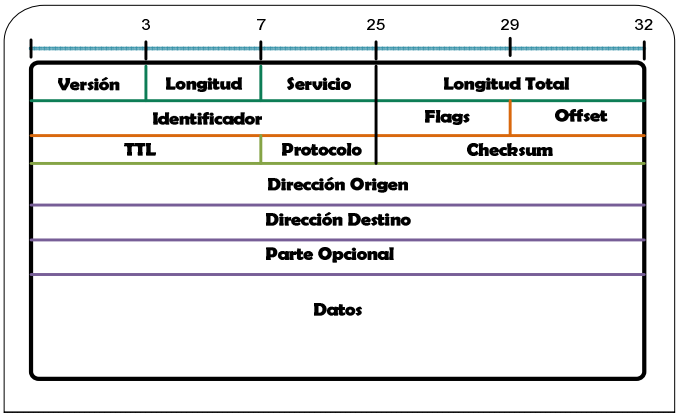


Fig. 1.1 Trama del Paquete IP

DIRECCIONES IP: Cada interfaz de red de cada host o router en una red IP se identifica mediante, al menos una, dirección única de 32 bits. Las direcciones IP se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección. Si un nodo dispone de varias interfaces físicas, como suele ser comúnmente el caso de un router, cada una de ellas deberá tener necesariamente una dirección IP distinta si se desea que sea accesible de forma diferenciada para este protocolo. Es posible también y en algunas situaciones resulta útil, definir varias direcciones IP asociadas a una misma interfaz física.

Las direcciones IP tienen una estructura jerárquica. Una parte de la dirección es denominada dirección de red, y la otra dirección de host dentro de la red. Cuando un router recibe un paquete por alguna de sus interfaces, compara la parte de red de la dirección con las entradas contenidas en sus tablas y reenvía el paquete por la interfaz correspondiente, situación denominada ruteo.

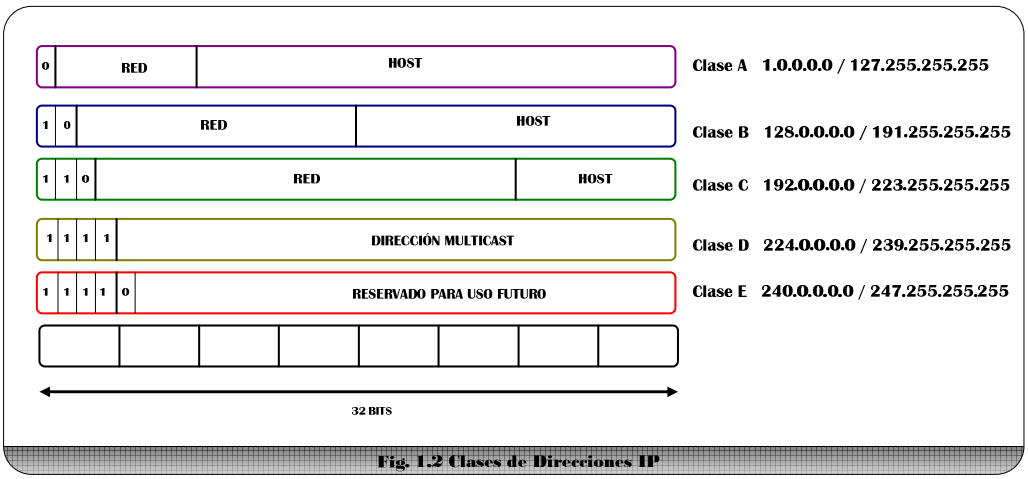


Fig. 1.2 Clases de Direcciones IP

Las clases de redes IP son:

- Una red de clase A se caracteriza por tener en 0 el primer bit de dirección. El campo red ocupa, además del primer bit que siempre está en 0, los 7 bits siguientes y el campo host los últimos 24. De aquí se tiene que puede haber hasta 128 redes (7 bits para manejar) clase A, con 16777216 direcciones o nodos cada una (24 bits para manejar).

- Una red de clase B tiene el primer bit en 1 y el segundo en 0. El campo red ocupa, además de los dos primeros bits que siempre están en 10, los 14 bits

siguientes, y el campo host los 16 últimos. Puede haber entonces 16384 redes clase B (14 bits para manejar) con 65536 direcciones o cada una (16 bits para manejar).

- Una red clase C tiene los primeros tres bits en 110. El campo red ocupa, además de los tres primeros bits que siempre están en 110, los siguientes 21 bits, y el campo host los 8 últimos. Entonces, puede haber hasta 2097152 redes (21 bits para manejar) clase C con 256 direcciones cada una (8 bits para manejar).

- Clase D - Utilizado para los multicast, la clase D es levemente diferente de las primeras tres clases. Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 0. Los otros 28 bits se utilizan para identificar el grupo de computadoras al que el mensaje del multicast esta dirigido. La clase D totaliza 1/16ava (268,435,456 o 228) de las direcciones disponibles del IP.

- Clase E - La clase E se utiliza para propósitos experimentales solamente. Como la clase D, es diferente de las primeras tres clases. Tiene un primer bit con valor de 1, segundo bit con valor de 1, tercer bit con valor de 1 y cuarto bit con valor de 1. Los otros 28 bits se utilizan para identificar el grupo de computadoras que el mensaje del multicast está dirigido. La clase E totaliza 1/16ava (268,435,456 o 228) de las direcciones disponibles del IP.

1.1.2 ASYNCHRONOUS TRANSFER MODE ATM

ATM es un estándar de la Unión Internacional de Telecomunicaciones, su funcionamiento se basa en el envío de celdas que puede soportar múltiples servicios, como voz, datos y videos. Las redes ATM son redes orientadas a conexión y asíncronas, es decir, los *time slot* son habilitados dependiendo de la necesidad para transferir información. ATM es una tecnología de conmutación de celdas y multiplexacción que combina los beneficios de conmutación de circuitos (garantiza una conexión constante) y paquetes (adecuado para tráfico intermitente).

La celda ATM es de tamaño fijo, 53 bytes. Los primeros 5 bytes contiene la cabecera y los 48 bytes restantes la carga (datos).

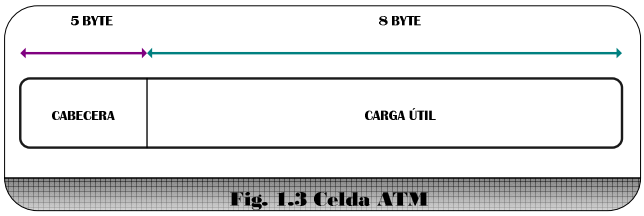


Fig. 1.3 Celda ATM

Las redes ATM soportan múltiples tipos de tráfico como: video, audio, Frame Relay, ip, etc. ATM Adaption Layer AAL permite adaptar los paquetes recibidos por la capa ATM a aquellos servicios que son requeridos por las capas más altas. AAL reciben paquetes de diferentes tipos y los encapsula en los 48 bytes de la celda ATM. Actualmente existen cinco tipos de AAL, con la finalidad que exista un AAL para cada tipo de datos. Los AAL más utilizados son AAL 1 y AAL 5.

AAL1: Se usa para transmitir tasas de bit constantes. Voz, videoconferencia, E1 o T1.

AAL 5: Permite transmitir paquetes IP.

IP over ATM: En los años 90 IP se convirtió en la base para ofrecer servicios a través del internet, esto produjo que los ISP busquen las herramientas necesarias para fusionar el trafico IP sobre las redes ATM, ya existentes.

Por su naturaleza IP se encuentra en la capa 3 del modelo OSI, para enviar un paquete IP es necesario el ruteo. En comparación de ATM que trabaja en la capa 2 del modelo OSI, su funcionamiento se basa en el intercambio de etiquetas o *switching*. IPoATM permitió que estas dos tecnologías puedan coexistir sobre una misma red, evitando que se traslapen sus funciones características. Aparecieron varios métodos para permitir que IP se integre a la red ATM, a continuación se menciona algunos de ellos.

Cell Switch Routers ó CSR: Permite conectar una red ATM con una red NO ATM, es muy parecido a *Tag Swiching*

Lan emulation: Fue creado por ATM FORUM para definir los parámetros que permitan integrar las redes ATM con los sistemas LAN.

MPOA: Se trata de una solución de *routing* para la capa de red que integran los protocolos existentes y los estándares para dar funciones de *routing* sobre las redes ATM. MPOA identifica flujos de datos y los mapea directamente en canales virtuales ATM.

Tag switching: Emplea etiquetas para identificar los flujos de datos. Posee funciones de envío y control. El envío se lleva a cabo usando técnicas de intercambio de etiquetas. El control se encarga de distribuirlas por la red.

Las empresas tecnológicas como IBM, Cisco y Ascend se percataron que IPoATM poseía muchas limitaciones, como la falta de circuitos virtuales para soportar el trafico IP, altos costos al momento de administrar dos redes diferentes. Bajo estas circunstancias realizaron investigaciones para asimilar y acoplar las mejores características de las soluciones ATM como Tag Switching y MPOA, surge una solución (MPLS) con posibilidades de convertirse en un estándar, avalado por la IEEE.

1.2 FUNDAMENTOS DE MPLS

Multiprotocol Label Switching es una tecnología de red efectiva, rápida y altamente escalable, utiliza la conmutación de etiquetas para enviar paquetes de datos a través de la red. Soporta cualquier tipo de tráfico como: ATM, Frame Relay o IP. Además inserta una etiqueta sobre el paquete para identificar la ruta y de esta manera el paquete llegue a su destino. La cabecera MPLS trabaja entre la capa de enlace de datos y la capa de red del modelo OSI.

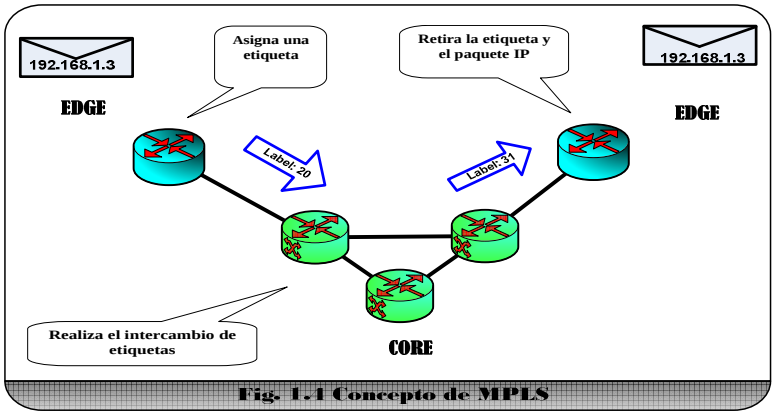


Fig. 1.1 Concepto de MPLS

1.2.1 BENEFICIOS DE UNA RED MPLS

A continuación se detalla los beneficios que posee una red MPLS:

- Capacidad de Transportar cualquier tipo de información
- Utilización de la conmutación por paquetes.
- Mayor rendimiento de IP sobre ATM
- Reestructuración del uso BGP
- Proporciona servicios de VPN
- Optimización de Flujo de Trafico
- Ingeniería de Trafico
- Calidad de servicio QoS

Capacidad de transportar cualquier tipo de información: **L**a red MPLS es capaz de transportar cualquier tipo de protocolo, por ejemplo IPv4, IPv6, DHCL, PPP y cualquier tecnología de capa 2. Cuando un paquete ingresa a una red MPLS no se analiza la procedencia, simplemente se inserta una etiqueta para ser transportado por la red.

Conmutación de paquetes: MPLS es una tecnología de conmutación creada para acelerar el tráfico en las redes y hacerlo más sencillo de gestionar. MPLS configura un camino específico para una secuencia de paquetes, identificados por una etiqueta insertada en cada paquete. De esa forma, el router realiza el envío del paquete conmutando etiquetas y disminuye la latencia al eliminar los procesos de análisis de capa de red.

Mayor rendimiento de IP sobre ATM: Durante la década de los 90´s varia empresas se dedicaron a buscar alternativas para transportar paquetes IP sobre las redes ATM, sin embargo no fueron soluciones permanentes. MPLS surge como una solución que utiliza las características principales implementadas anteriormente en IP sobre ATM. MPLS se transformó en una solución viable para transportar paquetes IP.

Reestructuración del uso BGP: BGP es un protocolo EGP, permite intercambiar información entre sistemas autónomos. Las redes tradicionales necesitan habilitar un protocolo externo sobre cada uno de sus ruteadores para que interactúen con diferentes sistemas autónomos, el núcleo de MPLS realiza el envío de paquetes a través de la conmutación de etiquetas, evitando así, la necesidad de configurar BGP, Por otra parte los router que se encuentran ubicados al borde de la red MPLS necesitan un protocolo que les permita comunicarse con otras redes.

1.2.2 ARQUITECTURA FÍSICA DE LA RED MPLS

Una red es un conjunto de elementos interconectados entre sí, donde cada elemento cumple una función específica y está ubicado en un lugar estratégico dentro de la red.

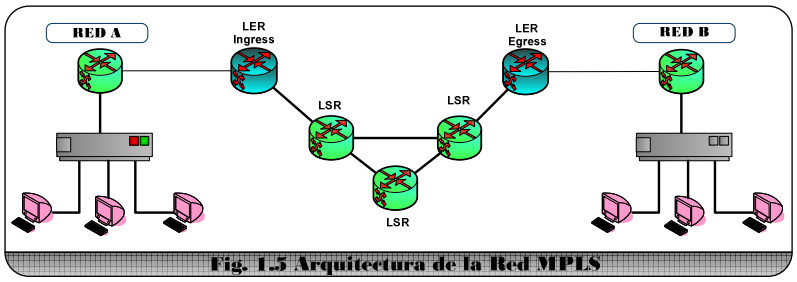


Fig. 1.5 Arquitectura de la Red MPLS

La red MPLS está conformada de ruteadores o Label Switch Router que tienen la capacidad de insertar, conmutar y extraer las etiquetas MPLS.

Los elementos de la red MPLS son:

Edge-LSR ó LER: Son ruteadores que se encuentran al borde de la red, su función principal es adaptar una red no MPLS (IP, ATM, Frame Relay), al *core* MPLS. LER realiza sus funciones basándose en la dirección IP (Capa de Red) para poder asignar una etiqueta al paquete.

Se lo puede clasificar de la siguiente manera:

- Ingress Edge-LSR: Es un router que tiene la capacidad de colocar una etiqueta al paquete que ingresa a la red MPLS.

- Egress Edge-LSR: Realiza la función inversa del Ingress Edge-LSR, se encarga de retirar la etiquete MPLS para enviar el paquete a su destino.

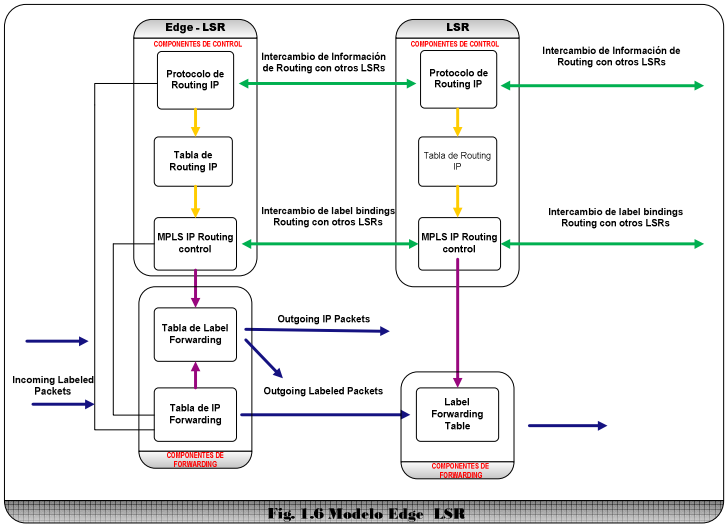


Fig. 1.6 Modelo Edge LSR

<u>Core-LSR o LSR:</u> Son ruteadores con gran velocidad de procesamiento, se encuentran en el núcleo de la red MPLS. Los LSR no realizan ninguna verificación a nivel de Capa de Red, su función es analizar la etiqueta del paquete recibido, retirar e inserta la etiqueta del próximo salto.

1.2.3 ARQUITECTURA LÓGICA DE LA RED MPLS

Todos los sistemas de comunicaciones necesitan establecer procesos para que los dispositivos se puedan comunicar. Un protocolo es una descripción formal de un conjunto de reglas y convenciones que rigen para todos los dispositivos de una red. La red MPLS no es la excepción, los LER necesitan establecer comunicación con sus vecinos para distribuir las etiquetas este proceso se lo realiza mediante protocolos de distribución.

Estructura de la cabecera MPLS: La cabecera MPLS tiene un tamaño total de 32 bits y está conformada por varios campos. La figura muestra los campos que posee la cabecera MPLS.

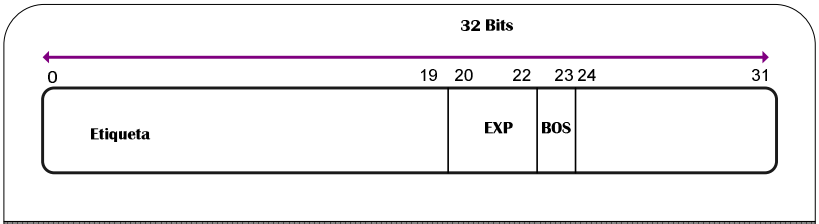


Fig. 1.7 Estructura de la cabecera MPLS

Etiqueta: 20 bits. Indica el valor de la etiqueta. Puede tener valore entre 0 hasta 2^{20} -1 ó 1`048,575. Los primeros 16 valores son de uso reservados.

Experimental: 3 bits. No está definido por la R.F.C., Cisco lo utiliza para definir la clase de servicio (CoS).

BOS: 1 bit. MPLS permite insertar múltiples etiquetas. El bit de pila permite ordenar las etiquetas de forma jerárquica. Si BOS vale 0 indica leer a la siguiente etiqueta, si vale 1 indica que es la ultima etiqueta. Este campo guarda relación con *Label Stacking* que se menciona mas adelante.

TTL: 8 bits. Especifica los saltos que puede dar un paquete antes de ser descartado.

1.2.4 EMPLEO DE ETIQUETAS

MPLS emplea etiquetas para definir la ruta por donde debe viajar un paquete. Se utiliza para señalar uno o diferentes FECs en diferentes enrutadores, cada etiqueta es encapsulada dentro de un encabezado de capa 2 junto con el paquete.

1.2.4.1 ETIQUETA

Es un identificador corto, de longitud fija que ocupa los 20 primeros bits de la cabecera MPLS, con significado local en cada interfaz empleada para identificar un FEC y el trayecto que el paquete debe cruzar.

1.2.4.2 OPERACIONES DE LAS ETIQUETAS

Label Swap: Operación de cambio del valor de la etiqueta en cada nodo

Label Merging: Cambio de varias etiquetas por una única, que identifican al mismo FEC

1.2.4.3 RESERVACIÓN DE ETIQUETAS

Los LSR no pueden usar etiquetas con valores 0 hasta 15 para enviar un paquete, la razón es porque dicho rango de etiquetas son reservadas para usos específicos. A continuación analizaremos sus usos:

- **Etiqueta 0 IPv4 y 2 IPv6 o Etiqueta explicita inválida**: Como se indica más adelante, la etiqueta 3 sirve para indicar el LSR del penúltimo salto que debe entregar el paquete IP al LSR de salida. Este proceso produce que el

LSR del penúltimo salto retire la cabecera MPLS y con ella se elimina el campo EXP. El campo EXP se lo utiliza para definir calidad de servicio. Para evitar que se elimine el campo EXP se habilita la etiqueta 0.

- **Etiqueta 1 o Etiqueta de alarma enrutable**: Esta etiqueta puede ubicarse en cualquier lugar de la pila de etiquetas, menos en el *bottom*. Cuando el enrutador detecta un paquete etiquetado con valor de uno, alerta al LSR para que realice una búsqueda minuciosa del próximo salto.

- **Etiqueta 3 o Etiqueta implícita inválida:** Indica al LSR del penúltimo salto, que debe entregar al *Egress* LSR el paquete sin etiquetar. De esta forma el *Egres*s LSR evita realizar la búsqueda en su base de datos, mejorando el desempeño de la red.

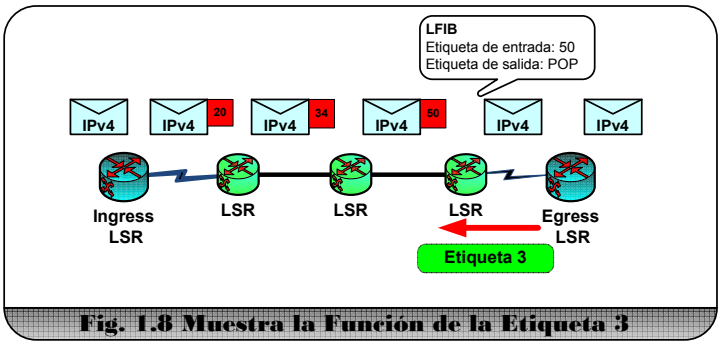


Fig. 1.8 Muestra la Función de la Etiqueta 3

- **Etiqueta 14 o etiqueta de operación y mantenimiento**: Esta etiqueta es usada para detectar fallas o para monitorear.

1.2.4.4 PILA DE ETIQUETA

Los enrutadores que se encuentran en la red MPLS, necesitan más de una etiqueta para enviar el paquete a través de la red hasta llegar a su destino, formando así un grupo de etiquetas a las que se conoce como pila de etiquetas. La primera etiqueta que se encuentra en la pila se llama *Top Label* y la última *Botton Label*, en medio de la primera y última etiqueta pueden existir varias etiquetas.

Usualmente se asigna una etiqueta por paquete, a continuación se indican diferentes escenarios donde escenario el apilamiento de etiquetas.

- MPLS VPN: Se necesita una etiqueta para identificar la VPN y otra para indicar la ruta que debe seguir el paquete.

- MPLS TE: Ingeniería de tráfico utiliza una etiqueta para identificar el túnel y otra para indicar el fundamento de LSP.

- MPLS VPN combinado con MPLS TE: Tres o más etiquetas son empleadas para identificar la VPN, túnel y el fundamento de LSP.

Cada nodo retira una etiqueta, de esta forma disminuye el tamaño de la pila y el campo BOS =0 indica que existe otra etiqueta, si vale 1 es la última etiqueta.

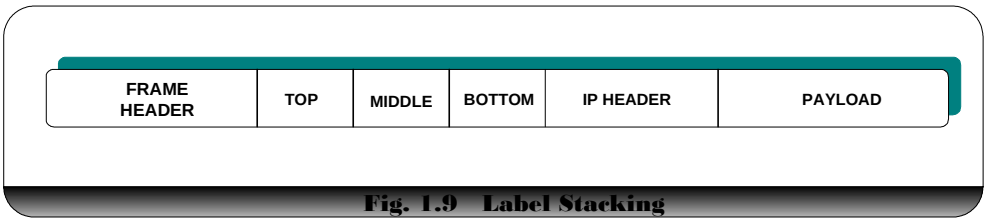


Fig. 1.9 Label Stacking

1.2.5 FORWARDING EQUIVALENCE CLASS (FEC)

Un FEC está conformado por un conjunto de paquetes con similares o idénticas características que se envía a través de la misma ruta (LSP) pero cada paquete puede tener diferentes destinos. Cuando un paquete es recibido por el LER lo asocia a un FEC, cada FEC es relacionado con una etiqueta para identificar el próximo salto.

Por ejemplo: Un paquete IP con dirección de destino 201.20.3.4 es recibido por un LER, si es la primera vez que se recibe dicho paquete se lo asocia a un FEC caso contrario se realiza una búsqueda para identificar el FEC al que corresponde, se inserta al paquete la etiqueta relacionada al FEC y se envía el paquete a su próximo salto.

Dest. Address	Dest. Port	FEC	Nest Hop	Label	Instructions
201.20.3.4	80	B	X.X.X.X	65	PUSH
201.20.4.5	443	S	Y.Y.Y.Y	18	PUSH
201.12.8.1	25	IP	Z.Z.Z.Z	-	NATIVE IP

TABLA 1.1 Direcciones del FEC

1.2.6 LABEL SWITCHED PATH (LSP)

Un LSP es una secuencia de LSR's que conmuta un paquete etiquetado a través de una red MPLS o parte de ella. Se lo puede definir como un circuito virtual unidireccional por donde viajan todos los paquetes pertenecientes a una misma FEC. Por ejemplo: En una red MPLS la ruta creada por el LSP para enviar un paquete desde un punto A hacia el punto B, puede ser diferente a la que se cree cuando se envíe un paquete desde el punto B hacia el punto A.

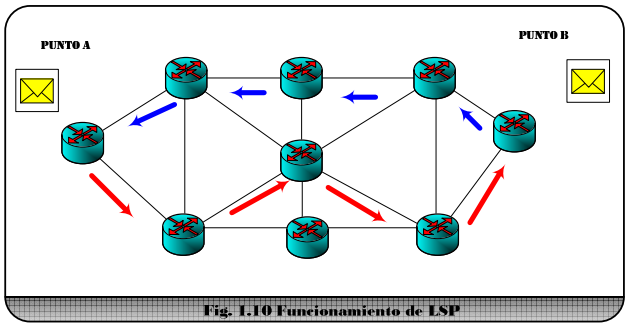


Fig. 1.10 Funcionamiento de LSP

Tipos de LSP: MPLS provee dos opciones para establecer un LSP.

Ruteo Hop by Hop (Salto a Salto): Cada LSR selecciona independientemente el siguiente salto para una FEC dada. Este método es similar al usado en redes IP. El LSR usa cualquiera de los protocolos de ruteo disponibles, como OSPF.

Ruteo Explicito: El LER de ingreso especifica la lista de nodos por la cual viaja la trayectoria explícita. La ruta explícita puede contener solamente la especificación de una parte del camino dentro del dominio MPLS. Si se define la entrada hasta la salida del dominio no se necesita ningún algoritmo de enrutamiento, y si solo

incluye una parte del camino, el resto se obtiene con ayuda de los algoritmos de enrutamiento. Sin embargo, la ruta especificada puede ser no óptima.

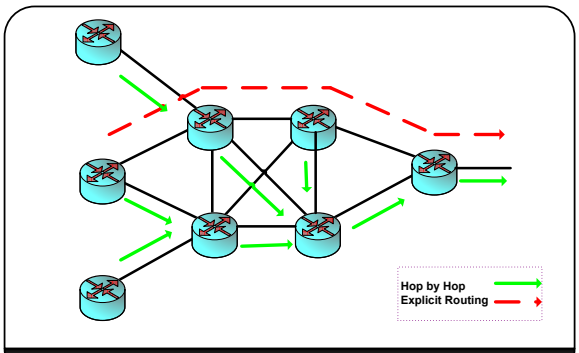


Fig. 1.11 Tipos de LSP

1.2.7 LABEL INFORMATION BASE (LIB)

Cada LSR vincula una etiqueta a un prefijo IP, para luego distribuirlo a sus vecinos. Los vecinos almacenan esta información en una base especial llamada base de información de etiquetas (LIB).

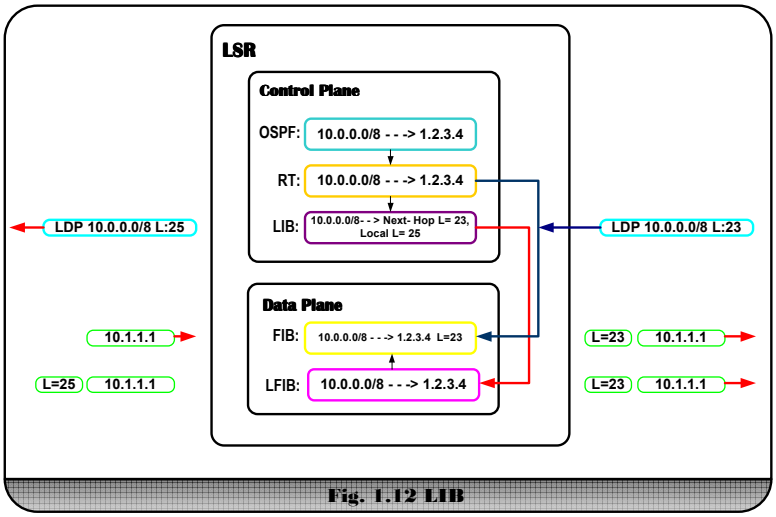


Fig. 1.12 LIB

1.2.8 FORWARDING INFORMATION BASE (FIB)

Se puede definir a FIB como una base de enrutamiento. Es decir, los protocolos IGP crean una base de enrutamiento IP que es usada para construir la FIB. Cuando existe algún cambio en la red, la tabla de enrutamiento se actualiza junto a la FIB. El paquete enviado es etiquetado, si el próximo salto dispone una etiqueta para la dirección IP destino.

1.2.9 LABEL FORWARDING INFORMATION BASE (LFIB)

LFIB es una base de datos exclusivamente para almacenar etiquetas. Permite el intercambio de etiquetas en los LSR del núcleo para conmutar el paquete basado en la etiqueta que posee.

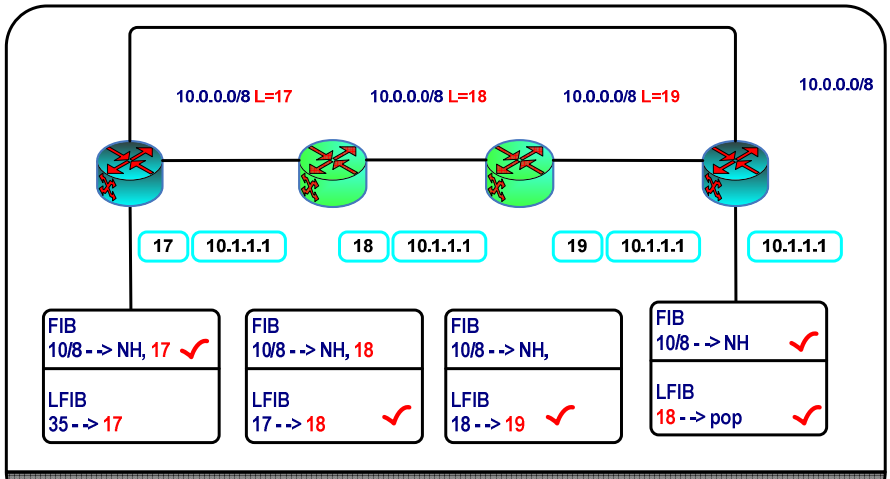


Fig. 1.13 Funcionamiento de FIB y LFIB

1.3 DISTRIBUCIÓN DE ETIQUETAS

Los LSR necesitan publicar las LFIB o tabla de etiquetamiento, a sus vecinos, con el objetivo que todos los nodos involucrados etiqueten correctamente los paquetes pertenecientes a un FEC, para realizar las publicaciones de etiquetas, MPLS utiliza diferentes modos y protocolos de distribución de etiquetas.

1.3.1 MODOS DE DISTRIBUCIÓN DE ETIQUETAS

Un LSR puede usar diferentes modos para intercambiar etiquetas con otros LSR. Existen tres modos para la distribución de etiquetas:

- Label Distribution Mode
- Label Retention Mode
- LSP Control Mode

1.3.1.1 LABEL DISTRIBUTION MODE

Existes dos formas para distribuir las etiquetas:

- Downstream-on-Demand (DoD)
- Downstream Unsolicited (UD)

Downstream-on-Demand: En la red MPLS, los LSR solicitan de forma específica, a su vecino de próximo salto, una etiqueta para un determinado FEC.

Es decir, un LSR upstream realiza peticiones a un LSR downstream, este a su vez realiza la asignación de etiquetas para un FEC.

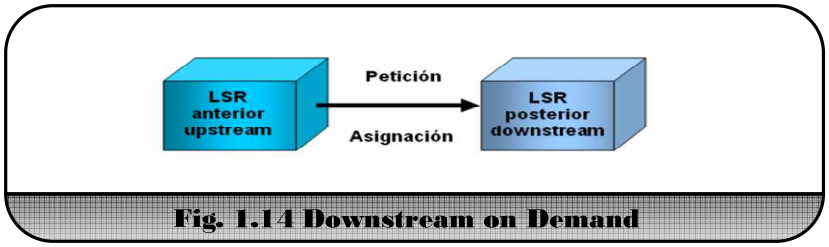


Fig. 1.14 Downstream on Demand

Unsolicited Downstream: Los LSR río abajo asignan las etiquetas y las distribuyen a sus vecinos que se encuentran río arriba, sin que hayan realizado peticiones.

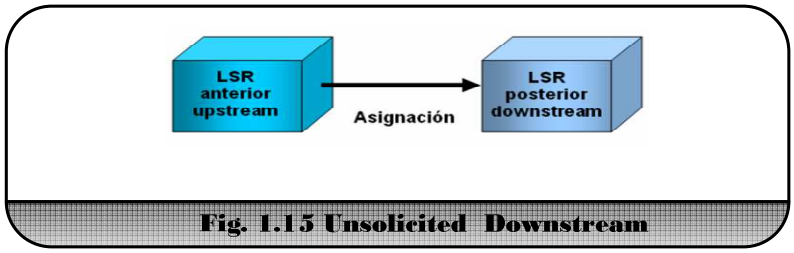


Fig. 1.15 Unsolicited Downstream

1.3.1.2 LABEL RETENTION MODE

Un LSR puede recibir información de asociaciones de etiquetas a FECs que no use. Por tanto, un LSR podrá guardar dicha información o descartarla. Los modos de retención de etiquetas especifican el comportamiento ante tal situación.

Existen dos modos de retención de etiquetas:

- Modo liberal de retención de etiquetas
- Modo conservador de retención de etiquetas

Modo liberal de retención de etiquetas: Una vez que el LSR ha recibido una asignación la mantiene indefinidamente. Su ventaja es que si se desea volver a establecer la relacione entre FEC y etiqueta no es necesario repetir el proceso de asignación. La desventaja es el alto consumo de etiquetas.

Modo conservador de retención de etiquetas: El LSR monitoriza la asignación y conoce cuando deja de estar activa, y al dejar de ser activa puede descartar esta asignación. Tiene la ventaja de que solo permanecen asignadas aquellas etiquetas que realmente están en uso. La desventaja es si establece nuevamente la relación entre FEC y etiqueta, es necesario repetir el procedimiento de asignación.

1.3.1.3 CONTROL DE DISTRIBUCIÓN DE ETIQUETAS

MPLS define dos modos para la distribución de etiquetas entre dos LSR adyacentes.

Control independiente: En este modo, un LSR reconoce una FEC en particular y toma la decisión de unir una etiqueta a la FEC independientemente de distribuir la unión a sus LSR pares.

Control ordenado: En este modo, el LER es responsable de la distribución de etiquetas.

1.3.2 PROTOCOLOS PARA LA DISTRIBUCIÓN DE ETIQUETAS

Considerando que se desea transmitir IPv4 sobre MPLS, el LSR debe tener la capacidad de soportar protocolos de enrutamiento interno, como OSPF, EIGRP o ISIS. Cuando el paquete IP ingresa al LER, realiza el proceso de búsqueda de la dirección IP destino en la tabla de enrutamiento para insertar la etiqueta correspondiente y enviar el paquete por la interface de salida. El LSR reciba el paquete etiquetado por el LER, retira la etiqueta anterior y coloca otra que representa al próximo salto. El LER que está conectado con la red destino, debe retirar la etiqueta y enrutar el paquete hacia su destino final.

Para realizar el proceso de envío del paquete IP a través de la red MPLS, es necesario algún mecanismo para permitir la comunicación entre los LSR. Los ruteadores no conocen el valor de la etiqueta de salida de un paquete etiquetado. Por esta razón los protocolos de distribución de etiquetas son necesarios.

Es posible realizar la distribución de etiquetas de dos formas:

- Extender la funcionalidad existente en los protocolos de enrutamientos
- Crear un nuevo protocolo dedicado al intercambio de etiquetas

Extender la funcionalidad existente en los protocolos de enrutamientos: Los protocolos de enrutamiento existentes deberían ser capaces de transportar etiquetas. La ventaja que tienen los protocolos de enrutamiento para transportar etiquetas es que tanto el enrutamiento como la distribución de etiquetas es síncrono, es decir no

es posible tener una etiqueta, si la dirección no existe o viceversa. Esto eliminaría la necesidad de desarrollar otro protocolo de enrutamiento para distribuir las etiquetas, pero las características que poseen los protocolos de enrutamiento vector distancia y estado de enlace restringe la posibilidad de utilizarlos para la distribución de etiquetas.

Ninguno de los IGP´s se ha modificado para transportar etiquetas. Sin embargo, BGP es un protocolo de enrutamiento que puede llevar prefijos y distribuir etiquetas al mismo tiempo. Sin embargo, BGP no es un IGP, es utilizado para transportar los prefijos externos. BGP se utilizar principalmente para la distribución en las etiquetas en redes MPLS-VPN.

Crear un nuevo protocolo dedicado al intercambio de etiquetas: La solución más óptima para la distribución de etiquetas fue la creación de protocolos de distribución. La ventaja de tener un protocolo único para la distribución de etiquetas es evitar el conflicto de sus funciones en relación al enrutamiento de prefijos IP. La desventaja es que los LSR deben ejecutar otro protocolo.

Existen varios protocolos de distribución.

- Tag Distribution Protocol (TDP)
- Label Distribution Protocol (LDP)
- Resource Reservation Protocol (RSVP)

1.3.2.1 TAG DISTRIBUTION PROTOCOL (TDP)

TDP es un protocolo de distribución de etiquetas desarrollado por CISCO, combina la flexibilidad y la funcionalidad que provee la capa de red, con la sencillez proporcionada por el intercambio de etiquetas. Los *tag* generados localmente en el router se intercambia con otros mediante el protocolo TDP. Este protocolo permite distribuir, requerir y actualizar la información de *tag*.

TDP es propiedad de CISCO, es decir, solo los router con marca CISCO lo podían ejecutar. La IETF desarrollo un protocolo estándar llamado *Label Distribution Protocol*. LDP y TDP son similares en la forma de operación, pero LDP posee más funcionalidad que TDP.

1.3.2.2 LABEL DISTRIBUTION PROTOCOL (LDP)

LDP está definido por la RFC 3036 como un protocolo que permite la distribución de etiquetas. LDP es un conjunto de procedimientos mediante los cuales un LSR informa a otros LSR´s del significado de las etiquetas utilizadas para identificar un FEC.

Dos LSR que mantienen sesiones LDP se los denomina “pares LDP”. Durante las sesiones los pares LDP intercambian información de forma bidireccional.

LDP utiliza cuatro tipos de mensajes, a continuación analizaremos cada uno de ellos:

- **Mensajes de descubrimiento:** Los LSR envían mensaje LDP HELLO a través de todas las interfaces donde está configurado LDP, con el objetivo de conocer a sus LSR vecinos. La figura 1.16 muestra el envío de los paquetes HELLO para descubrir nuevos vecinos.

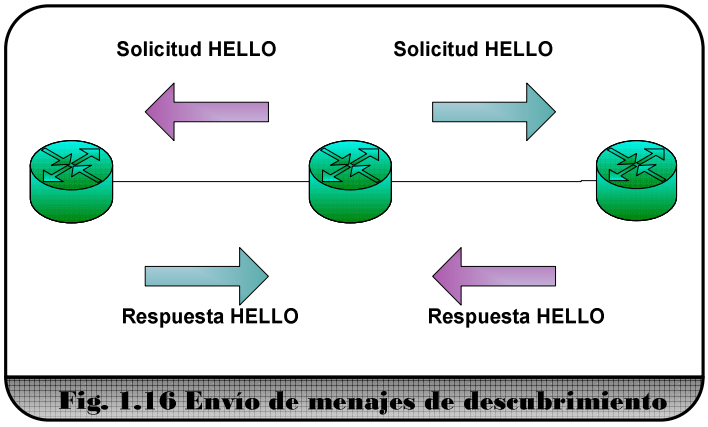


Fig. 1.16 Envío de menajes de descubrimiento

- **Mecanismo básico de descubrimiento:** Este mecanismo envía paquetes HELLO a intervalos constantes, a través de todas las interfaces donde tiene configurado el protocolo de descubrimiento LDP. Es decir, permite descubrir los LSR´s que están conectados directamente a las interfaces.

- **Mecanismo extendido de descubrimiento:** Este mecanismo se emplea para descubrir LSR´s que no están conectados directamente a las interfaces. Es decir, el LSR local envía un paquete HELLO con una dirección IP específica que permitirá descubrir un LSR puntual.

- **Mensajes de sesión:** Cuando dos LSR´s se descubren mediante los mensajes HELLO, proceden a establecer conexión entre ellos mediante el puerto TCP 646. Si la conexión TDP se estable, ambos LSR empiezan a negociar los parámetros de sesión.

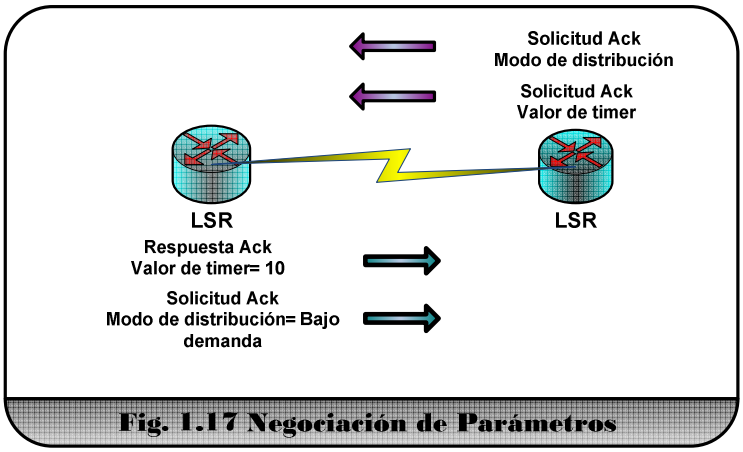


Fig. 1.17 Negociación de Parámetros

- **Mensajes de publicación:** Uno de los parámetros que se negocian durante la sesión es el modo de publicaciones de etiquetas, En los mensajes de publicaciones se envían las etiquetas que contiene cada LSR, de esta forma cada LSR construye su base de datos

- **Mensajes de notificación:** Estos mensajes permiten la gestión interna de una sesión LDP. Pueden existir dos tipos de notificaciones: error fatal e información consultiva. Cuando ocurre un error fatal automáticamente se cierra la sesión entre los LSR.

1.3.2.3 RESOURCE RESERVATION PROTOCOL (RSVP)

RSVP está definido por la RFC 2205, como un protocolo de control de red usado para especificar calidad de servicio en una red en particular. RSVP no es un protocolo de enrutamiento; utiliza mecanismos para establecer LSPs, distribuir etiquetas y realizar trabajos para satisfacer los requerimientos que demanda la ingeniería de tráfico.

En RVSP, un flujo de datos es una secuencia de mensajes que tienen la misma fuente, destino y calidad de servicio. Los requerimientos de calidad de servicio son comunicados a través de la red mediante una especificación de flujos, como una estructura de datos usada por un host para solicitar servicios especiales a la red.

RVSP soporta tres tipos de tráfico:

- Mejor esfuerzo
- Sensibilidad de flujo
- Sensibilidad de retardo

Mejor esfuerzo: Conocido como *Best Effort*, es el trafico tradicional IP. Es decir los paquetes circulan por la mejor ruta.

Sensibilidad de flujo: Este método garantiza que el tráfico fluya en un determinado tiempo, caso contrario lo descarta. En un canal de 100 Mbps de ancho de banda deseamos enviar 200 Mbps por un largo periodo, el router eliminara el tráfico.

Sensibilidad de retardo: Se aplica en aplicaciones donde la exactitud en la entrega de los paquetes es fundamental para su correcto funcionamiento.

Los flujos de datos RSVP generalmente son habilitados por sesiones, sobre el cual se envían los paquetes de datos. Una sesión es un conjunto de datos que están dirigidos a una misma dirección *unicast* o *multicast*, donde el flujo se origina del mismo nodo.

Para determinar la mejor ruta que deben seguir los paquetes con calidad de servicio, los nodos intercambian mensajes que se incorporan en los paquetes RSVP. Estos paquetes permiten crear circuitos virtuales entre el emisor y el receptor. Existen cuatro tipos de mensajes.

El primer mensaje que se envía cuando se desea establecer una sesión es de solicitud de reserva o RESV. Este mensaje es generado por el nodo receptor y atraviesa la ruta de forma inversa, de esta forma el nodo emisor determine el control de flujo necesario. Para que se produzcan los mensajes de reserva, el nodo emisor debe enviar un mensaje que contenga la ruta o LSP según la información de los protocolos de enrutamiento, esta solicitud es conocida como mensaje de trayectoria. El protocolo maneja mensajes de error y confirmación. Se producen mensajes de error en la reservación si la solicitud no se puede realizar por algún problema en la red y mensajes de error de trayectoria cuando el trazado de la ruta no tiene éxito. Los mensajes de limpieza se encargan de eliminar los estados transmisión, trayectoria y reserva, sin tener que esperar a que expire su tiempo de vida.

RSVP almacena el estado de los nodos o LER actualizando periódicamente la información mediante los mensajes de trayectoria y solicitud de reservación. Los cambios de las rutas tienen un mínimo de retardo porque si los mensajes que informan sobre el estado defieren sobre el almacenamiento, se actualiza inmediatamente y se propagan las actualizaciones al resto de las etapas.

2.1 INTRODUCCIÓN

Hasta hace poco tiempo sucursales de una empresa podían tener de forma individual, una red local que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

Con la aparición de las empresas multinacionales en los años 1940, surgieron grandes inconvenientes relacionados a la actualización de información financiera, control administrativo o el manejo de los recursos. Surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. El gran inconveniente del uso de las líneas telefónicas es su alto costo. Las Virtual Private Networks (VPN) son una alternativa a la conexión WAN (Wide Area Network), que permitió bajar los costos de éstos y brindar los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

2.2 DEFINICIÓN VPN

Una Virtual Private Network (VPN) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura 2.1 la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

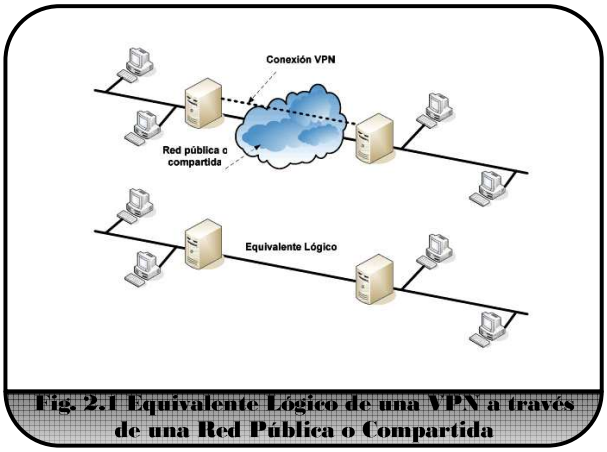


Fig. 2.1 Equivalente Lógico de una VPN a través de una Red Pública o Compartida

Las VPN´s también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

La tecnología de túneles (*Tunneling*) es un modo de transferir información encapsulada dentro de un paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

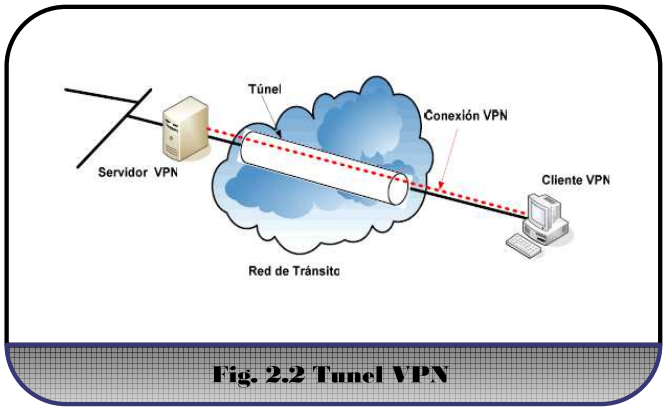


Fig. 2.2 Tunel VPN

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN´s es conceptualmente parecido a la autenticación en un sistema, como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación se lleva a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer

participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Cualquier desviación en el campo de *checksum* indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados para que no puedan ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

Existen dos tipos de técnicas de encriptación que se usan en las VPN:

- ✓ Encriptación de clave secreta
- ✓ Encriptación de clave pública

Encriptación de clave secreta: Se utiliza una contraseña conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes, puede ocasionar problemas de seguridad.

Encriptación clave pública: Implica la utilización de dos claves, una pública y una secreta donde la primera se envía a los demás participantes. Al encriptar, se usa la

clave privada propia y la clave pública del otro participante de la conversación. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la clave secreta.

2.2.1 BENEFICIOS DE VPN

- Ofrece conectividad a zonas geográficas
- Mejora la seguridad
- Reduce costos frente a otras soluciones WAN
- Mejora la productividad
- Simplifica las redes de datos
- Abre un nuevo abanico de oportunidades
- Favorece el soporte remoto
- Es compatible con las conexiones de banda ancha

2.2.2 TIPOS DE VPN

Podemos hablar de dos tipos de VPN´s básicamente:

- Intanet y Extranet

Intranet: Una Intranet es aquella red que interconecta sitios geográficamente separados de la misma compañía y por la que se puede tener aplicaciones que permita a los clientes internos utilizar adecuadamente la información.

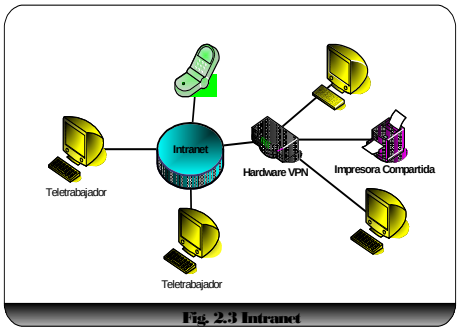


Fig. 2.3 Intranet

Extranet: Una Extranet es una red en la cual se han conectado al menos dos sitios de compañías distintas, y el tema de la seguridad es un factor muy importante debido a que se permite el acceso a los usuarios remotos a la información exclusivamente necesaria.

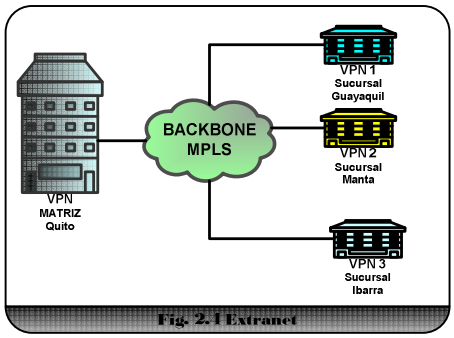


Fig. 2.4 Extranet

2.2.3 MODELOS DE VPN

Actualmente existen varias opciones para repartir las responsabilidades del manejo de las políticas, una de las opciones es dejar esta posibilidad al proveedor del servicio, la otra que sea el cliente quien las maneje y la tercera distribuir el trabajo

entre la empresa y el cliente de esta manera se puede dividir al estudio de las VPN en dos modelos

- ✓ Modelo de sobrecapas (*Overlay Model*)
- ✓ Modelo par a par (*Peer to peer Mode*l)

Modelo de sobrecapas: En este tipo de tarea tanto el proveedor de servicio como del cliente están claramente definidas. El primero se encarga de brindar servicio de circuitos virtuales VC (*Virtual Circuit*), mientras el cliente establece la comunicación entre los enrutadores, la información se intercambia entre los equipos del cliente. Las arquitecturas más comunes en las que funciona este modelo son *Frame Relay*, X.25, ATM, *Tunneling* IP.

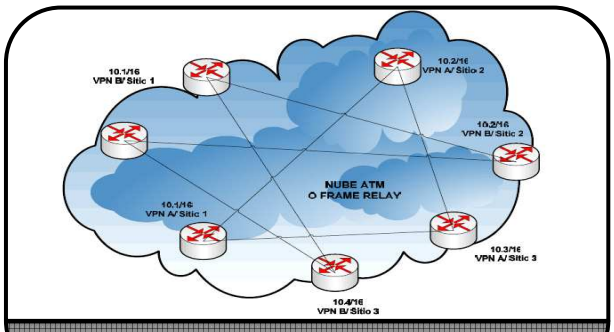


Fig. 2.5 Modelo de Sobrecapas

Modelo Par a Par: Con este modelo se facilitan funciones como la escabilidad y la posibilidad de habilitar calidad de servicio en la capa de red, la diferencia radica en que el router del cliente o CPE *(Customer premises Equipment)* ó CE *(Customer*

Equipment) ahora se conecta con un router del proveedor de servicio PE *(Provider Equipment)* y no directamente con otro CE.

El motivo de llamar Par a Par a este modelo radica en que desde el punto de vista del enrutamiento de la red del proveedor de servicio, actúa como una par con la red del cliente desde que los CE´s se conectan directamente con los PE´s.

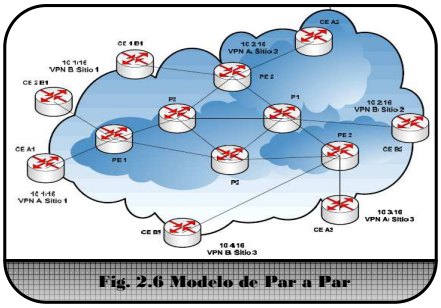


Fig. 2.6 Modelo de Par a Par

VENTAJAS

- El intercambio de información de enrutamiento entre los routers del cliente y del proveedor del servicio permiten obtener gran escabilidad pues el número de sitios se puede incrementar sin tener que aumentar la tabla de enrutamiento.
- Con el aumento de un cliente no se producen cambios en la red, solamente entre el CE y PE al cual se conecte. Mientras que en modelo de sobrecapas se requiere crear VC´s hacia todos los sitios de red.

2.3 MODELO MPLS VPN

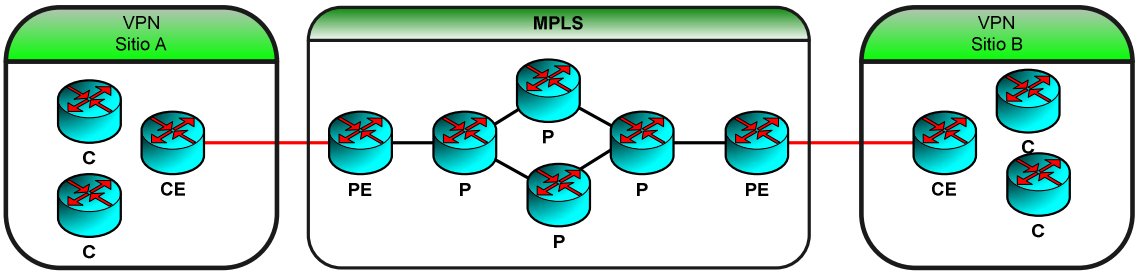


Fig. 2.7 Modelo MPLS VPN

El modelo que describe VPN utilizando MPLS se denomina técnicamente como BGP/MPLS VPN debido a que en el núcleo de la red corre BGP (*Border Gateway Protocol*). Debido a sus características de escalabilidad, permite al proveedor del servicio manejar cientos de VPN´s manteniendo un bajo costo por el servicio. Este modelo se basa en cuatro llaves tecnológicas:

- Distribución restringida de la información de enrutamiento.
- Múltiples tablas de enrutamiento
- Uso de un nuevo tipo de direcciones: direcciones VPN –IP
- MPLS

2.3.1 DISTRIBUCIÓN RESTRINGIDA DE LA INFORMACIÓN DE ENRUTAMIENTO

Es de esperar que el proveedor de servicios, por motivos de seguridad, no permita que un cliente de una VPN tenga acceso al resto de VPN´s debido a que no posee enlaces dedicados que proveen seguridad como en el modelo de sobrecapas, de la misma manera, no se desea que la tabla de enrutamiento de un cliente se publique hacia los demás clientes del proveedor del servicio. De ahí, que crear VPN´s requiere que el flujo de datos sea restringido a través de los diferentes routers en la red del proveedor.

Para que este flujo de datos se restrinja también es necesario que el flujo de información de enrutamiento se restrinja entre las diferentes VPN´s. Para lograr esto, la distribución de la información de enrutamiento de describe a continuación:

1. La información de enrutamiento se propaga desde el sitio del cliente hasta el proveedor de servicios, en otras palabras, desde el router CE hacia el router PE, usando protocolos de enrutamiento como RIP (*Routing Information Protocol*), OSPF (*Open Shortest Path First*), BGP o rutas estáticas.

2. En el router de ingreso PE, la información de enrutamiento se exporta hacia el proveedor de BGP (*núcleo de la red*).

3. Esta información se enruta hacia los routers PE usando BGP.

4. En el router PE de egreso, la información se importa desde el proveedor de BGP, paso totalmente opuesto al segundo.

5. La información de enrutamiento se envía desde el router PE hacia el router CE, utilizando RIP, OSPF, BGP o rutas estáticas, paso totalmente opuesto al primero.

La técnica de Filtrado de Rutas del atributo de BGP denominado Comunidad BGP (*BGP Community*) se usa para restringir la distribución de la información de enrutamiento. La comunidad BGP sirve como identificador que se puede atar a una ruta. En el paso 2, el router de ingreso PE debido a su configuración, coloca una apropiada Comunidad BGP a una ruta y la exporta al proveedor BGP. En el paso 4, como resultado de su configuración, el router de egreso PE utiliza este atributo para controlar las rutas importadas desde el proveedor BGP hacia el router CE. Es decir, se utiliza al atributo de Comunidad BGP como un identificador que permite distinguir entre las diferentes VPNs y mantener un plan IP de direccionamiento independiente para cada una.

Hay que notar que la restricción de la distribución de la información de enrutamiento está limitada a los pasos 2 y 4 que se manejan por el proveedor de servicios y, por

tanto, el cliente usuario de la VPN no está envuelto en la implementación de estos mecanismos.

En la figura 2.8 se ilustra el funcionamiento de la restricción de la información de enrutamiento en una red BGP/MPLS VPN desde el sitio 1 al sitio 3 de la VPN A.

En el paso 1, la ruta para 10.1/16 se distribuye desde el router CE en el sitio 1 de la VPN A, CEA1, hacia el router PE que está directamente conectado PE1. Ésta distribución se puede realizar mediante RIP. En el paso 2, la ruta se exporta hacia el proveedor BGP, el router de ingreso PE1 y, bajo el control de su configuración local, coloca la Comunidad BGP apropiada a la ruta. En el paso 3, esta ruta se distribuye hacia otros conmutadores PE usando los procedimientos BGP. En el paso 4, el router PE de egreso, PE3, la ruta se importa desde el proveedor BGP.

Esta importación se controla mediante el mecanismo de filtrado de rutas del BGP realizado por el PE3 (*bajo el control de su configuración local*) y se basa en el atributo de Comunidad BGP que lleva la ruta importada. Finalmente, en el paso 5, la ruta se distribuye desde el PE3 al CE3 en el sitio 3 de la VPN A que puede ser ejecutada por RIP u otro protocolo, como en el paso 1.

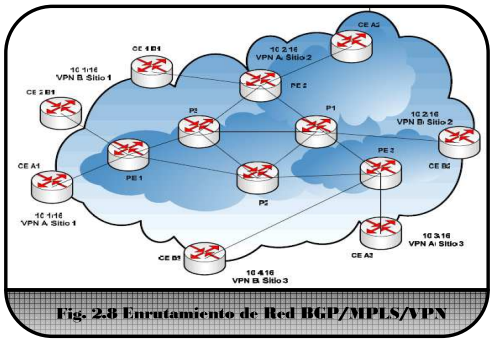


Fig. 2.8 Enrutamiento de Red BGP/MPLS/VPN

Deben realizarse algunas observaciones en el mecanismo de interconexión de sitios BGP/MPLS VPN que tienen implicación en la escalabilidad.

- El router CE mantiene solamente adyacencia de enrutamiento con su par, el router PE, y no tiene adyacencia con los demás routers CE de las demás VPNs. Como consecuencia, el número de adyacencias que un router CE tiene que mantener es independiente del número de sitios que posea la VPN. Esto facilita el mantenimiento de VPNs que tengan cientos o miles de sitios. En el modelo de Sobrecapas, cada router debe tener adyacencia con los demás routers de la VPN, y si los sitios son cientos, la tabla de enrutamiento de cada CE es muy compleja.

- Para agregar un nuevo sitio a una VPN, se debe configurar adecuadamente el router PE al cual el nuevo CE se va a conectar. No se realiza ninguna configuración en los CEs de los demás sitios de la VPN. En el modelo de Sobrecapas, al añadir un nuevo sitio, se deben realizar configuraciones en todos los demás routers de la VPN, nuevos circuitos virtuales hacia todos los demás sitios. En conclusión, administrativamente, el modelo Par a Par es mucho más escalable.

- El router PE no tiene que mantener rutas de otros sitios de VPN´s que no estén directamente conectados. El número de Comunidades BGP está limitado a 216 (*65536*), para aumentar esta capacidad se ha definido el

atributo de Comunidad BGP extendida con una capacidad de 232 (*más de 4294 millones*) que son administradas por cada proveedor de VPNs para identificarlas.

2.3.2 MULTIPLES TABLA DE ENRUTAMIENTO

Uno de los principales problemas en la implementación de VPN´s sobre el modelo par a par es que diferentes clientes pueden utilizar las mismas direcciones, la tecnología MPLS/VPN planteas que para cada VPN exista su propia tabla de enrutamiento en el router PE, por tanto cualquier cliente o sitio que pertenece a una VPN tiene acceso únicamente a la tabla que contiene las rutas para esa VPN.

Los routers PE de la red MPLS/VPN contienen un número de tablas de enrutamiento por VPN.

El concepto de routers virtuales permite al cliente usar cualquier dirección IP en su red, sea esta pública (*dirección válida de Internet*) o privada, y esto es gracias a que la dirección tiene significado solo dentro de una misma VPN.

Ruta objetivo (Route Target) y tabla de enrutamiento VRF (VPN routing fowarding table VRF): La combinación entre la tabla de enrutamiento VPN tradicional y la tabla de enrutamiento VPN basada en conmutación de etiquetas se la conoce como VRF. Es necesario notar la diferencia entre ellas. En IP tradicional, el siguiente salto puede no estar conectado al router, la tabla posee la dirección del siguiente salto

pero no la interfaz de salida correspondiente. La tabla de enrutamiento en MPLS contiene toda la información necesaria para enrutar el paquete hacia el destino.

No existe una correspondencia directa entre VPN y *Virtual Routing and Forwarding*, ya que la VRF está definida solamente en el router PE, entonces ¿Cómo el router conoce cuales rutas deben ser introducidas dentro de la VRF?, aquí se introduce el concepto de *Route Target* (Ruta Objetivo) de 64 bits de longitud. Cada ruta VPN se etiqueta con una o más Rutas Objetivo cuando se exporta desde una VRF (para ser ofrecida a otras VRF´s en otros PE´s). La Ruta Objetivo (*Route Target*) puede ser considerada como un identificador de VPN y en definitiva sirve para identificar las VRF´s que deben recibir la ruta.

Cada VRF en un router PE se conforma desde dos fuentes: la primera de ellas es el conjunto de rutas correspondientes al router CE de la VPN directamente conectada. La segunda fuente es el conjunto de rutas que recibe de los otros routers PE, las cuales, para mantener correspondencia a la misma VPN, y no sean mezcladas con otras, pasan por el mecanismo de filtrado de rutas basado en la Comunidad BGP.

2.3.3 DIRECCIONES VPN – IP

Las razones por las que BGP se usa como protocolo de enrutamiento entre los routers PE, en una red par a par BGP/MPLS VPN, son las siguientes:

- La red del proveedor de servicios es un sistema autónomo y es necesario que los paquetes transiten por él a otros sistemas autónomos.

- El sistema autónomo del proveedor de servicios debe poseer múltiples conexiones a otros sistemas autónomos.

- La necesidad de que el tráfico cursante dentro de la red del proveedor de servicios sea administrado.

- El número de rutas VPN en una red puede llegar a incrementarse, BGP es un protocolo de enrutamiento que puede soportar un gran número de rutas.

- BGP fue diseñado para un ambiente multiprotocolo MP-BGP (*multiprotocol BGP*), ya que puede manejar diferentes familias de direcciones (*IP, IPX, VPNIP*).

- Está diseñado para intercambiar información entre routers que no están directamente conectados, lo que permite que la información de enrutamiento de VPN se mantenga fuera del núcleo de la red del proveedor de servicios (*routers P*) y sea intercambiada entre los routers PE.

- BGP puede llevar a cualquier información atada a la ruta como un atributo BGP opcional. Además, se puede definir cualquier atributo que puede ser enrutado transparentemente por cualquier routers BGP que no entienda este atributo, lo que permite que la distribución de las Rutas Objetivo sea extremadamente simple.

Al usar BGP dentro de la red del proveedor del servicio, las direcciones IP deben ser únicas. Lo cual se contrapone con la característica de que las VPN´s pueden manejar un plan de direccionamiento IP iguales. Para lograr que las direcciones IP sean únicas, se añade un campo a ellas llamado Distinguidor de Rutas (*Route Distinguisher*) creando un nuevo tipo de direcciones IP-VPN. Cada VRF dentro de un router PE necesita tener un Distinguidor de Ruta asociada a cada VPN, el cual puede o no estar asociada con un sitio particular de una VPN. En los casos más comunes, si la VPN es una Intranet, es posible usar un Distinguidor de Ruta único para la VPN, pero si un sitio en el futuro llega a ser miembro de una Extranet VPN, no se recomienda este direccionamiento ya que se incurrirá en cambios en las configuraciones para lograr una red Extranet. Es decir, si se usa un Distinguidor de Ruta diferente para cada VPN y un sitio en particular decide ser miembro de una VPN múltiple, no es posible identificar que Distinguidor de Ruta usar para el sitio pues pertenece a más de una VPN.

Se debe establecer la asignación de un valor particular de un Distinguidor de Ruta para cada VRF en el router PE. La estructura de este valor puede ser ASN:nn

(*Autonomous System Number : número de VRF*). Es recomendable el uso de este formato pues el ASN es asignado por la Autoridad de Asignación de Direcciones de la Internet IANA (*Internet Asigned Numbers Authority*) para que sea única dentro de los proveedores de servicio. Los clientes pueden conectarse a diferentes proveedores de servicio MPLS/VPN, por lo que es recomendable que los dos primeros bytes sean para el ASN para contrarrestar el uso de iguales direcciones VPN-IP en dominios MPLS/VPN separados. El proveedor de servicios asigna la segunda porción del Distinguidor de Ruta que debe ser único para cada VRF.

El funcionamiento de BGP para la VPN A, el router PE1 recoge información de enrutamiento del router CEA mediante cualquier protocolo como OSFP, RIP o rutas estáticas. Esta información es redistribuida, es decir, que se pasa la información de enrutamiento (*tablas métricas, etc*.) desde un protocolo hacia otro, hacia fuera del PE1 mediante MPBGP.

A las direcciones IP de la VPN se añaden el Distinguidor de Ruta para hacerlas únicas, y así el router PE mantenga las rutas de diferentes VPN´s separadas. Además en el PE1 se identifica la VRF del sitio 1 de la VPN A con la Ruta Objetivo correspondiente. Viajan además atributos adicionales de BGP como la Ruta Objetivo definida por las Comunidades BGP. Toda esta información se propaga por MP-BGP hacia el router PE2. Los routers P no están envueltos dentro del ambiente MP-BGP, ya que el mecanismo de enrutamiento para estos routers usa MPLS, no necesita

tomar decisiones basándose en las direcciones IP-VPN. El enrutamiento se basa en la etiqueta llevada por el paquete incrementándose de esta manera la escalabilidad.

El router PE2, después de recibir las rutas MP-BGP, utiliza la Ruta Objetivo correspondiente a la VRF del sitio 2 de la VPN A, y la compara con el Distinguidor de Ruta que viajó desde el sitio 1 y así trasladar la información de enrutamiento a la VRF que le corresponda. Se retira el Distinguidor de Ruta de la dirección VPNIP resultando de nuevo en IP tradicional. Finalmente la información de enrutamiento recibida por BGP se redistribuye en el proceso de RIP, OSPF, etc. Y se traslada hacia el sitio 2 de la VPN A.

2.3.4 MPLS COMO MECANISMO DE ENRUTAMIENTO

Los paquetes enrutados a través del backbone del proveedor de servicios (routers P) deben ser únicos para poder reconocerlos, para lo cual se le añade el Distinguidor de Ruta. El enrutamiento se puede realizar mediante este campo leyendo los 96 bits que lo conforman (VPN + dirección IP) en cada salto hacia el destino, haciendo un poco complicado el proceso. Para proveer el enrutamiento mediante direcciones VPN-IP se usa MPLS, debido a que separa la información de datos del paquete de la cabecera IP. Se puede asociar con una LSP (Label Switched Path) a cada ruta VPN-IP y luego enrutarlos mediante MPLS. Las direcciones VPN-IP son confinadas dentro de la red del proveedor de servicios y por lo tanto también MPLS está confinada dentro de la red del proveedor.

Cada router PE necesita un identificador único mediante una dirección IP, el cual se propaga a través de la red de routers P usando BGP. Esta dirección IP se usa como el atributo del siguiente salto de BGP (BGP next hope attribute) para todas las VPNs publicadas en un router. PE. Una etiqueta se asigna en cada router P para cada ruta hacia un router PE y propagada hacia todos sus vecinos. Los demás routers PE reciben la etiqueta asociada con el router de egreso PE de los demás routers PE a través de un proceso de distribución de etiquetas. Luego de que la etiqueta asociada al router de egreso se recibe en el router de ingreso, se crea el LSP y el intercambio de paquetes VPN puede comenzar. Este procedimiento solo ocurre en el plano de control, pues en el plano de datos lo único que se intercambia son etiquetas asociadas a las VRFs y etiquetas para la conmutación entre los routers PE.

Un router PE se comporta como un LSR (Label Switching Router) de borde. Cuando un router CE envía un paquete IP hacia un router PE, el router PE usa la interfaz de entrada para identificar la VPN a la que el router CE pertenece y más precisamente la tabla de enrutamiento o VRF asociada a esa VPN. Una vez que se identifica la VRF, se añade el Distinguidor de Ruta al paquete, la etiqueta que identifica esa VRF. El router PE determina la interfaz de salida, envía el paquete hacia el router P con otra etiqueta apilada la cual fue recibida desde el router PE de egreso. La etiqueta del nivel superior (top label) se asocia en el router PE de egreso y distribuida al router PE de ingreso, sirve para el enrutamiento dentro de la red de servicios.

La segunda etiqueta sirve como índice para identificar la VRF a la cual se debe apuntar para entregar los paquetes de una VPN determinada en el router PE de egreso y posteriormente enrutarlos hacia el router CE de la VPN.

En la figura 2.9 se muestran dos sitios dentro de una VPN, y en cada sitio se muestra su router CE (CE1 y CE2). Los routers PE1 y PE2 están configurados con el apropiado Distinguidor de Ruta para esa VPN y la apropiada Comunidad BGP para ser usada cuando exporten e importen las rutas desde el proveedor de BGP. En el router PE1, la interfaz que conecta PE1 con CE1 está asociada con la VRF de esta VPN.

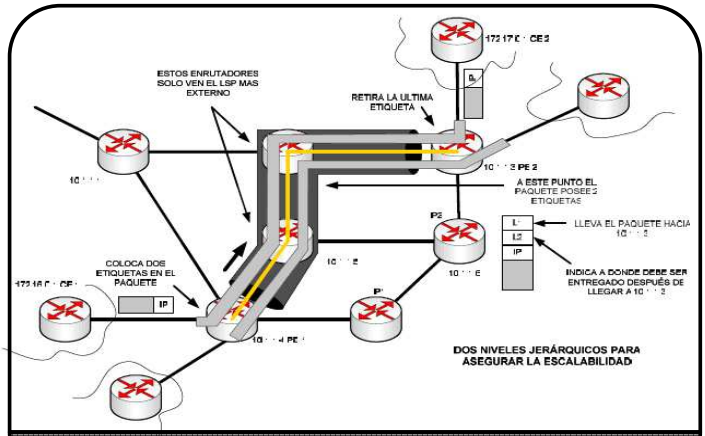


Fig. 2.9 Transporte de Datos de Una red MPLS VPN

Cuando el router PE2 recibe una ruta con información que permite alcanzar la red 172.17/16, desde el CE2, el router PE2 convierte la información de esa ruta desde IP tradicional a VPN-IP, coloca el atributo extendido de Comunidad BGP y exporta esta ruta hacia el proveedor BGP. En el atributo BGP del siguiente salto se coloca la dirección del router PE2. Además, a toda la información BGP adicional, la ruta

también lleva una etiqueta asociada con esa ruta VPN-IP. Esta información es distribuida hacia el router PE1 usando BGP. Cuando PE1 recibe la ruta, convierte de IP-VPN a IP y lo usa para publicar la VRF asociada con la VPN.

Además, existe un LSP desde el router PE1 al router PE2, el cual está asociado con una ruta hacia el router PE2 que se puede mantener mediante LDP (*Label Distribution Protocol*) o Ingeniería de Tráfico MPLS. Hay que notar que la ruta distribuida a través de BGP lleva como Atributo de Siguiente Salto (*Next HopeBGP Attribute*) la dirección del router PE2, y la ruta hacia ese router está dada por BGP. Es entonces la dirección del router PE2 la que establece la correspondencia entre el enrutamiento interno del proveedor de servicios y las rutas de la VPN detallada (*por ejemplo, la ruta hacia 172.17/16*). En este punto, la VRF en el router PE1 contiene una ruta para la red 10.1.1/24 y una pila de etiquetas en donde la etiqueta más interna es la etiqueta que el router PE1 recibe vía BGP y la etiqueta externa es la asociada con la ruta hacia el router PE2.

Si se lo expone de una manera más simple, el router CE1 envía un paquete con destino 172.17.0.1 cuando el paquete arriba al router PE1, determina la apropiada VRF para esa VPN que está asociada a la interfaz de entrada (*que está directamente conectada a CE1)*. El router PE1 coloca dos etiquetas L1 y L2 envía el paquete hacia el router P1. Éste a su vez, usa la etiqueta más externa (*top label*) para tomar su decisión de enrutamiento y enviarlo hacia el router P2, el cual es el penúltimo salto antes de llegar a un LSR de borde, entonces P2 retira la etiqueta externa L1 antes de

enviarla hacia el router PE2. Cuando PE2 recibe el paquete, usa la etiqueta interna L2 para realizar su decisión de enrutamiento. El router PE2 retira la etiqueta y envía el paquete hacia el router CE2.

2.4 ENRUTAMIENTO ESTÁTICO:

El encaminamiento estático es un método manual para alcanzar redes que se encuentran en otros segmentos. Es manual porque el administrador debe configurar todos los ruteadores que fueran necesarios para alcanzar una red, si se produce algún cambio en la red el administrador debe eliminar o aumentar rutas.

La distancia administrativa es un parámetro que está relacionado con la confiabilidad de una ruta. Un valor menor en la distancia administrativa indica una ruta estable. El valor por defecto de la distancia administrativa es de 1 y las redes directamente conectadas 0.

Para configurar una ruta estática en equipos CISCO se debe seguir el siguiente esquema:

1. Ingresar en modo privilegiado
2. Ingresar a configuración global
3. Digitar el siguiente comando:

   ip route [dirección de red de destino] [mascara de red] [interface de salida ó dirección del próximo salto]

2.5 ROUTING INFORMATION PROTOCOL Ó RIP V. 2

RIP es un protocolo simple de vector distancia y se basa en estándares abiertos. RIP evita que los bucles de enrutamiento se prolonguen en forma indefinida, mediante la fijación de un límite en el número de saltos permitido en una ruta, desde su origen hasta su destino. El número máximo de saltos permitido en una ruta es de 15.

Cuando un router recibe una actualización de enrutamiento que contiene una entrada nueva o cambiada, el valor de la métrica aumenta en 1, para incluir el salto correspondiente a sí mismo. Si este aumento hace que la métrica supere la cifra de 15, se considera que es infinita y la red de destino se considera fuera de alcance. RIP incluye diversas características las cuales están presentes en otros protocolos de enrutamiento. Por ejemplo, RIP implementa los mecanismos de espera y horizonte dividido para prevenir la propagación de información de enrutamiento errónea.

Para configurar RIP en router Cisco es necesario realizar lo siguiente:

1. Ingresar en modo privilegio
2. Ingresar a configuración global
3. Ejecutar el siguiente comando:

   # router rip

   # network [redes directamente conectadas]

2.6 OPEN SHORTEST PATH FIRST PROTOCOL OSPF

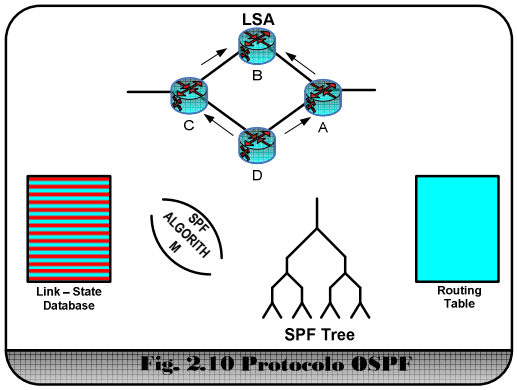


Fig. 2.10 Protocolo OSPF

Una característica importante en las redes OSPF es que poseen una arquitectura plana, es decir, todos los ruteadores conocen la estructura de la red. Cada vez que un ruteador detecta algún cambio en la topología, envía mensajes indicando la ruta inalcanzable. Los ruteadores vecinos que reciben estos mensajes actualizan su base de datos y reenvían las notificaciones a los siguientes vecinos, de esta forma todos los ruteadores que forman parte de la red conocen los cambios que se produjeron.

Cuando se activa OSPF en una red, cada router envía mensajes HELLO para detectar a los vecinos que están conectados a cada interface. Este proceso se repite hasta que todos los ruteadores tengan información de sus vecinos. Cada ruteador crea una base de datos de topológica, esta base de datos contiene información de todos los ruteadores.

Una vez creada la base de datos topológica, cada ruteador aplica un algoritmo llamado *Shortest Path First* ó SPF. El algoritmo SPF o también conocido como

algoritmo DIJKSTRA aplica un cálculo matemático para determinar la ruta más corta hacia todos los puntos de la red.

La ejecución del algoritmo SPF permite crear el árbol SPF. La estructura del árbol SPF inicia con el enrutador local como raíz, las ramificaciones están conformadas por todos los enrutadores que formen parte de una ruta con valores de costos bajos. La tabla de enrutamiento se basa en la información obtenida del árbol SPF.

Para reducir la cantidad de intercambios de información de enrutamiento entre los distintos vecinos de una misma red, los enrutadores seleccionan un enrutador designado ó DR y un router designado de respaldo ó BDR que sirven como puntos de enfoque para el intercambio de información de enrutamiento.

2.6.1 ESTRUCTURA DE SISTEMA AUTÓNOMO OSPF

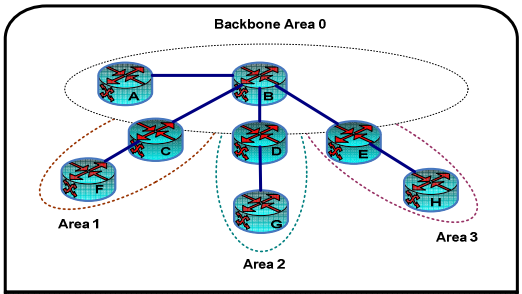


Fig. 2.11 Estructura OSPF

Cuando se configura OSPF en una red conformada por decenas de ruteadores, es necesario tomar en cuenta que cada vez que una red se publique como inalcanzable se producirá una inundación de paquetes HELLO. Este fenómeno puede mermar el funcionamiento de la red, en respuesta a este problema se puede recurrir a la

separación o segmentación de la red en diferentes sistemas autónomos ó AS (por sus siglas en ingles Au System).

El concepto de sistemas autónomos se define como el conjunto de enrutadores que forman parte de una comunidad, es decir cada vez que se produce algún cambio o evento en la red solo se enviarán mensajes HELLO a los miembros de esta sociedad, mejorando los tiempos de convergencia y disminuyendo los gastos de procesamiento. De esta forma podemos dividir nuestra red para evitar las tormentas de paquetes HELLO. Existe una estructura jerárquica para aplicar el concepto de sistemas autónomos.

- Área de distribución o área de Backbone.
- Área regular.

Área de distribución o Backbone: Esta área es la más importante, en ella acogerá la mayor cantidad de requerimientos. Por ellos los equipos que se empleen deben soportar grandes volúmenes de procesamientos y velocidad de transmisión. Generalmente en esta área no se conectaran los usuarios finales.

Área regular: En esta área se encontrara los usuarios finales, es decir no necesita de muchos requisitos. Las áreas regulares se las representa con valores mayores a 1.

2.6.2 TIPOS DE ENRUTADORES OSPF

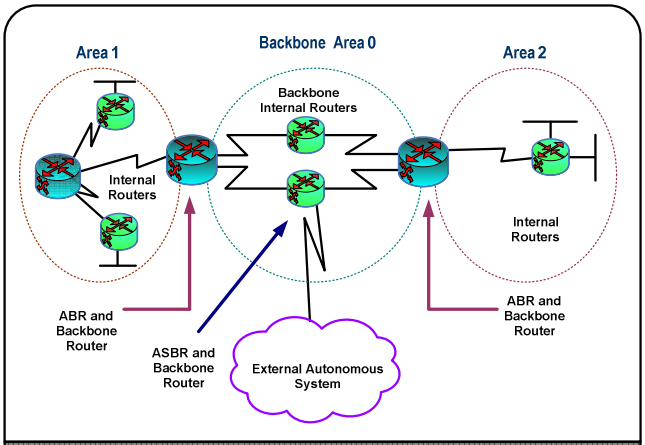


Fig. 2.12 Tipos de Protocolos OSPF

En una red OSPF existen varios tipos de enrutadores que cumplen funciones específicas dentro de la estructura. Existen cuatro tipos de enrutadores:

- Enrutadores internos: Estos enrutadores tienen la característica que todas sus interfaces pertenecen a una misma área y tiene idéntica base de datos de estado de enlace.

- Enrutadores principales: Son equipos que están dentro del perímetro de la área de distribución y sus interfaces se conectan al área 0.
- Enrutadores de borde o ABR: Este enrutador posee algunas interfaces conectadas al área 0 o distribución y las demás interfaces pertenecen a otras áreas.

- Router de borde de sistemas autónomos ó ASBR: Son enrutadores que tiene al menos una interface conectada a una red diferente, es decir permite el intercambio de entre diferentes sistemas autónomos o protocolos de enrutamiento. El intercambio de información de enrutamiento se denomina redistribución.

2.7 PROTOCOLO DE ENRUTAMIENTO DE GATEWAY INTERIOR MEJORADO Ó EIGRP

EIGRP es un protocolo propietario de CISCO que combina las características de protocolo de estado de enlace y vector distancia. Los enrutadores EIGRP mantienen información de la topología de la red a disposición de la memoria, con el objetivo que el tiempo de convergencia sea mínima cuando se presente cambios en la red.

EIGRP utiliza el protocolo DUAL ó Algoritmo de Actualización Difusa, es un algoritmo de vector distancia que permite calcular la mejor ruta para alcanzar una red en particular

EIGRP almacena la información en tres tablas:

- Tabla de vecinos
- Tabla de topología
- Tabla de enrutamiento

Cada router mantiene una tabla de vecinos en la cual registra la dirección y la interface. Cuando dos enrutadores envían paquetes Hello cada uno publica un tiempo de espera, el tiempo de espera es un lapso en el cual un enrutador se puede mantener sin recibir notificaciones de su vecino, una vez superado este tiempo el router publica a su vecino como inalcanzable.

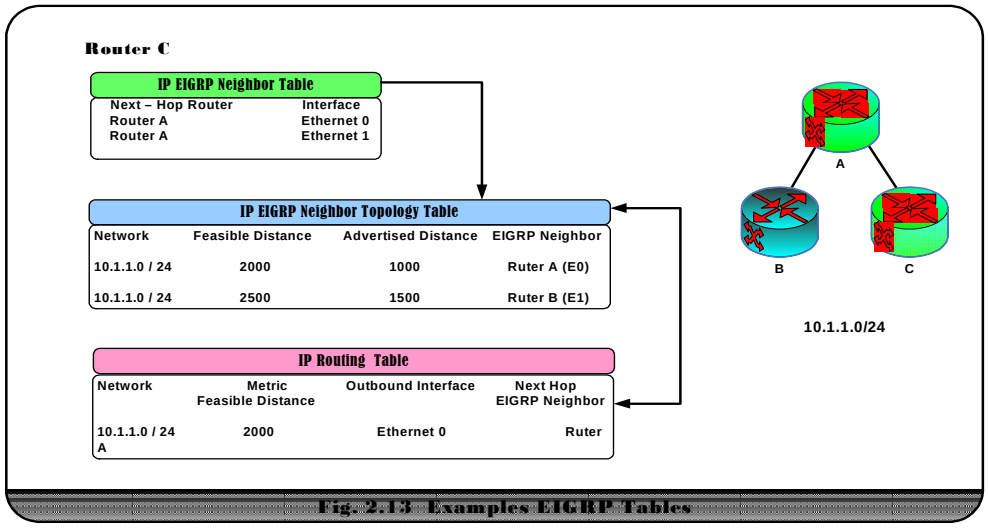


Fig. 2.13 Examples EIGRP Tables

La tabla topológica reúne todas las tablas de enrutamiento que se encuentran dentro de un sistema autónomo.

Una vez actualizada la tabla topológica EIGRP aplica el algoritmo Dual para identificar la ruta con la métrica más baja.

La tabla de enrutamiento EIGRP contiene las rutas hacia un destino específico. Se denomina sucesor a la ruta o rutas con el valor de métrica más bajo, puede existir

hasta cuatro sucesores para un mismo destino. Un sucesor factible es una ruta de respaldo, es decir si falla la ruta principal o sucesor automáticamente entra en funcionamiento la ruta del sucesor factible.

EIGRP garantiza tiempos rápidos de convergencia porque evita los bucles, lo que permite la sincronización de todos los enrutadores involucrados en el cambio de topología. EIGRP envía actualizaciones parciales y limitadas, esto provoca un uso eficiente del ancho de banda.

El método que EIGRP utiliza para mejorar el rendimiento del ancho de banda en la red es enviar las actualizaciones únicamente a los router que lo necesitan.

TECNOLOGÍAS USADAS EN EIGRP

EIGRP emplea en su estructura tres tecnologías claves para alcanzar la estabilidad y ventajas que brinda. Estas tecnologías son:

- Recuperación y detección de vecinos.
- Protocolo de transporte confiable
- Algoritmo de máquina de estado finito DUAL

Recuperación y detección de vecinos: Esta característica permite detectar vecinos a través del envío de mensajes Hello. Los mensajes Hello son enviados constantemente

cada cinco segundos, si el enrutador no recibe contestación de su vecino en un tiempo determinado lo cataloga como inalcanzable.

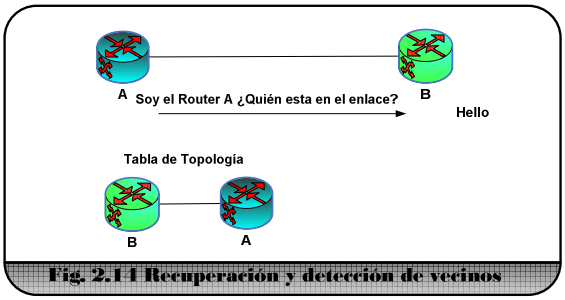


Fig. 2.14 Recuperación y detección de vecinos

<u>Protocolo de transporte confiable</u>: Es un protocolo de capa de transporte, al igual que TCP garantiza la entrega oportuna y segura de la información de enrutamiento.

RTP brinda la posibilidad de proporcionar un servicio confiable o no confiable, por ejemplo los paquetes Hello no requiere que se los clasifique como confiable ya que son enviados cada cinco segundos.

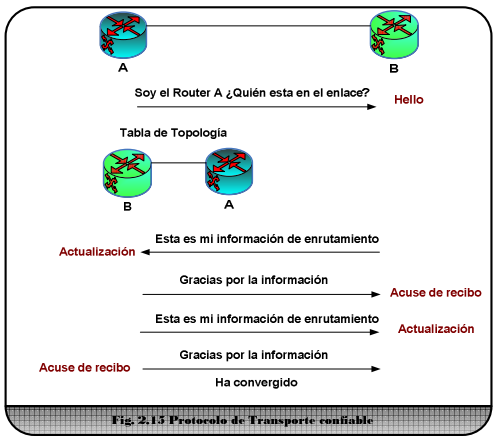


Fig. 2.15 Protocolo de Transporte confiable

Algoritmo de máquina de estado finito DUAL: Dual es el algoritmo de estado de enlace que utiliza EIGRP para calcular la mejor ruta. DUAL rastrea todas las rutas publicadas por los vecinos, se comparan mediante la métrica y evita los bucles.

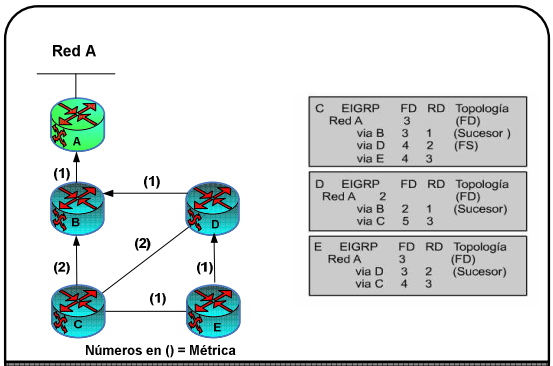


Fig. 2.16 Algoritmo de Estado Finito Dual

2.8 Border Gateway Protocol

BGP es un protocolo de encaminamiento usado entre sistemas autónomos. Está siendo utilizado ampliamente para conectar grandes redes de proveedores. El protocolo utiliza mensajes que se envían utilizando conexiones TCP. Los distintos tipos de mensajes que maneja este protocolo son :

Open: se utiliza para establecer una relación de vecindad con otro encaminador.

Actualización (Update): se utiliza para transmitir información a través de una ruta y/o enumerar múltiples rutas que se van a eliminar.

Mantenimiento (Keepalive): utilizado para confirmar un mensaje Open y para confirmar periódicamente la relación de vecindad.

Notificación: este tipo de mensajes se envían cuando se detecta una condición de error.

Los procedimientos funcionales de BGP son:

Adquisición de vecinos: ocurre cuando dos encaminadores situados en diferentes sistemas autónomos se ponen de acuerdo para intercambiar información de encaminamiento regularmente. Un encaminador le enviará a otro un mensaje Open. Si el destino acepta la solicitud le devolverá un mensaje de mantenimiento.

Detección de vecino alcanzable: una vez realizada la adquisición de vecinos se utiliza este procedimiento para mantener la relación. Periódicamente ambos dispositivos de encaminamiento se envían mensajes de mantenimiento para asegurarse que su par sigue existiendo y desea continuar con la relación de vecindad.

Detección de red alcanzable: cada encaminador mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para alcanzar dichas redes. Cuando se realiza un cambio a esta base de datos, el encaminador enviará un mensaje de actualización por difusión. De esta forma el resto de los encaminadores BGP podrán construir y mantener la información de encaminamiento.

3.1 PARÁMETROS PARA DISEÑAR UNA RED

El primer paso para diseñar una red, es tener un claro panorama de los objetivos de diseño. Cada red se diseña dependiendo de las necesidades de la compañía u organización. Usualmente los diseñadores se enfocan en cuatro pilares importantes al momento de implementar una red, son los siguientes:

- Funcionalidad
- Escalabilidad
- Adaptabilidad
- Administración
- Seguridad

Funcionalidad: Un Backbone de ser capaz de proporcionar seguridad, velocidad y confiabilidad. La red debe ser segura para evitar que usuarios extraños manipulen o causen daño a nuestra información. La red debe ser capaz de soportar grandes flujos de tráfico según la aplicación que se ejecute sobre ella. La confiabilidad y robustez es fundamental para proporcionar un servicio de calidad, debe existir enlaces de redundancia y los dispositivos deben cumplir con las especificaciones mínimas tanto en hardware como en software.

Escalabilidad: Cuando se diseña una red se debe tener en cuenta que la cantidad de usuarios, clientes, aplicaciones y necesidades van a aumentar con el transcurso de los años o será proporcional al crecimiento comercial de la empresa. Es decir, el diseño

original debe aumentar de tamaño sin que se produzcan cambios importantes en el diseño general.

Adaptabilidad: Cada año aparecen nuevas tecnologías informáticas y con ello nuevas necesidad, nuestra red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que estas van apareciendo.

Facilidad de administración: La red debe proporcionar las herramientas necesarias para facilitar su monitoreo y administración, con el objetivo de asegurar una estabilidad de funcionamiento constante.

3.2 DISEÑO DE LA RED FÍSICA DE UN BACKBONE MPLS

Una red está compuesta por dispositivos que se conectan entre sí mediante líneas de comunicación (cable de red, fibra óptica, medio inalámbrico, etc.) y elementos de hardware (adaptadores de red, repetidores, modem, etc.) que garantizan el correcto viaje de los datos.

En el diseño de un Backbone MPLS o cualquier tipo de red, es necesario tomar en cuenta algunos parámetros. A continuación se mencionan los más importantes:

- Tamaño de la red
- Capacidad de transporte
- Aplicaciones o servicios
- Factor económico

Una vez recopilada la información mencionada anteriormente, el Ingeniero de Diseño está en capacidad de elegir la topología más adecuada a su red. Entre las cuales se pueden mencionar:

- **Estrella:** La característica de esta red es que todos los elementos de la red se conectan a un punto tal como un concentrador, switch o enrutador.

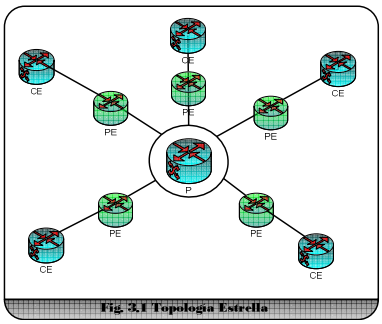


Fig. 3.1 Topología Estrella

- **Malla:** En esta red al menos un dispositivo se conecta con todos los elementos que conforma la red.

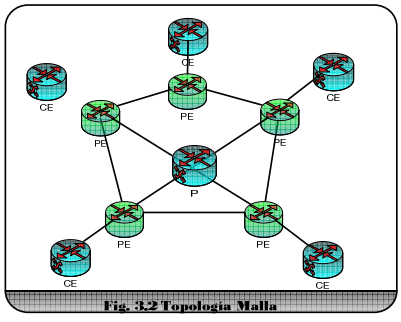


Fig. 3.2 Topología Malla

- **Mallada completa:** Tiene la particularidad que cada elemento se conecta con cada uno de los elementos restantes.

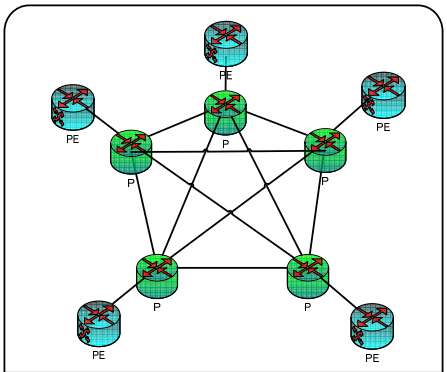


Fig. 3.3 Topología Full Malla

- **Anillo:** Los dispositivos están conectados de tal forma que forman un círculo.

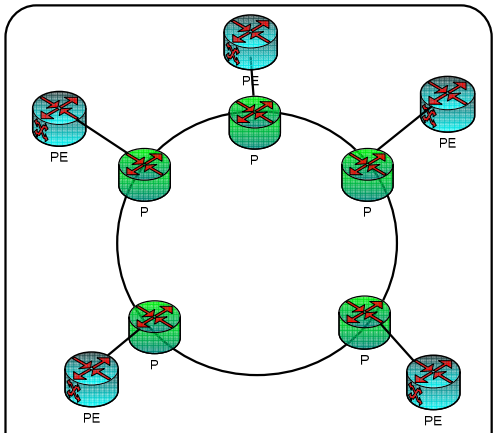


Fig. 3.4 Topología Anillo

3.3 CARACTERÍSTICAS DE HARDWARE DEL BACKBONE

Existen varios fabricantes de equipos informáticos que soportan MPLS, sin embargo no garantizan su correcto funcionamiento. El Ingeniero de Diseño debe considerar que el hardware a utilizar debe cumplir con ciertas especificaciones técnicas. A continuación se menciona las más relevantes.

- Interfaces: En el momento de decidir el tipo de interface, se debe temer en cuenta la extensión geográfica de nuestro Backbone y cuáles serán los medios para comunicar cada nodo de la red. Se pueden catalogar dos tipos de interfaces:

  Fast-Ethernet y Gigabit-Ethernet: Son capaces de transportar paquetes Ethernet pero la velocidad de transmisión son diferentes. Fast-Ethernet transmite datos a una velocidad máxima de 100 Mbps, mientras que Giga bit-Ethernet a 1000 Mbps. A menudo se utiliza este tipo de interfaces para enlaces de radio, fibra óptica o cobre.

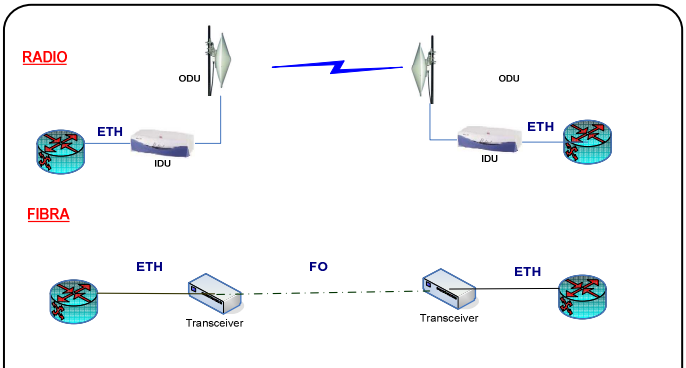


Fig. 3.5 Conexiones Interfaz Ethernet

Serial: Son interfaces que permiten enviar datos bit a bit. Sus aplicaciones son varias radio enlace con capacidad TDM o par de cobre.

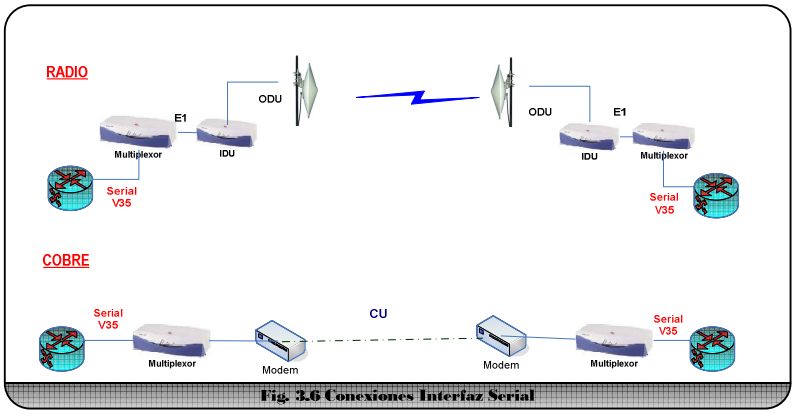


Fig. 3.6 Conexiones Interfaz Serial

- Procesamiento: Los dispositivos que se encuentran dentro del *core* deben ser capaces de procesar o transmitir toda la información que le envían. El *back plane* es un parámetro importante de un enrutador o conmutador, se la puede definir como un espacio de memoria donde almacenan los datos recibidos y los procesa.

3.4 DISEÑO DEL BACKBONE MPLS

Para el estudio de Tesis se diseñará un *backbone* MPLS ubicado en la ciudad de Guayaquil, que consta de cinco nodos ubicados estratégicamente para ofrecer servicios en toda la urbe. Los nodos son:

- Edificio World Trade Center
- Cerro Azul

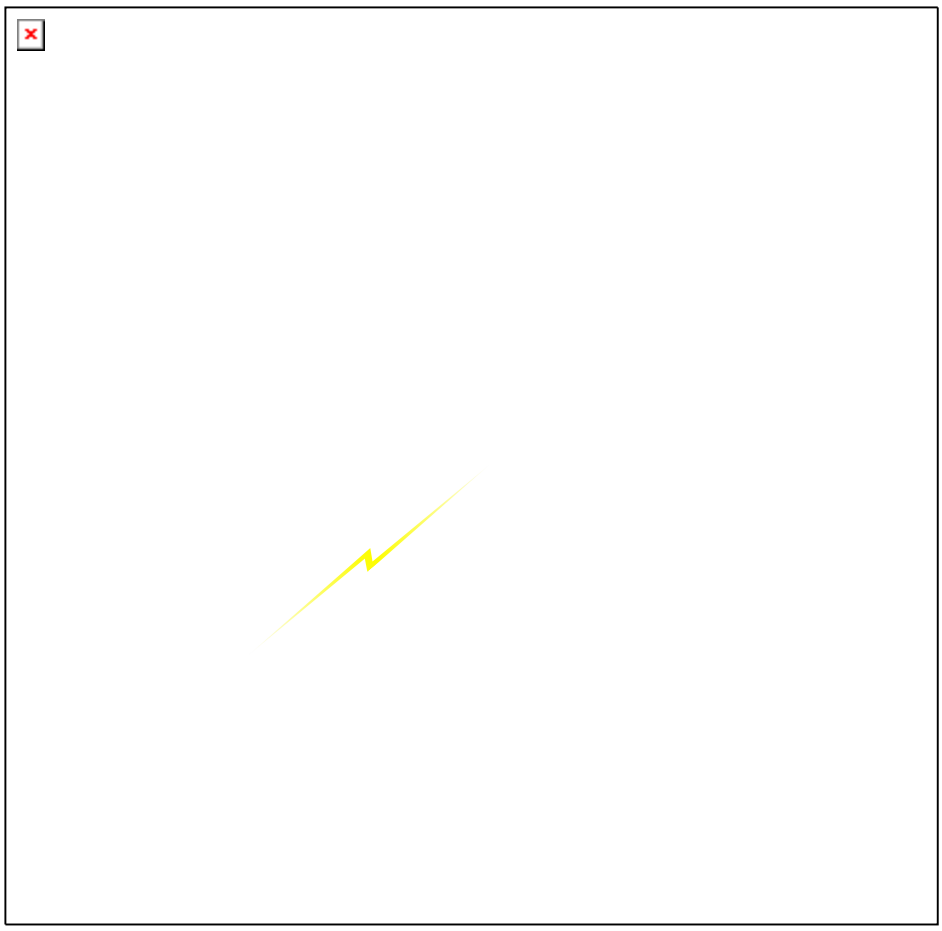
- Cerro del Carmen
- Cerro Jordan
- Cerro Bellavista

Para garantizar el buen funcionamiento del *backbone*, los medios a utilizar son fibra y enlaces de radio, teniendo como principal el tendido de fibra y como *backup* el sistema inalámbrico de radio, de esta forma se garantiza el prefecto funcionamiento de nuestro *backbone* en condiciones normales.

Para que nuestro *backbone* sea escalable se elegirá equipos que posean *slot* con capacidad de insertar nuevas tarjetas como seriales, Ethernet ó controladores E1. Los nodos tienen la particularidad que están en sitios elevados con línea de vista y ubicación céntrica que permite extenderse a gran parte de la ciudad.

3.5 TOPOLOGÍA DEL BACKBONE MPLS

Después de analizar la ubicación de los nodos y las particularidades de cada uno, se optó por la topología estrella, además aparecieron factores relevantes como la administración de la red y la escalabilidad para su expansión. En la figura 3.7 se observa el esquema de *backbone*.



Teniendo como objetivo el monitoreo y administración la red, el nodo central o núcleo se encuentra en el edificio WTC, lugar donde estarán ubicadas nuestras oficinas asegurando de esta manera el control de toda la red.

Es ventajoso utilizar la topología estrella que permite incorporar nuevos puntos sin afectar el diseño de la red, ya que con el pasar del tiempo la carga que va a soportar el *backbone* MPLS se va a incrementar y se debe expandir la red para no afectar su correcto funcionamiento.

Una vez aclarados los puntos antes mencionados se considera que la topología nos brinda las herramientas necesarias para garantizar el óptimo desempeño y cubrir con las necesidades que se presenten en el futuro.

Características de hardware del Backbone MPLS

En el mercado encontramos una lista muy larga de empresas dedicadas a fabricar dispositivos que soportan MPLS pero por motivos de estudio, maleabilidad y la facilidad de simulación, se decidió utilizar enrutadores CISCO. El backbone estará conformado por Cisco 7200 y para el cliente Cisco 1700, las características técnicas de cada uno se estudiarán a continuación.

Ruteador Cisco Serie 7200

La serie 7200 es uno de los ruteadores de rango medio más utilizado en la implementación de *backbone*. Se caracteriza por poseer gran relación precio/rendimiento, capacidad Gigabit, transporte de IP sobre WDM, integración de voz, datos o video y soporta múltiples protocolos.

CARACTERÍSTICAS TÉCNICAS RUTEADORES 7200 VXR

Con velocidad de procesamiento de hasta 2 millones de paquetes por segundo, adaptadores de puertos y servicios desde Nxds0 hasta Gigabit-Ethernet y OC-3. Permite ofrecer calidad de servicio (QoS), hasta 16000 sesiones protocolo punto a punto (PPP), transmisión de voz, datos y video a través de TDM, crear 5000 túneles IPSec/VPN y mucho más.

APLICACIONES QUE SOPORTA

- Capacidad multiservicio: La serie 7200 VXR provee soluciones escalables para servicio de voz, desde 3 hasta 20 T1´s y E1´s.

- Gestión de servicios de redes CPE: Incluye QoS, MPLS (MPLS VPN, MPLS QoS, MPLS TE), servicios WAN de frontera (soporta VLAN, NetFlow, NBAR), servicios de seguridad (NAT, ACL, encriptación para VPN) e integración de voz, datos y videos.

- Soporte IP: Soporta múltiples protocolos del modelo OSI como: Cisco Express Forwarding (CEF), MPLS, PPP, RIP, OSPF, EIGRP, BGP, ISIS,

L2TPv3, ACL, NAT, IPv4, IPv6, ATM, TFTP, SNMP, ARP, UDP, TCD, ICMP, DHCP y otros.

3.6 PRESUPUESTO DEL PROYECTO

El presupuesto se basa en la adquisición de los dispositivos elementales para poner en marcha el proyecto, además se asume que la red de fibra ótica hacia los nodos ya existe.

CANTIDAD	EQUIPO	PRECIO UNITARIO	PRECIO TOTAL	UBICACIÓN
5	CISCO 7200	$ 6,000	$ 30,000	Backbone
4	TARJETAS PA-GE	$ 200	$ 800	Backbone
4	TRANCEIVER	$ 70	$ 280	Backbone
4	JUEGO DE RADIO ENLACES	$ 750	$ 3,000	Backbone
2	CISCO 1700	$600	$ 1,200	Cliente
2	TARJETA WIC-1ENET	$100	$ 200	Cliente
2	JUEGO DE RADIO ENLACE	$400	$ 800	Cliente
TOTAL DE INVERSIÓN			**$ 36,280**	

Tabla 3.1 Presupuesto de proyecto

4.1 SIMULACIÓN DEL BACKBONE MPLS Y SERVICIO VPN

Para validar el funcionamiento de la red MPLS y la operatividad de la VPN, es necesario utilizar un programa de simulación de equipos CISCO. El programa debe ser capaz de soportar todas las aplicaciones de los equipos y permitir la captura de los paquetes, de esta forma elaborará un escenario muy cercano a la realidad. Dynamips es un programa de simulación de IOS de router CISCO que brinda la robustez y estabilidad que requerimos.

La demostración visual se la realizará configurando dos maquinas virtuales que representaran una matriz y una sucursal, La configuración se la realizará en el programa VMWARE que permite utilizar diferentes sistemas operativos como, todas las versiones de Windows y Linux.

4.1.1 SIMULADOR DYNAMIPS

Dynamips es un simulador de routers CISCO desarrollado por Christopher Fillot. Dynamips soporta las IOS de los routers 1700, 2600, 3600, 3700 y 7200. Este emulador no puede reemplazar un router real, simplemente es una herramienta para las personas que desean perfeccionar sus conocimientos para certificarse CCNA, CCNP o CCIE.

4.1.1.1 OBTENCIÓN DE DYNAMIPS

Dynamips es un programa de licencia libre, es decir el usuario que lo desee adquirir no debe pagar por los derechos de autor. Para adquirir este programa se lo puede bajar varios servidores que se encuentran en el Internet o ir a la pagina principal.

4.1.1.2 PLATAFORMAS QUE SOPORTA

El simulador soporta varias series de los enrutadores CISCO entre ellos tenemos:

- Serie 1700
- Serie 2600
- Serie 3600
- Serie 7200

Además permite la habilitación de diferentes tarjetas según la serie. En la parte inferior se detalla cada uno de ellos:

Serie 1700

- WIC-1T (1 puerto serial)
- WIC-2T (2 puertos seriales)
- WIC-1ENET (1 puerto ethernet)

Serie 2600

- NM-1E (1 puerto Ethernet)
- NM-4E (4 puertos Ethernet)
- NM-1FE-TX (1 puerto FastEthernet)
- NM-16ESW (Modulo de switch, 16 puertos)
- WIC-1T (1puerto serial)
- WIC-2T (2 puertos seriales)

Serie 3600

- NM-1E (1 puerto Ethernet)
- NM-4E (4 puerto Ethernet)
- NM-1FE-TX (1 puerto FastEthernet)
- NM-16ESW (1 modulo de switch Ethernet, 16 puertos)
- NM-4T (4 puertos seriales)

Serie 7200

- C7200-IO-FE (FastEthernet, solo slot 0)
- C7200-IO-2FE (2 puertos FastEthernet, solo slot 0)
- PA-FE-TX (FastEthernet)
- PA-2FE-TX (2 puertos FastEthernet)
- PA-4E (4 puertos Ethernet)
- PA-8E (8 puertos Ethernet)
- PA-8T (8 puertos Seriales)

- PA-A1 (ATM)
- PA-POS-OC3 (POS)
- PA-GE (GigabitEthernet)

4.1.1.3 MODO DE OPERACIÓN

Como la mayoría de los programas, Dynamips posee manual de uso que permite al usuario tener conocimiento de los comandos y la forma correcta de utilizarlo. El manual se lo puede descargar en la misma página donde se ofrece el programa, sin embargo en el anexo F se resume como utilizarlo.

4.1.2 SIMULADOR DE MAQUINAS VIRTUALES VMWARE

VMWARE es un programa de virtualización de ordenadores, cuando se ejecuta esta herramienta proporciona las mismas características que un ordenador físico. VMWARE se ejecuta sobre el sistema operativo del ordenador físico y permite arrancar varios ordenadores bajo el mismo *hardware*, es obvio suponer que las maquinas virtuales que se han creado pasan a un segundo plano al momento de procesar las aplicaciones.

4.1.2.1 REQUERIMIENTOS DEL SISTEMA

Para la validación de este proyecto se eligió VMWARE WORK-STATION v. 5, es la versión comercial que permite simular plataformas de PC x86. Los requisitos de sistema para utilizar este programa en un ordenador son:

COMANDO	OBJETIVO
Procesador:	Intel Celeron o superiores, ADM, Athon, Athon MP, Athon XP, Athon 64, Turion, Seprom.
Memoria RAM:	Mínimo 128 Mb.
Disco duro:	IDE o SCSI hasta 950 Gb 1 Gb de espacio libre como mínimo para cada maquina virtual.

Tabla 4.1 Requerimientos del sistema

4.1.2.2 SISTEMAS OPERATIVOS A SIMULAR

VMWARE permite simular una gama extensa de sistemas operativos desde las versiones de Windows, pasando por GNU-LINUX, hasta llegar a MAC OS.

A continuación se menciona las versiones mas utilizadas:

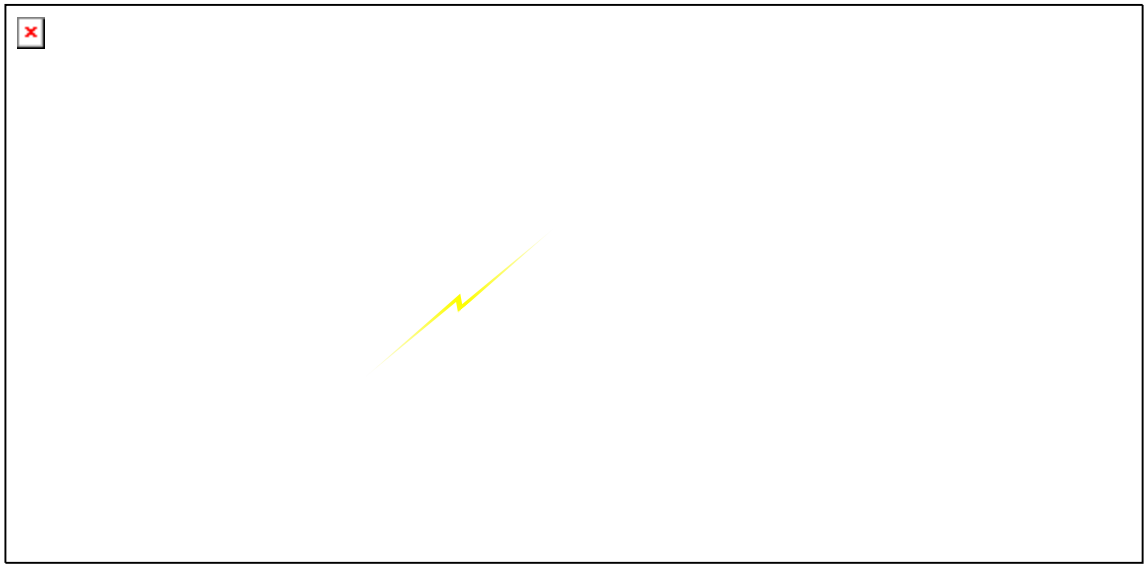
COMANDO	OBJETIVO
Windows	2003 *SERVER* XP HOME y PROFESIONAL 2000
GNU-LINUX	Centos X Ubunto X Mandraque

	Red Hat

Tabla 4.2 Tipos de Sistemas Operativos

4.2 CONFIGURACIÓN DEL BACKBONE MPLS

Antes de comenzar con la configuración de los dispositivos que intervienen en la red, es necesario definir las conexiones que van ha unir los enrutadores del backbone y los del cliente.



En el anexo F se explica detenidamente la estructura y funcionamiento de los comandos que se introducen en *DYNAMIPS*. Basándonos en el esquema de la figura 4.1 Se procederá a configurar la red.

CONFIGURACIÓN DEL ROUTER 7200

Serie del enrutador a utilizar

image=C:\Archivosdeprograma\Dynamips\images\IOS\ c7200-jk9s-mz.124-13a.bin

Ubicación y nombre del IOS de Cisco

ram = 128

Memoria disponible

CONFIGURACIÓN DEL ROUTER DE BORDE

[[ROUTER P]]

Nombre del enrutador

model = 7200

Modelo a utilizar

slot1 = PA-GE

Inserción de tarjeta Gigabit Ethernet en el Slot 1

slot2 = PA-GE

Inserción de tarjeta Gigabit Ethernet en el Slot 1

g1/0= PE1 g1/0

Conexión interface g1/0 del enrutador P con la interface g1/0 del enrutador PE1

g2/0= PE2 g1/0

Conexión interface g2/0 del enrutador P con la interface g1/0 del enrutador PE2

[[ROUTER PE1]]

model = 7200

Modelo a utilizar

slot1 = PA-GE

Inserción de tarjeta Gigabit Ethernet en el Slot 1

[[ROUTER PE2]]

model = 7200

Modelo a utilizar

slot1 = PA-GE

Inserción de tarjeta Gigabit Ethernet en el Slot 1

CONFIGURACIÓN DEL ROUTER DEL CLIENTE

[[ROUTER CE1]]

model = 7200

Modelo a utilizar

f0/0 = PE1 f0/0

Conexión interface f0/0 del enrutador CE1 con la interface f0/0 del enrutador PE1

F0/1= NIO_gen_eth:\Device\NPF_{EE3B1D21-D305-4A00-9BD4-2D7332684C94}

Conexión interface f0/1 del enrutador CE1 con la tarjeta de red de la Maquina Virtual 1

[[ROUTER CE2]]

model = 7200

Modelo a utilizar

f0/0 = PE1 f0/0

Conexión interface f0/0 del enrutador CE2 con la interface f0/0 del enrutador PE2

F0/1= NIO_gen_eth:\Device\NPF_{FE16D0BE-07B9-4D4C-A283-FBD5F525ACF6}

Conexión interface f0/1 del enrutador CE2 con la tarjeta de red de la Maquina Virtual 2

4.2.1 CONFIGURACIÓN DE ENRUTADORES DEl PROVEDOR

Los LSR son dispositivos que se encuentran en el núcleo de la red MPLS, los cuales tienen la función de procesar la información y determinar la mejor ruta hacia su destino. Los dispositivos que se encuentra en el núcleo de la red deben poseer mecanismos de respaldo para garantizar la operatividad del sistema.

Los protocolos de estado de enlace como OSPF y EIGRP se caracterizan por su rápida convergencia al momento de detectar una ruta como inalcanzable, por esta razón en muy común aplicar estos protocolos en redes que tienen redundancia.

4.2.1.1 HABILITACIÓN MPLS

Los enrutadores LSR se caracterizan porque en cada una de sus interfaces soportan tráfico con encapsulamiento MPLS, lo cual es necesario habilitar la función de conmutación de etiquetas en cada interface.

COMANDO	OBJETIVO
Router(config)# ip cef	Habilita la función de conmutación y envío propietaria de CISCO.
Router(config)# interface <tipo> <slot/puerto>	Permite ingresar a la configuración de la interface.
Router(config - if)# mpls ip	Habilita el envío de paquetes IPv4 con encapsulamiento MPLS.

Tabla 4.3 Comandos para habilitar MPLS en routers CISCO

Se debe tener en cuenta que al aplicar los comandos que se mencionó anteriormente solo se los ejecutaran sobre las interfaces que van a soporta IP-MPLS. Por ejemplo las interfaces de los enrutadores PE que se conectan al enrutador del cliente ó CE no se habilitaran la función MPLS.

4.2.1.2 PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS

Después de habilitar IP-MPLS sobre la interfaz específica es necesario definir el protocolo de distribución de etiquetas, como se analizó en la sección 1.3.1 existen tres tipos de protocolos LDP, TDP y RSVP.

COMANDO	OBJETIVO
Router(config - if)# mpls label protocol <ldp | tdp | both>	Configura el protocolo de distribución de etiquetas en una interfaz

Tabla 4.4 Comandos para habilitar Protocolos de Distribución

4.2.1.3 PROTOCOLO DE ENRUTAMIENTO

En la sección 4.2.1 se menciona la importancia de utilizar un protocolo de enrutamiento de estado de enlace en el área principal de la red. OSPF es el protocolo más utilizado debido a su estabilidad, rápida convergencia y sobre todo que es de arquitectura abierta, es decir pueden existir varios dispositivos conectados de diferentes fabricantes utilizando OSPF y trabajar sin problema.

COMANDO	OBJETIVO
Router (config)# router ospf <*process-id*>	Habilita en enrutamiento OSPF
Router (config - router)# network <*ip-address*> <*wildcard-mask*> area <*area-id*>	Define una interfaz en la cual se ejecuta OSPF y señala el área para aquella interfaz

Tabla 4.5 Comandos para habilitar Protocolos de Enrutamiento

4.3 CONFIGURACIÓN DE MPLS-VPN

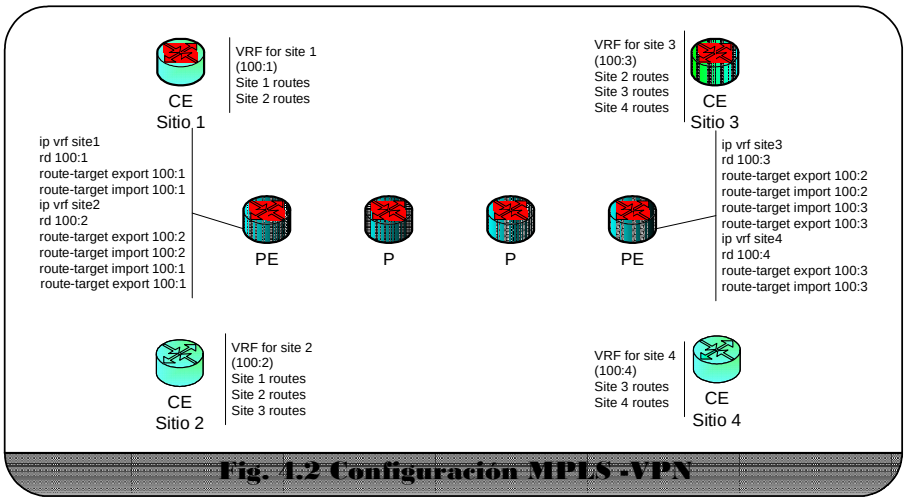


Fig. 4.2 Configuración MPLS -VPN

Para comprender la configuración y el funcionamiento de MPLS-VPN es necesario entender que cada vez que se cree una VPN se asociará a una o más tablas virtuales de enrutamiento denominado instancia virtual de envío y enrutamiento. Un VRF puede ser visto como un enrutador virtual, debido que se crea una tabla de enrutamiento y FIB independiente al proceso MPLS.

Cada vez que el enrutador del cliente envíe una paquete IP v4 hacia enrutador PE para ser enviado a través de la VPN, el dispositivo ubicado al borde del *backbone* MPLS colocará un prefijo de 64 bits como distintivo de la ruta. RD sirve para distinguir la dirección IP del cliente de esta forma evita la confusión con la dirección IP de otro cliente.

Cada VRF tiene asociado uno o más *Router Target*, atributo con el cual se marcan a los prefijos insertados en cada VRF, recibidos desde un CE o bien por rutas estáticas. De aquí en adelante cada PE seleccionará, de acuerdo a los RT pre-configurados a cada VRF, que prefijos VPN debe seleccionar e insertar o advertir.

Los parámetros que se configura para construir una VPN son los mismos que se mencionó anteriormente, los comandos que se mencionará a continuación solo se ejecutan en los enrutadores de frontera de la red MPLS.

COMANDO	OBJETIVO
Router(config)# ip vrf <nombre VRF>	Definir el nombre del enrutamiento virtual
Router(config-vrf)# rd <distinguidor de ruta>	Crear tablas de enrutamiento y envío
Router(config-vrf)# route-target import <routetarget-ext-community>	Crear una lista de importación de comunidades extendidas.
Router(config-vrf)# route-target export <routetarget-ext-community>	Crear una lista de exportación de comunidades extendidas.

Router(config-vrf)# interface <type> <slot/port>	Ingresar al modo de configuración de Interfaz.
Router(config-if)# ip vrf forwading <vrf-name>	Asociar la VRF a la interfaz que se conecta el cliente.

Tabla 4.6 Configuración Backbone MPLS - VPN

COMUNICACIÓN ENTRE PE LOCAL – PE REMOTO

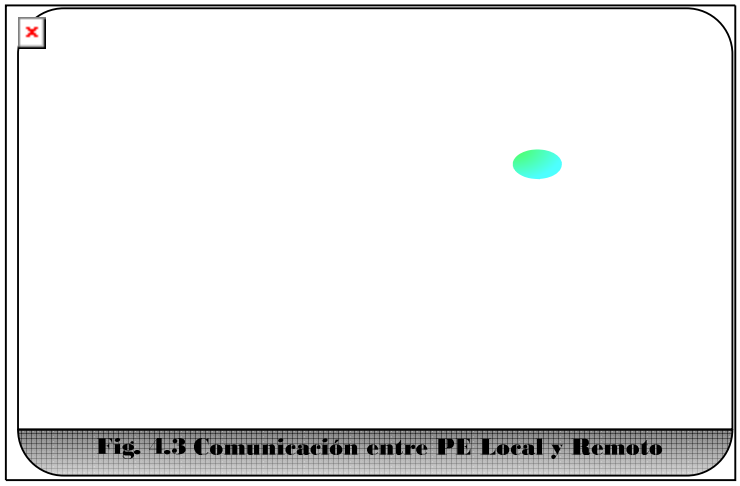


Fig. 1.3 Comunicación entre PE Local y Remoto

El protocolo puerta de enlace de frontera BGP, permite el intercambio de información entre las fronteras de una red. BGP es muy utilizado para conectar sistemas autónomos diferentes, sin embargo se lo puede utilizar como protocolo de interior. Al momento de configurar BGP se debe especificar el nombre y el sistema autónomo del vecino con el que establecerá comunicación.

COMANDO	OBJETIVO
Router(config)# router bgp *<AS número>*	Configura el proceso de enrutamiento IBGP con el número de

	sistema autónomo que será pasado a otros vecinos IBGP
Router(config-router)# neighbor <ipaddress | peer-group-name> remoteas <AS-number>	Especifica la dirección IP de un vecino con el cual se establecerá en enrutamiento BGP identificando el sistema autónomo al que pertenece
Router(config-router)# neighbor <ipaddress | peer-group-name> updatesource <loopback-interface>	Configura a BGP para que utiliza cualquier interface operacional en conexiones TCP
Router(config-router)# neighbor <ipaddress | peer-group-name> activate	Establece el emparejamiento con un Vecino especificado.

Tabla 4.7 Configuración PE

4.4 VALIDACIÓN DE LA IMPLEMENTACIÓN MPLS -VPN

Después de configurar toda la red MPLS del proveedor tanto en los enrutadores P como PE, es necesario realizar una secuencia de pruebas para certificar la operatividad del backbone.

Una vez que el backbone MPLS está operativo es factible revisar la conectividad entre los enrutadores PE´s y los enrutadores CE´s para culminar con la prueba de la aplicación entre la oficina principal del cliente y la sucursal.

4.4.1 OPERATIVIDAD DEL BACKBONE MPLS

Para validar el funcionamiento de la red MPLS es necesario chequear cada parámetro que se configuró en la sección 4.2.1.1, 4.2.1.2 y 4.2.1.3.

COMANDO	OBJETIVO
Router# Show mpls interfaces	Revisar las interfaces que pertenecen al dominio MPLS.

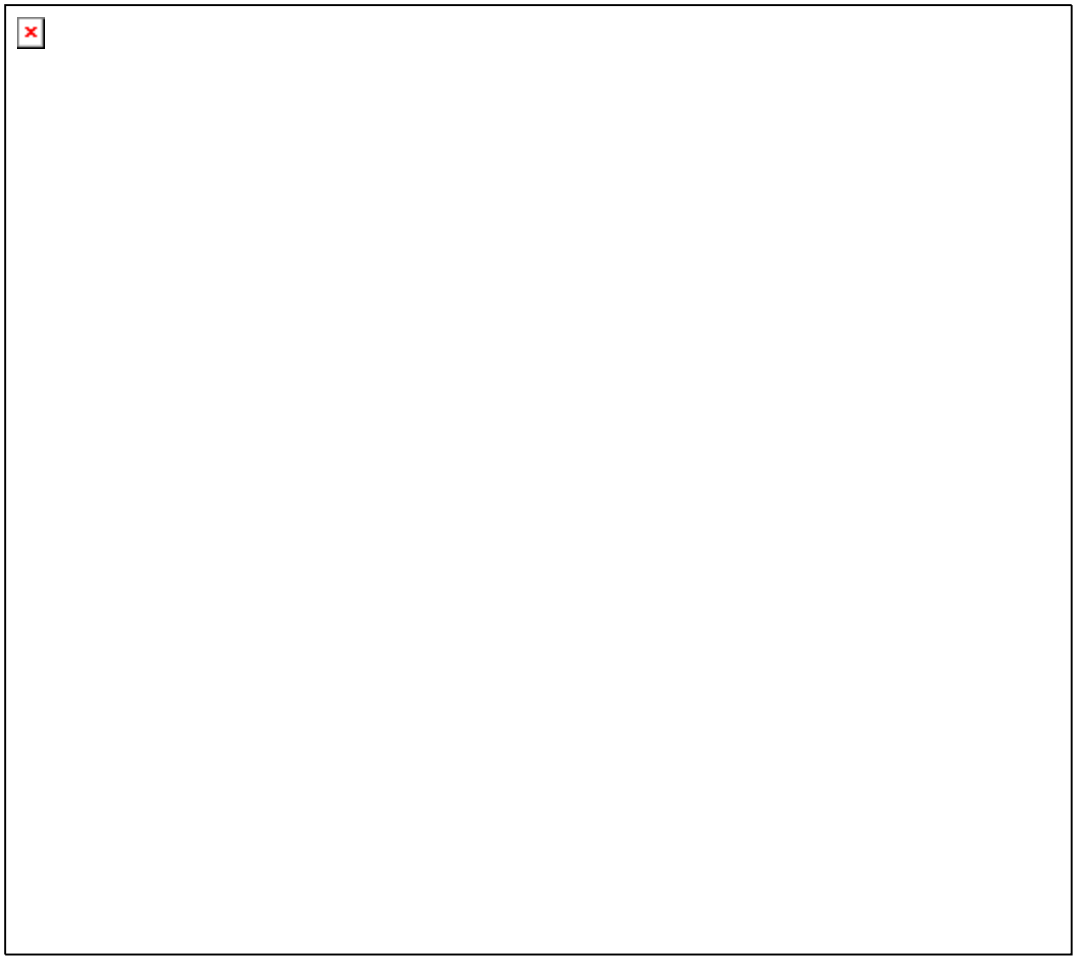
Tabla 4.8 Comando para revisar configuraciones de interfaces

Fig. 4.4 Muestra Configuración de Interfaces PE

En la figura (a) se observa que el enrutador P tiene habilitado en sus dos interfaces la función MPLS y en los equipos PE, figura b y c, solo están operando como MPLS las interfaces que se conectan al backbone.

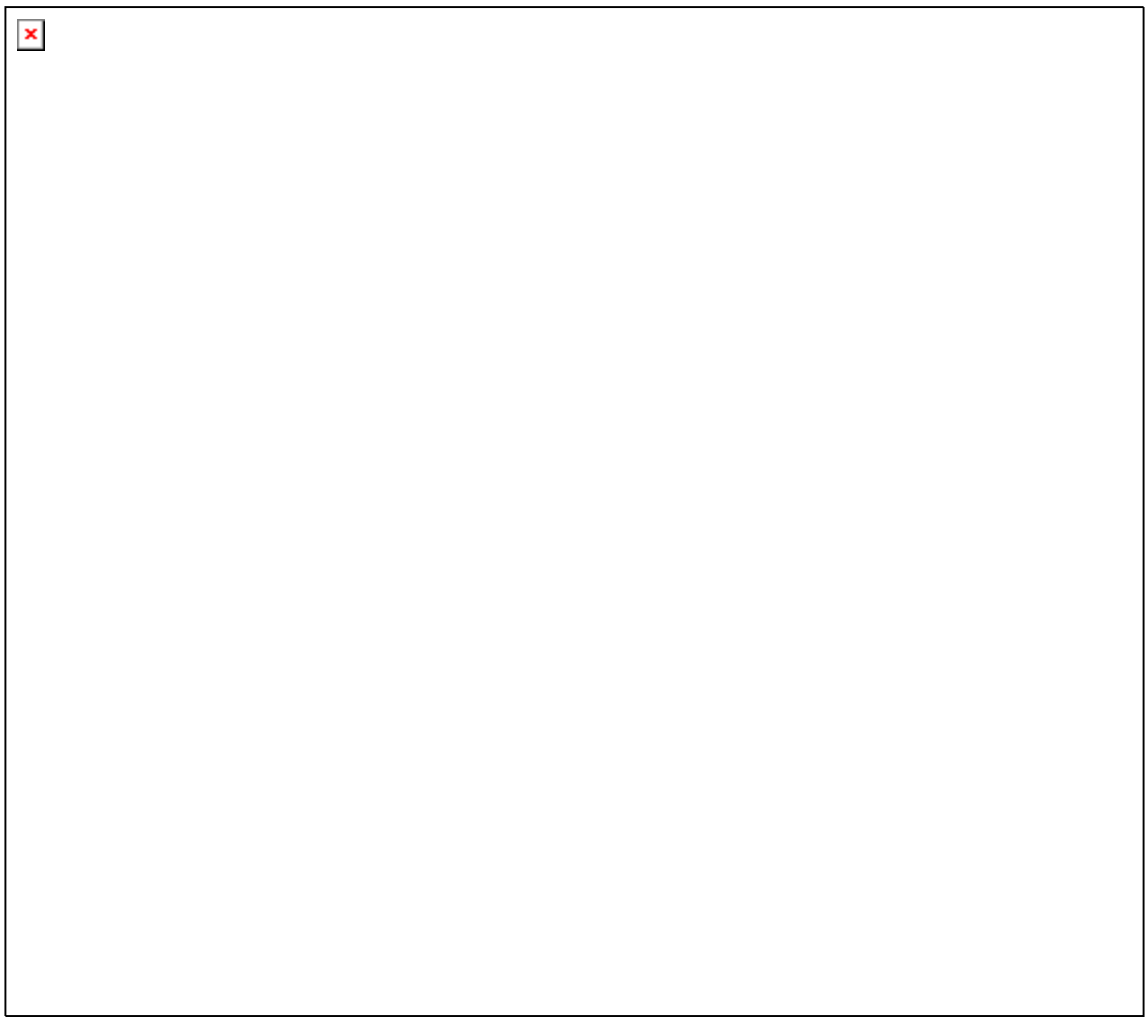
COMANDO	OBJETIVO
Router# Show mpls ldp neighbor	Muestra los vecinos con los que se mantiene comunicación por medio de paquete hello.

Tabla 4.9 Comando muestra configuración de LDP



COMANDO	OBJETIVO
Router# Show mpls forwarding-table	Presenta la tabla de enrutamiento para paquetes etiquetados.

Tabla 4.10 Comando muestra configuración de Tablas de enrutamiento



4.4.2 OPERATIVIDAD DEL SERVICIO VPN

La primera fase para validar la implementación de la VPN es demostrar que esta creado correctamente el túnel. En la figura 4.8 se ejecutó el comando *ping* a la dirección IP 192.168.1.1 que es el gateway de la red LAN en la sucursal. Sin embargo no se obtuvo respuesta debido que no se trata de un caso de enrutamiento dinámico.

Después se ejecutó el comando *ping* y se especifica que se trata de una VPN con el parámetro *VRF*, se coloca el nombre de la VPN en esta caso vpn1 y la dirección IP de la LAN en la sucursal. Como el túnel está creado correctamente se obtuvo respuesta a la petición de *eco.*

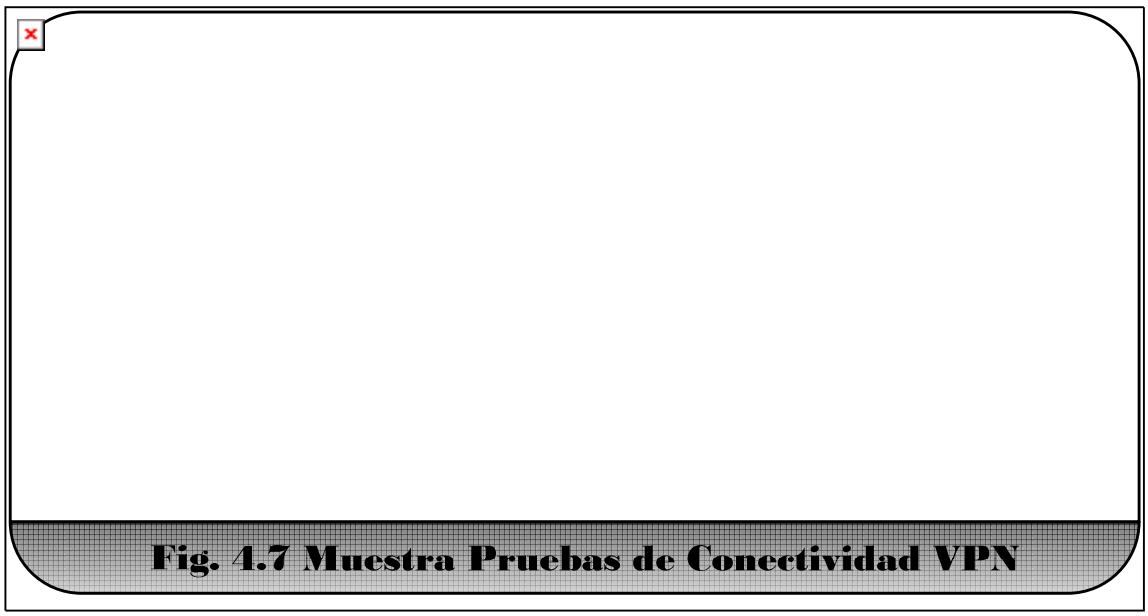


Fig. 4.7 Muestra Pruebas de Conectividad VPN

Después de validar el funcionamiento de la VPN entre los enrutadores de borde, el siguiente paso es realizar las pruebas de conectividad desde los equipos del cliente tanto en la sucursal como en la matriz.

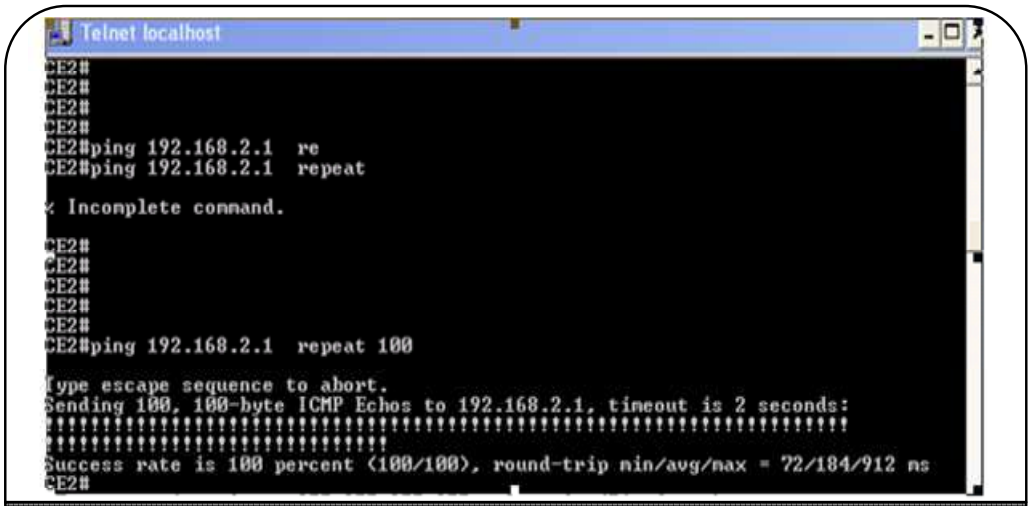


Fig. 4.8 Pruebas de eco entre enrutadores Matriz hacia Sucursal

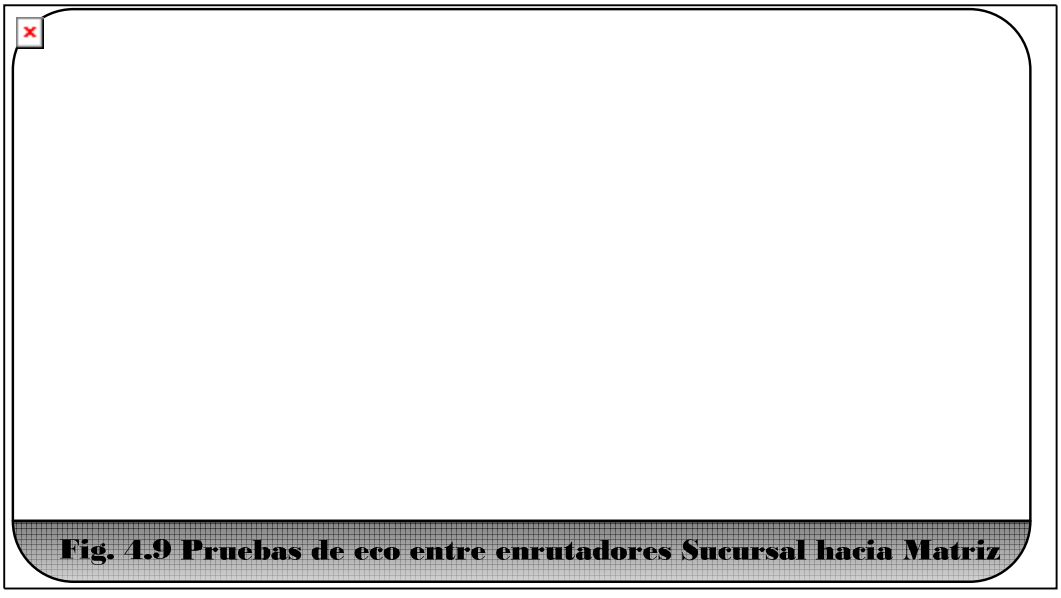
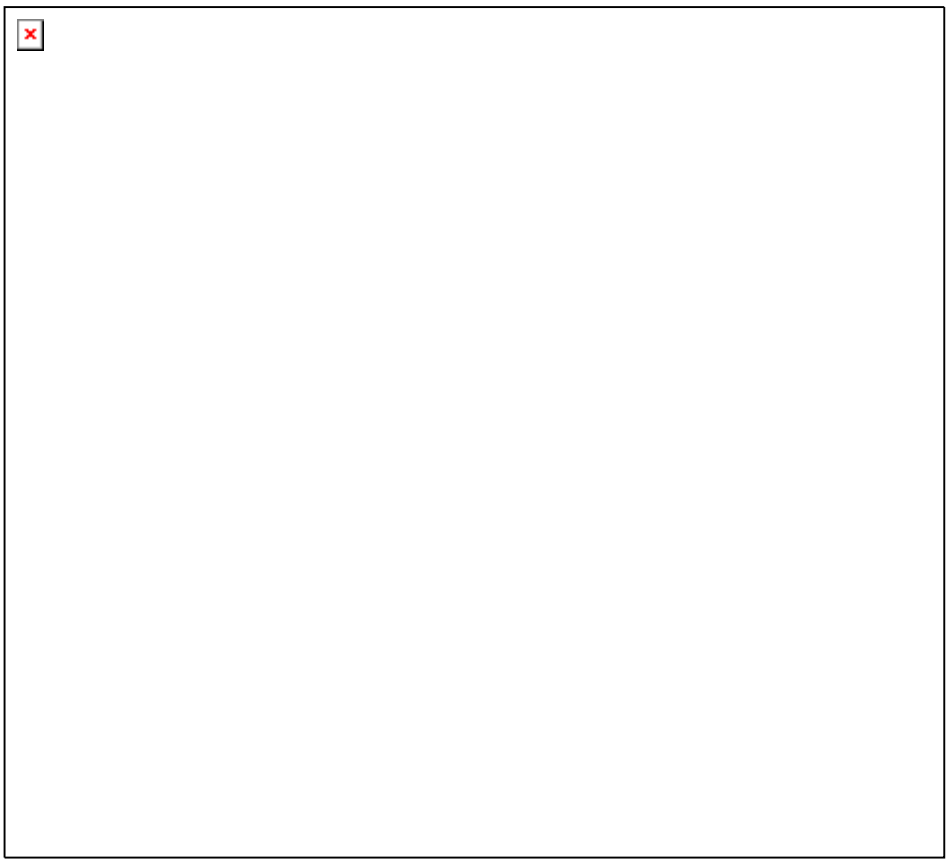
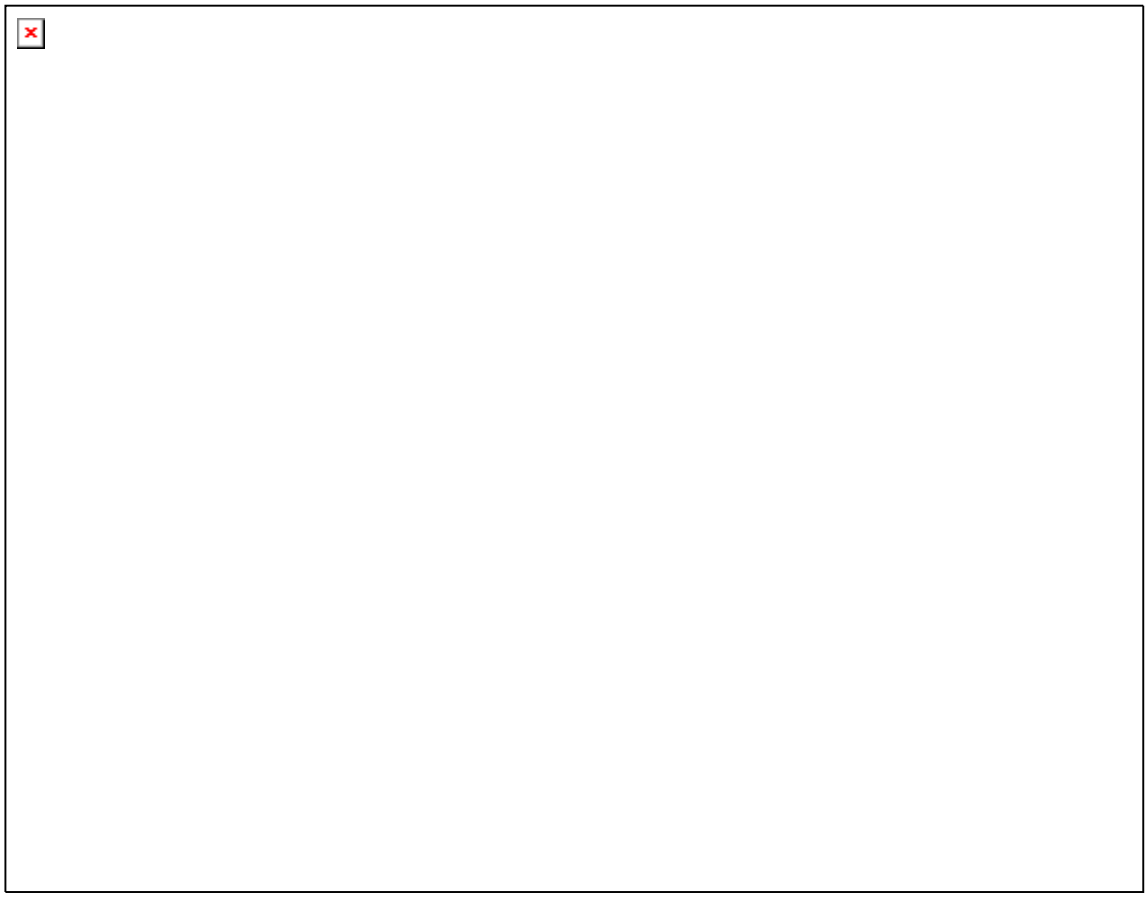


Fig. 4.9 Pruebas de eco entre enrutadores Sucursal hacia Matriz

Las pruebas de conectividad finalizan realizando peticiones de eco desde el Servidor de Archivos que esta ubicado en la matriz y la maquina que representa la sucursal.

Como se observa en la figura 4.8 y 4.9 existe conectividad desde el Servidor hacia la Sucursal y viceversa.





Por último ejecutará la transferencia de archivos para corroborar el funcionamiento de la aplicación entre los dos puntos.

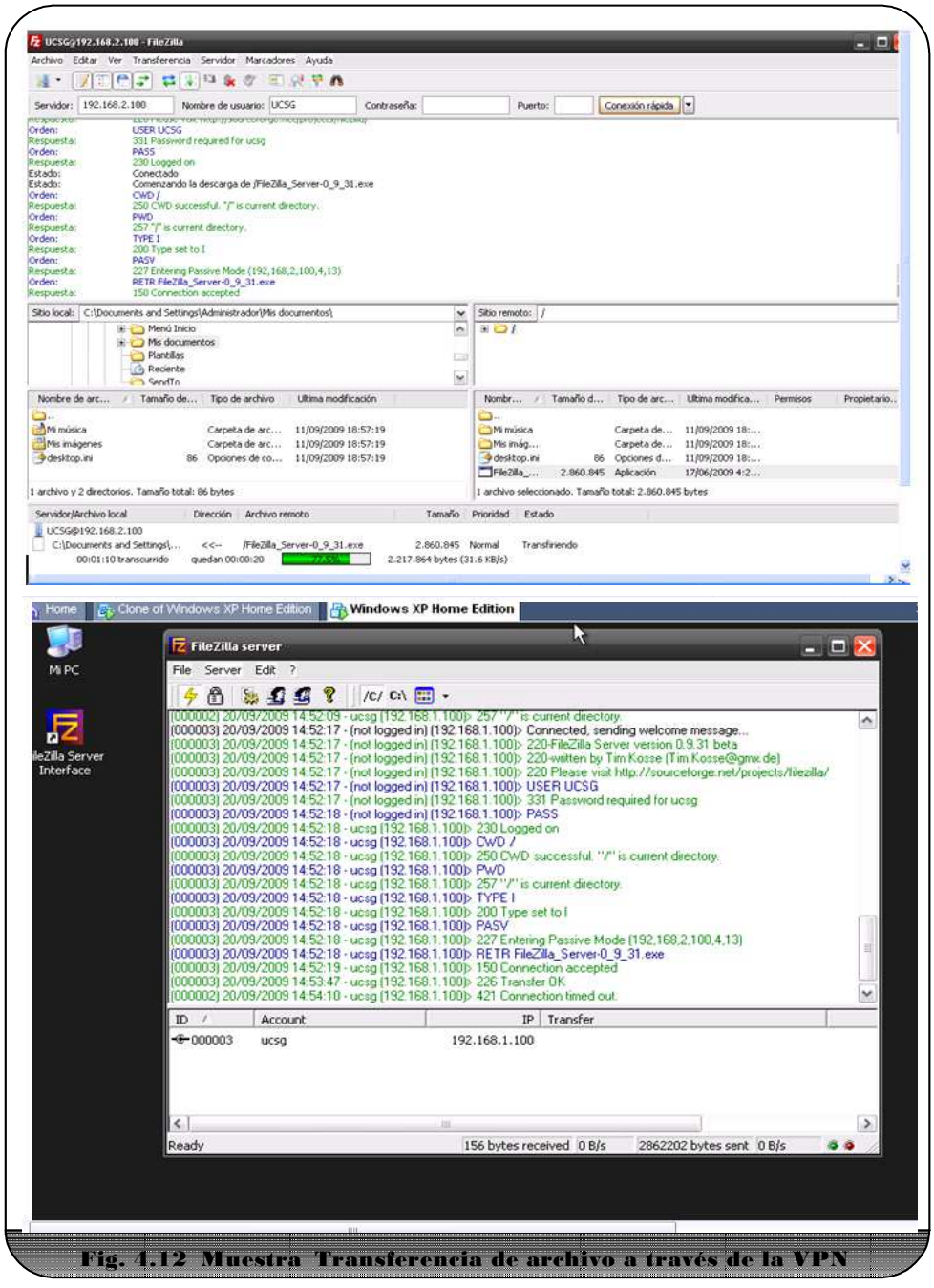


Fig. 4.12 Muestra Transferencia de archivo a través de la VPN

CONCLUSIONES

- La arquitectura MPLS se desarrolló para solventar las limitantes y defectos que poseen las redes Frame Relay y ATM, mejorando los tiempos de respuesta y la capacidad de soportar múltiples protocolos.

- La implementación de MPLS en las redes de los proveedores de servicio permite ofrecer servicios de valor agregado como: calidad de servicio (QoS), Ingeniería de tráfico y Redes Privadas Virtuales (VPN).

- Para crear una VPN sobre la nube MPLS no es necesario asignar una dirección pública para el enlace punto a punto, MPLS-VPN se basa en la instancia de enrutamiento y envío (VRF) lo que permite mantener el esquema de direccionamiento del cliente sin la necesidad de utilizar el enmascaramiento.

- Al aplicar una VPN para unir dos o más puntos es posible ejecutar aplicaciones como: correo electrónico, transferencia de archivos, ejecución de sistemas, acceso a escritorios remotos y utilización de elementos de red.

- Los resultados obtenidos en la implementación de la MPLS-VPN permite demostrar la vialidad del proyecto y el alcance de los objetivos planteados.

RECOMENDACIONES

- Antes de iniciar el estudio de MPLS es necesario que el lector posea conocimientos acerca de protocolos de enrutamiento, direccionamiento IP y conocimiento general de redes.

- Al momento de diseñar una red MPLS es recomendable conocer las características físicas, funciones y ubicación de cada dispositivo dentro de la red.

- Al configurar una VPN es necesario utilizar el mismo valor de RD y nombre de la VRF en todas las redes pertenecientes a una mismas VPN.

BIBLIOGRAFIA

- MPLS "Multiprotocol Label Switching"

  María Sol Canalis

  Dpto. Informática. Universidad Nacional del Nordeste. Corrientes. Argentina.

- Advanced MPLS Design and Implementation

CISCO NETWORK ACADEMY

- MPLS VPN—VRF Selection Based on Source IP Address

CISCO NETWORK ACADEMY

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/vrfselec.pdf

- Routing Basic

CISCO NETWORK ACADEMY

CCNA II

- Intermediate Routing and Switching

CISCO NETWORK ACADEMY

CCNA III

- WAN Technologies

CISCO NETWORK ACADEMY

CCNA IV

- Building Cisco Multilayer Switched Network

Volumen 1 y 2

CISCO NETWORK ACADEMY

CCNP

- Building Scalable Cisco Internetworks

Volumen 1 y 2

CISCO NETWORK ACADEMY

CCNP

- Implementing Secure Converged Wide Area Network

Volumen 1 y 2

CISCO NETWORK ACADEMY

CCNP

- Optimizing Converged Cisco Networks

Volumen 1 y 2

CISCO NETWORK ACADEMY

CCNP

- Tutorial Dynamips

http://dynagen.org/tutorial.htm

SUMARIO

Este trabajo de investigación está conformado por cuatro capítulos donde se detallan las características de la tecnología MPLS soportando VPN´s, explicado de forma sencilla de tal forma que llene las expectativas en las personas interesadas en el tema.

El primer capítulo brinda una breve reseña de los motivos por los cuales surge el diseño de MPLS, además muestra objetivos, conceptos, elementos que forman parte en la red y los protocolos utilizados para enviar los datos.

El segundo capítulo se centra en explicar las ventajas que propone la implementación de una VPN como solución para la interconexión de varios puntos a través de una infraestructura pública.

En el tercer capítulo se detallan los aspectos que se deben tomar en cuenta para diseñar un backbone MPLS como: topología, medio de interconexión y la elección de los dispositivos.

El cuarto capítulo se realiza la implantación y demostración del diseño de la topología de la red MPLS mediante la utilización del simulador Dynamip y la configuración de un Servidor FTP.

GLOSARIO

AS – Autonomous System – Sistema Autónomo.

ATM – Asynchronous Transfer Mode - Modo de Transferencia Asíncrono.

BGP – Border Gateway Protocol - Protocolo de puerta de frontera.

CE – Customer Equipment - Equipamiento en lado del Cliente.

CEF – Cisco Express Forwarding - Envío expreso de Cisco.

EIGRP – Enhanced Interior Gateway Routing Protocol - IGRP reforzado.

EXP – Campo “Experimental” Usado por MPLS para Calidad Servicio.

FEC – Forwarding Equivalence Class. Clase equivalente de envío.

FIB – Forwarding Information Base - Base de información de envío.

FTP – File Transfer Protocol - Protocolo de transferencia de archivos.

IOS – Internetworking Operative System - Sistema operativo de Inter-redes.

IP – Internet Protocol - Protocolo de Internet.

IS – IS – Intersystem – Intersystem - Protocolo de enrutamiento Inter - Sistemas.

ISP – Internet Service Provider - Proveedor de servicios de internet.

LAN – Local Area Network - Red de área local.

LDP – Label Distribution Protocol - Protocolo de distribución de etiquetas.

LER – Label Edge Router - Enrutador de frontera de etiquetas

LIB – Label Information Base - Base de información de etiquetas.

LSA – Link State Advertisement - Publicación de estado de enlace.

LSP – Label Switched Path - Ruta conmutada de etiquetas.

LSR – Label Switch Router - Enrutador conmutador de etiquetas.

MAC – Media Access Control - Control de acceso al medio.

MP-BGP – Multi Protocol Border Gateway Protocol - Extensión Multiprotocolo para BGP.

MPLS – Multiprotocol Label Switching.

P – Provider. Ruteador del proveedor.

PDU – Protocol Data Unit - Unidad de datos de protocolo.

PE – Provider Edge - Enrutador del frontera al proveedor.

RD – Route Distinguisher - Distinguidor de ruta.

RFC – Request For Comment - Petición para comentarios.

RIP – Routing Information Protocol - Protocolo de información de enrutamiento.

TCP/IP – Transport Control Protocol / Internet Protocol - Protocolo de control

de transporte / Protocolo de internet.

TOS – Type of Service - Tipo de servicio.

TTL – Time To Live - Tiempo de existencia.

UDP -- User Datagram Protocol - Protocolo de data grama de usuario.

VPN – Virtual Private Network - Red privada virtual.

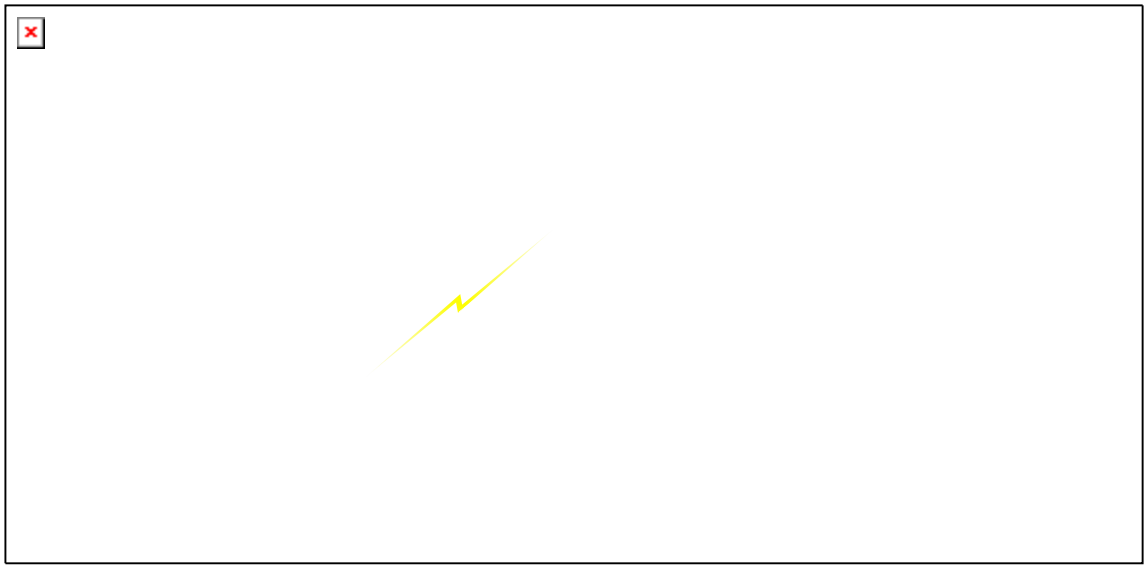
VRF – VPN Routing and Forwarding Instances - Instancias de enrutamiento y envío VPN.

WAN - Wide Area Network - Red de área amplia.

WIC – WAN Interface Card - Tarjeta de interfaz WAN.

ANEXOS

CONEXIÓN, DIRECCIONAMIENTO IP Y DESCRIPCIÓN DE LAS INTERFACES DE CADA DISPOSITIVO QUE FORMA PARTE DE LA RED



ANEXO A

CONFIGURACIÓN DE LOS DISPOSITIVOS DEL BACKBONE MPLS Y EL SERVICIO VPN

ANEXO A-1 Configuración Enrutador P

Proveedor#show runn

Building configuration...

Current configuration : 950 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Proveedor

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

```
!
ip cef
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.2 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 32.0.0.1 255.0.0.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
```

```
interface GigabitEthernet2/0
 ip address 33.0.0.1 255.0.0.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.2 0.0.0.0 area 0
 network 32.0.0.0 0.255.255.255 area 0
 network 33.0.0.0 0.255.255.255 area 0
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
!
```

```
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

Proveedor#
```

ANEXO A-2 Configuración Enrutador PE1

```
PE1#show running-config
Building configuration...

Current configuration : 1573 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
ip vrf vpn1
```

```
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
interface Loopback0
 ip address 10.10.10.3 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn1
 ip address 31.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 ip address 32.0.0.2 255.0.0.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 10.10.10.3 0.0.0.0 area 0
```

```
 network 32.0.0.0 0.255.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 neighbor 31.0.0.1 remote-as 200
 neighbor 31.0.0.1 activate
 neighbor 31.0.0.1 as-override
 neighbor 31.0.0.1 advertisement-interval 5
 no synchronization
 exit-address-family
!
!
```

```
no ip http server
no ip http secure-server
!
!
!
!
mpls ldp router-id Loopback0
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
```

login

!

!

end

PE1#

ANEXO A-3 Configuración Enrutador PE2

```
PE2#show running
Building configuration...

Current configuration : 1583 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
ip vrf vpn1
```

```
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn1
 ip address 34.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 ip address 33.0.0.2 255.0.0.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 network 10.0.0.1 0.0.0.0 area 0
 network 33.0.0.0 0.255.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.10.10.3 remote-as 100
 neighbor 10.10.10.3 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-community extended
```

```
 bgp scan-time import 5
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute connected
 neighbor 34.0.0.1 remote-as 200
 neighbor 34.0.0.1 activate
 neighbor 34.0.0.1 as-override
 neighbor 34.0.0.1 advertisement-interval 5
 no synchronization
 exit-address-family
!
!
no ip http server
no ip http secure-server
!
!
!
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
```

```
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
end

PE2#
```

ANEXO A-4 Configuración Enrutador CE1

```
CE1#show running
Building configuration...

Current configuration : 1062 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname CE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
mpls label protocol ldp
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.8 255.255.255.255
!
```

```
interface FastEthernet0/0
 ip address 31.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 31.0.0.2 remote-as 100
 !
 address-family ipv4
 redistribute connected
 neighbor 31.0.0.2 activate
 neighbor 31.0.0.2 advertisement-interval 5
 no auto-summary
 no synchronization
```

```
 exit-address-family
!
!
no ip http server
no ip http secure-server
!
!
!
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
!!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
```

line vty 0 4

login

!

!

end

CE1#

ANEXO A-5 Configuración Enrutador CE2

CE2#

CE2#show running

Building configuration...

Current configuration : 1065 bytes

!

version 12.4

service config

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname CE2

!

boot-start-marker

boot-end-marker

```
!
!
no aaa new-model
!
!
ip cef
!
!
mpls label protocol ldp
!
!
!
!
interface Loopback0
 ip address 10.0.0.9 255.255.255.255
!
interface FastEthernet0/0
 ip address 34.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 negotiation auto
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 34.0.0.2 remote-as 100
 !
 address-family ipv4
 redistribute connected
 neighbor 34.0.0.2 activate
 neighbor 34.0.0.2 advertisement-interval 5
 no auto-summary
 no synchronization
 exit-address-family
!
!
no ip http server
no ip http secure-server
!
!
!
!
```

```
mpls ldp router-id Loopback0
!
!
control-plane
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

CE2#
```

ANEXO B

TABLA DE ENRUTAMIENTO DE LOS ELEMENTOS DE LA RED

ANEXO B-1 Enrutador P

Proveedor# 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

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

C 32.0.0.0/8 is directly connected, GigabitEthernet1/0

C 33.0.0.0/8 is directly connected, GigabitEthernet2/0

10.0.0.0/32 is subnetted, 3 subnets

C 10.10.10.2 is directly connected, Loopback0

O 10.10.10.3 [110/2] via 32.0.0.2, 01:54:44, GigabitEthernet1/0

O 10.0.0.1 [110/2] via 33.0.0.2, 01:54:44, GigabitEthernet2/0

ANEXO B-2 Enrutador PE1

```
PE1#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
       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

C    32.0.0.0/8 is directly connected, GigabitEthernet1/0
O    33.0.0.0/8 [110/2] via 32.0.0.1, 01:46:14, GigabitEthernet1/0
     10.0.0.0/32 is subnetted, 3 subnets
O       10.10.10.2 [110/2] via 32.0.0.1, 01:46:14, GigabitEthernet1/0
C       10.10.10.3 is directly connected, Loopback0
O       10.0.0.1 [110/3] via 32.0.0.1, 01:46:14, GigabitEthernet1/0

PE1#show ip route vrf vpn1

Routing Table: vpn1
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

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

B 34.0.0.0/8 [200/0] via 10.0.0.1, 02:03:56

10.0.0.0/32 is subnetted, 2 subnets

B 10.10.10.8 [20/0] via 31.0.0.1, 02:05:03

B 10.0.0.9 [200/0] via 10.0.0.1, 02:02:06

B 192.168.1.0/24 [200/0] via 10.0.0.1, 02:02:06

B 192.168.2.0/24 [20/0] via 31.0.0.1, 02:05:03

31.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

B 31.0.0.0/24 [20/0] via 31.0.0.1, 02:05:03

C 31.0.0.0/8 is directly connected, FastEthernet0/0

PE1#

ANEXO B-3 Enrutador PE2

PE2#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

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

O    32.0.0.0/8 [110/2] via 33.0.0.1, 02:07:08, GigabitEthernet1/0
C    33.0.0.0/8 is directly connected, GigabitEthernet1/0
     10.0.0.0/32 is subnetted, 3 subnets
O       10.10.10.2 [110/2] via 33.0.0.1, 02:07:08, GigabitEthernet1/0
O       10.10.10.3 [110/3] via 33.0.0.1, 02:07:08, GigabitEthernet1/0
C       10.0.0.1 is directly connected, Loopback0

PE2#show ip route vrf vpn1
Routing Table: vpn1
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
       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
C    34.0.0.0/8 is directly connected, FastEthernet0/0
     10.0.0.0/32 is subnetted, 2 subnets
B       10.10.10.8 [200/0] via 10.10.10.3, 02:07:06
```

B 10.0.0.9 [20/0] via 34.0.0.1, 02:05:19

B 192.168.1.0/24 [20/0] via 34.0.0.1, 02:05:19

B 192.168.2.0/24 [200/0] via 10.10.10.3, 02:07:06

31.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

B 31.0.0.0/24 [200/0] via 10.10.10.3, 02:07:06

B 31.0.0.0/8 [200/0] via 10.10.10.3, 02:07:06

ANEXO C

PRUEBAS DE CONECTIVIDAD ENTRE LOS ELEMENTOS DEL BACKBONE MPLS

ANEXO C-1. Prueba de conectividad entre enrutador P y los enrutadores de borde.

Proveedor#ping 32.0.0.2 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 32.0.0.2, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 8/49/156 ms

Proveedor#ping 33.0.0.2 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 33.0.0.2, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/49/172 ms

Proveedor#

ANEXO C-2. Prueba de conectividad entre enrutador PE1 y los enrutadores que conforman la red.

PE1#ping 32.0.0.1 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 32.0.0.1, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 8/50/196 ms

PE1#ping 33.0.0.2 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 33.0.0.2, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 16/104/788 ms

PE1#

ANEXO C-3. Prueba de conectividad entre enrutador PE2 y los enrutadores que conforman la red.

PE2#ping 33.0.0.1 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 32.0.0.1, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!!!!!!!!!!!!!!!!!!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 8/50/196 ms

PE2#ping 32.0.0.2 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 32.0.0.2, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 16/104/788 ms
PE2#
```

ANEXO D

PRUEBAS DE CONECTIVIDAD ENTRE LOS DISPOSITIVOS DEL CLIENTE

ANEXO D-1. Prueba de conectividad entre CE1 y CE2

CE1#ping 192.168.1.1 repeat 1000

Type escape sequence to abort.

Sending 1000, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

!!

Success rate is 100 percent (1000/1000), round-trip min/avg/max = 80/224/464 ms

ANEXO D-2. Prueba de conectividad entre CE2 y CE1

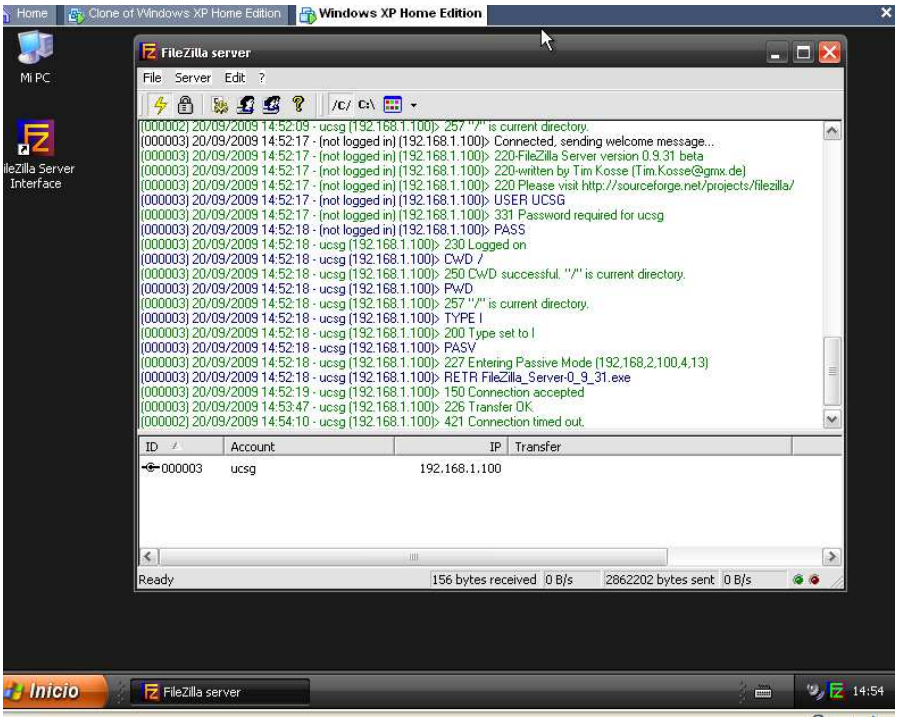
```
CE2#ping 192.168.2.1 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 80/224/464 ms
```

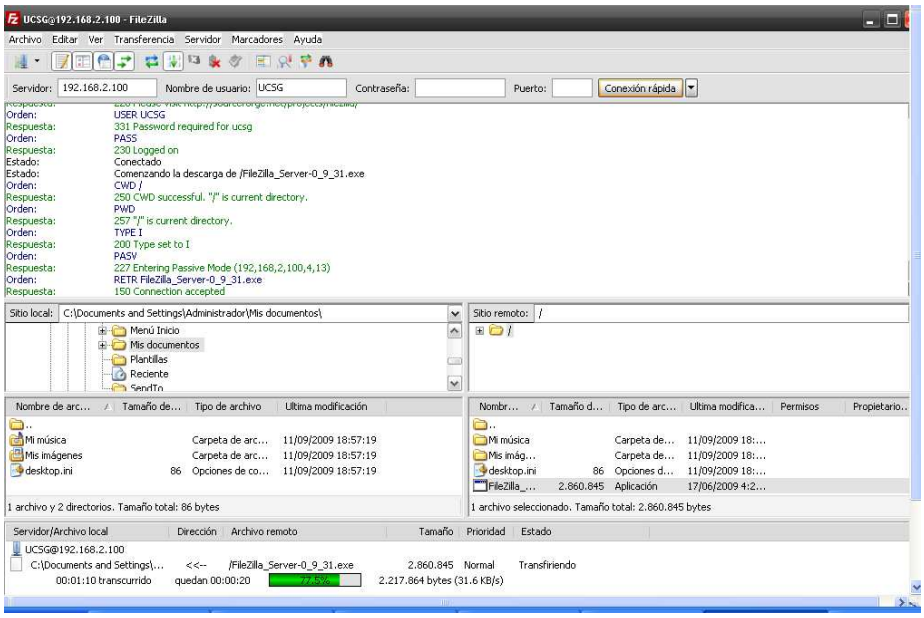
ANEXO E

PRUEBA DE APLICACIONES DEL SERVIDO FTP

ANEXO E-1. Registro del cliente en el Servidor FTP.



ANEXO E-2. Descarga de archivo desde el Servidor FTP.



ANEXO F

MANUAL DE USO DE DYNAMIPS

Dynamips es un emulador de routers CISCO desarrollado por Christopher Fillot. Dynamips soporta las IOS de los routers 1700, 2600, 3600, 3700 y 7200. Este emulador no puede reemplazar un router real, simplemente es una herramienta para las personas que desean perfeccionar sus conocimientos para certificarse CCNA, CCNP o CCIE.

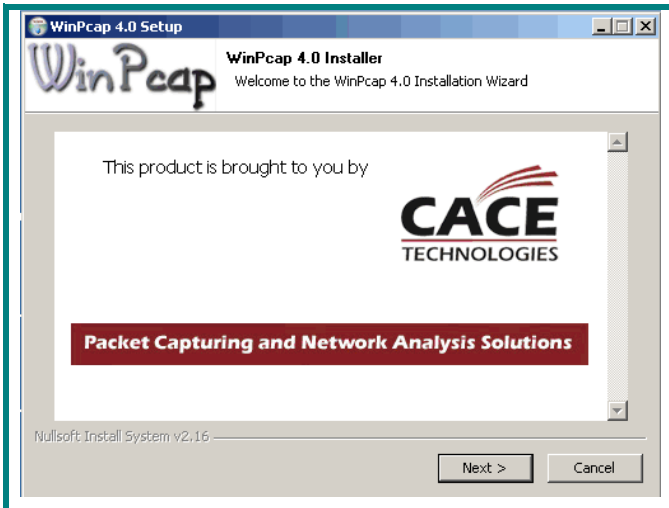
Requisitos mínimos del sistema

- Procesador Pentium 4 en adelante
- Memoria RAM 512Mbyte
- Disco Duro de 80 Gbyte
- Mouse y teclado
- Monito CRT 15”
- Sistema Operativo Windows o Gnu/Linux

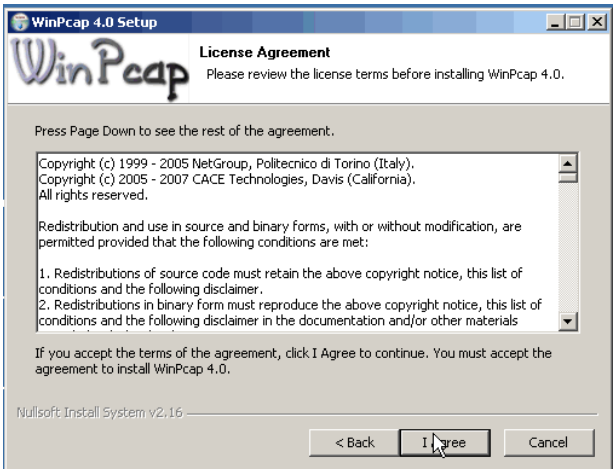
Instalación

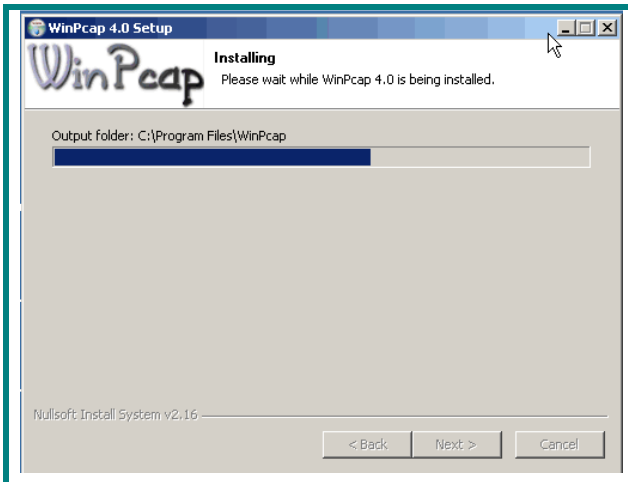
1. Ejecutar el instalador de WinPcap_4_0

2. Se abre la ventana de instalación y se realizan los siguientes pasos:

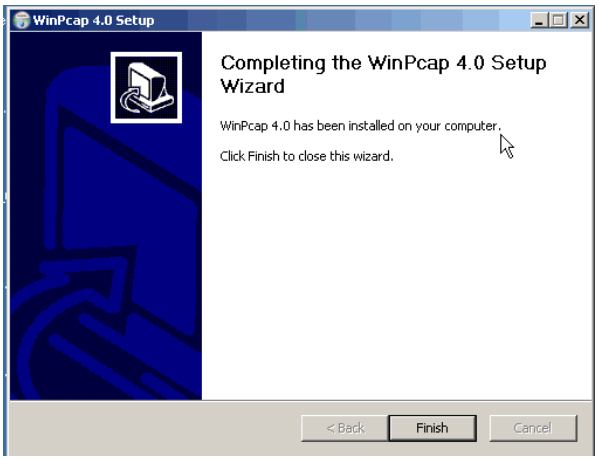


Click izquierdo en el botón Next

	Aparece una ventana de bienvenida y nos pregunta si deseamos continuar con la instalación. Hacemos Click en el botón NEXT.
	La ventana a la derecha nos presenta los términos de uso del software. Confirmamos nuestro acuerdo aceptando en el Botón I AGREE

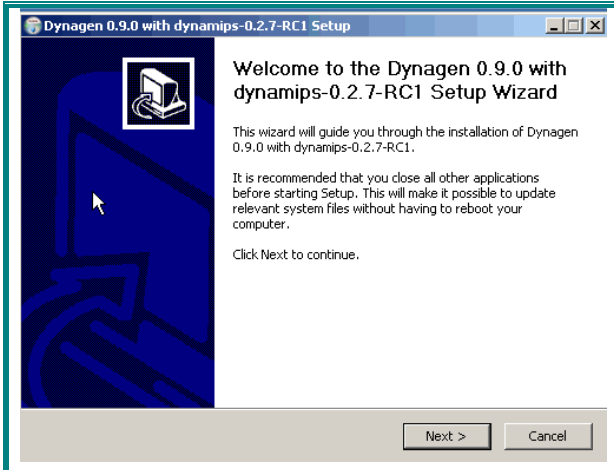
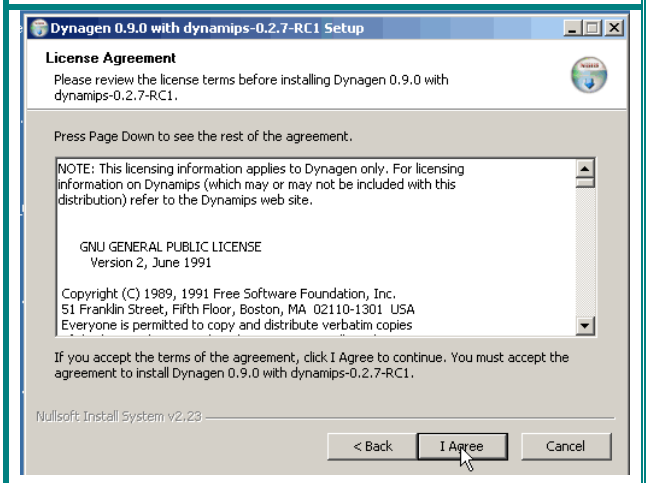


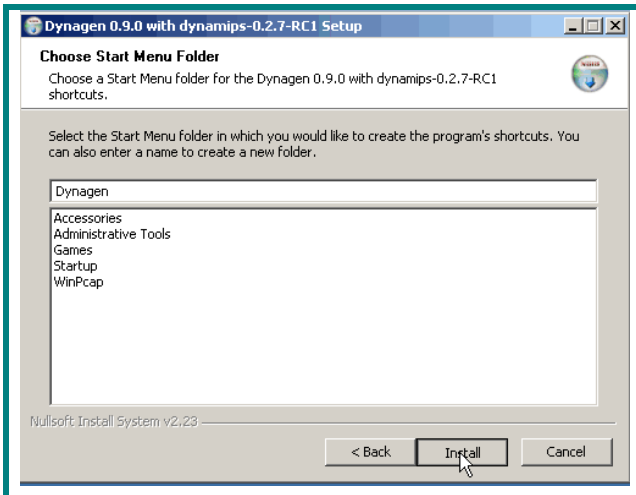
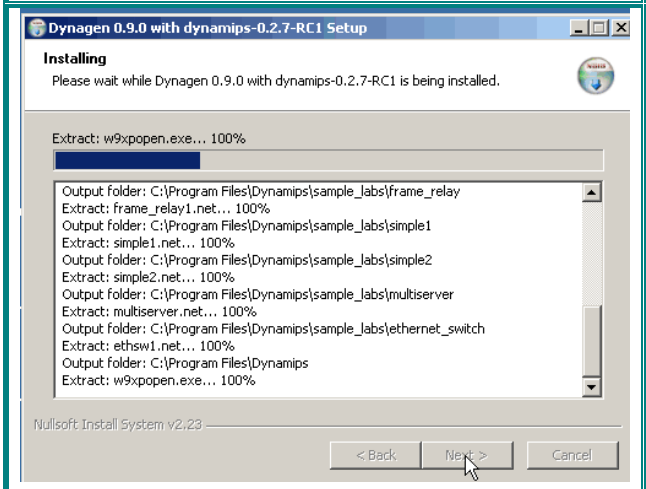
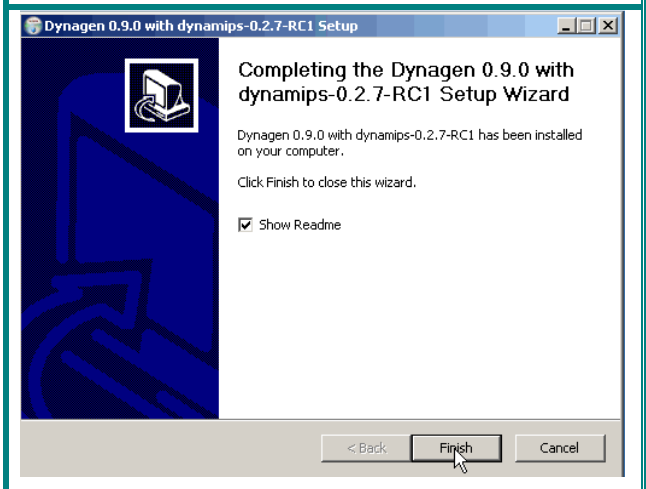
La ventana presenta el proceso de instalación de los archivos que se necesitan que funcione WinPcap.



La ultima ventana indica que todos los componentes fueron instalados sin inconvenientes, damos Click en el botón FINISH

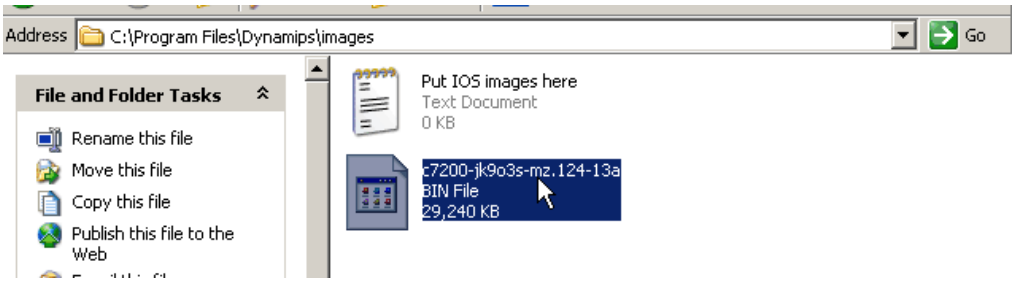
3. Una vez instalada la interfase de texto Dynagen, ejecutamos el instalador de Dynamips. Además procedemos a realizar las siguientes acciones:

	Tenemos la ventana de bienvenida de Dynamips, procedemos hacer Click en NEXT
	Aparece la ventana de dialogo acerca de las condiciones de uso del software, aceptamos los términos en el botón I AGREE.

	Hacemos Click en INSTALL
	Empieza a instalar los archivos necesarios para ejecutar Dynamips.
	Por último tenemos la ventana de finalización.

Donde guardar IOS

Si utilizas sistema operativo Windows, se debe colocar las imágenes en el siguiente directorio C:\archivo de programa\Dynamips\images. En caso que desee ubicar la carpeta de las IOS en otro lugar debes configurara la ruta en el ejercicio del laboratorio.



Como configurar nuestra red

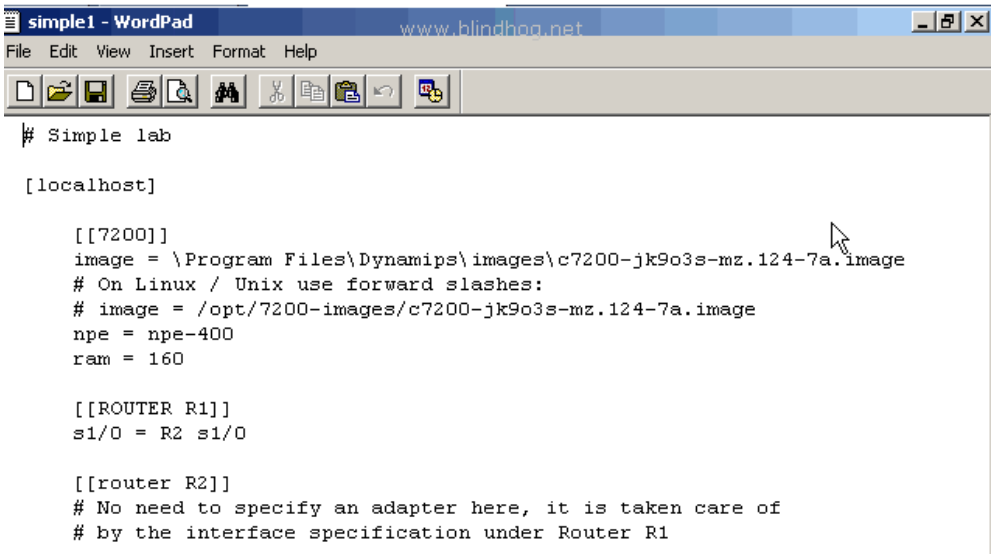
Después de instalar el Dynamips aparecerán unos iconos en nuestro escritorio como se aprecia en la siguiente figura.

A. Ingresamos a la carpeta Dynagen Samples Labs

B. Abrimos la carpeta Samples 1

C. Damos Click derecho sobre siguiente icono

D. Elegimos la opción Abrir con y escogemos WordPad



Simple lab: Es el titulo de nuestro laboratorio. Hay que tener en cuenta que cada línea que empiece con el signo numeral #, significa que es un comentario o recordatorio.

[localhost]: Esta línea especifica en que host se va ejecutar el simulador Dynamips. En este caso se va ejecutar Dynamips en la misma máquina donde está instalado. Si deseamos correr el simulador desde otra máquina que no sea la nuestra es necesario que este en red y colocar el nombre del host o la dirección IP.

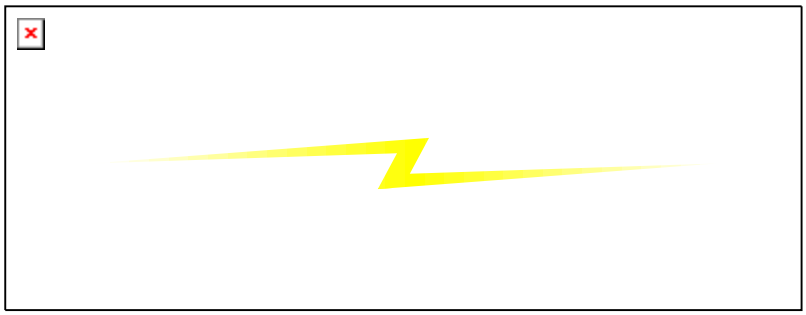
[[7200]]: Esta línea indica que los comandos que se mencionan a continuación se guardara en las características del router 7200.

Image=\Archivo de programa\Dynamips\images\.....bin: Indica que la imagen del router 7200 esta almacenada en esa dirección para que emule las características de dicho dispositivo.

npe = npe-400 ; ram = 160: Estas dos líneas son por defecto.

[[router R1]]: Nos indica que el nombre de nuestro router es R1 y los siguientes comandos van ha ser almacenados para el router 1 R1

s1/0 = R2 s1/0: Esta línea especifica cómo van a estar conectados nuestros router.



[[router R2]]: Indica que todo comando que se mencione debajo de esta línea se almacenara en R2

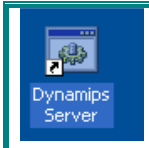
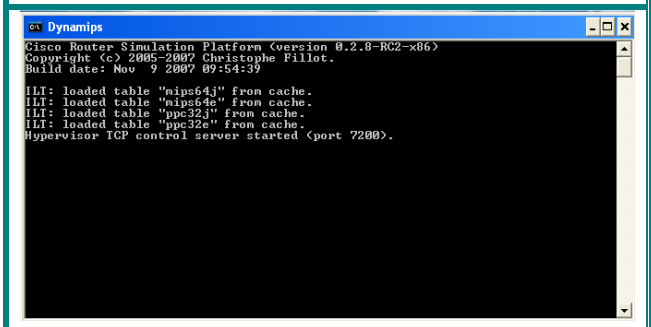
No need to specify an adapter here, it is taken care of

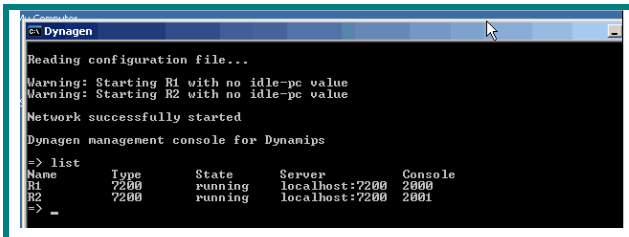
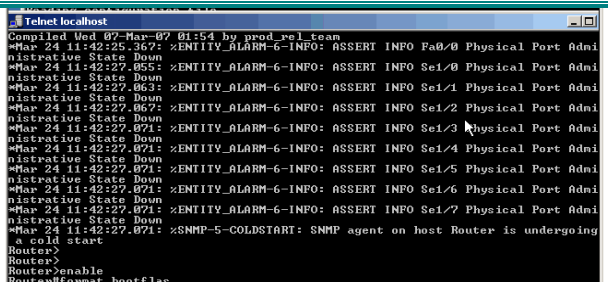
by the interface specification under Router R1

Estas últimas líneas son un comentario que significa lo siguiente “No es necesario especificar una conexión en el router R2, ya que se indico la conexión en el R1”

Nota: En este momento tenemos la configuración o esquema de nuestra red. En resumen, trabajaremos con dos router 7200 y que van estar conectados a través de la seria 1/0 de cada uno.

Empezar a usar Dynamips

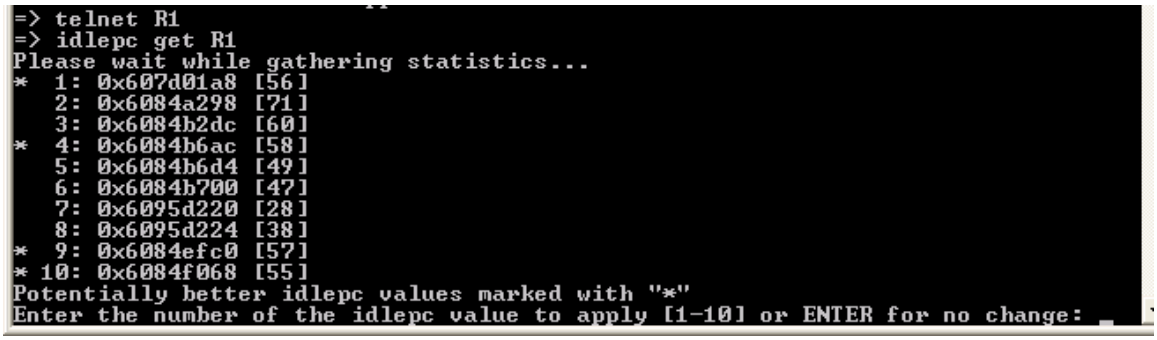
	Damos doble Click con el botón izquierdo sobre el icono de Dynamips Server
	Aparecerá una ventana en modo DOS. Durante la utilización de Dynamips no hay que cerrar esta ventana.
	Damos doble Click izquierdo sobre el icono simple 1

	Aparece la ventana de Dynagen, en la cual podemos ingresar a nuestros router utilizando el comando Conect o telnet y el nombre del router. Al ejecutar telnet o Conect el uso del procesador y memoria llegan hasta el 100% de su capacidad.
	Como podemos observar ingresamos al router R1, y la apariencia de la pantalla de configuración es idéntica como si estuviéramos utilizando un router real. Hacemos hincapié que en este momento el uso de la maquina esta al 100%.

Utilización de recursos

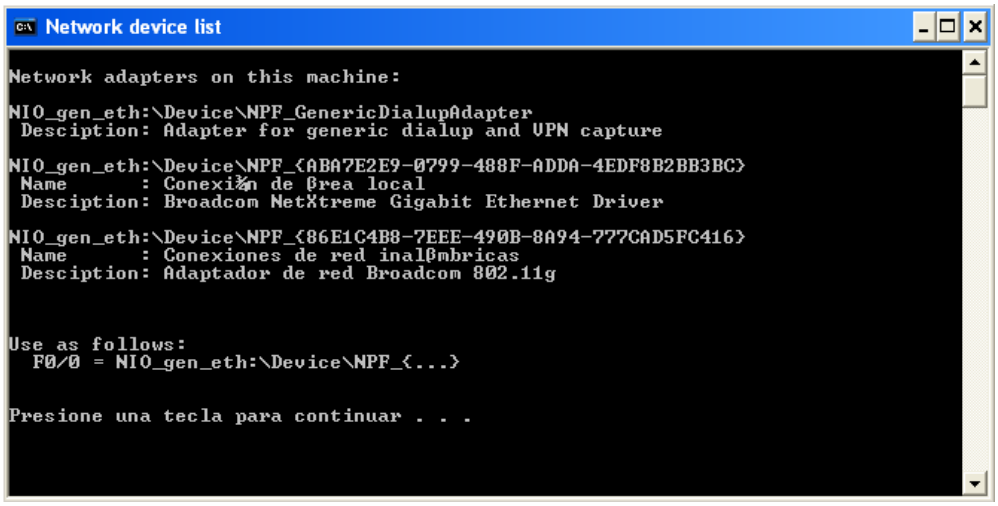
Dynamips usa una buena cantidad de RAM y de capacidad del CPU con el fin de emular los routers, puede llegar a consumir el 100% de los recursos de la PC. Para evitar este inconveniente se ejecuta una herramienta muy importante como idelpc.

En la ventana de Dynagen, ejecutamos el comando idlepc get R1 y elegimos uno de los valores que nos recomienda la maquina en este caso el 1. Guardamos el cambio con el comando idlepc save R1 db.



Interactuar con el mundo real

Dynamips aparte de ser una herramienta poderosa para simular redes con router cisco, nos permite crear un bridge o puente de una interface del router simulado con la interface de la tarjeta de red de nuestra PC. Con esto podemos switch u otras PCs para extender nuestra red.



Damos doble Click sobre el icono Network Device List y aparecerá la pantalla de arriba.

Aparece la tarjeta de red y la tarjeta inalámbrica que posee mi PC de prueba.

F0/0 = NIO_gen_eth:\Device\NPF _{ABA7E2E9-0799-488F-ADDA-4EDF8B2BB3BC}

Captura de paquetes

Dynamips/Dynagen nos permite capturar los paquetes que se envía a través de las interfaces virtuales, usando Sniffer como tcpdump, wireshark u otro software que pueda leer el archivo de formato de captura libpcap.

Ejemplo

Vamos a utilizar dos router 3660, los cuales le colocamos una tarjeta serial en el slot 2. Se van a comunicar por medio de la serial 2/1.

[localhost]

[[3660]]

image=C:\Archivos de programa\Dynamips\images\IOS\3600\c3660-is-mz.121-6.bin

ram = 160

idlepc = 0x60288028

[[ROUTER Carol]]

model = 3660

slot2 = NM-4T

s2/1 = Edu S2/1

[[ROUTER Edu]]

model = 3660

slot2 = NM-4T

Configuración:

Router Carol:

Serial 2/1: 10.10.10.1 255.255.255.0 clock rate 1200

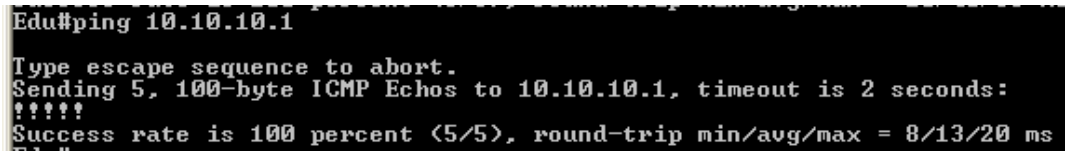
Router Edu:

Serial 2/1 10.10.10.2 255.255.255.0

En la ventana de administración de Dynagen colocamos el siguiente comando.

- capture Edu s2/1 ucsg.cap HDLC

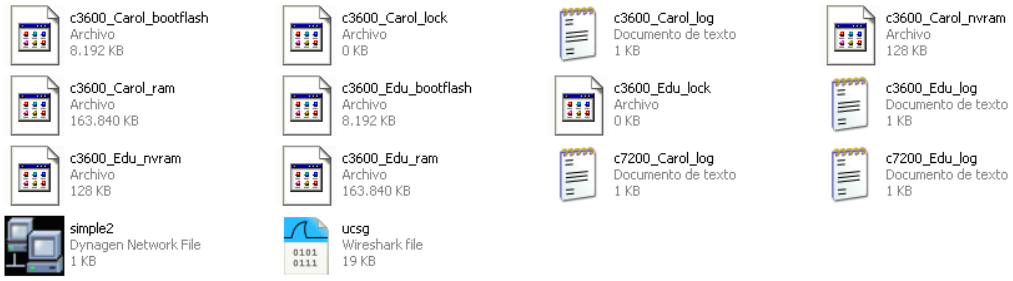
Para demostración, realizamos prueba de conectividad PING.



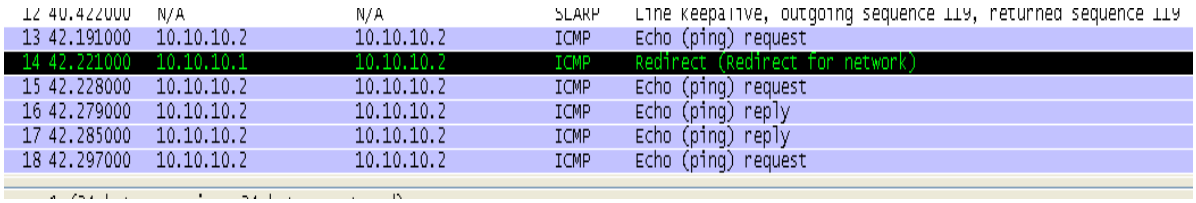
En la siguiente captura de pantalla nos podemos dar cuenta de dos cosas muy importantes:

1. Utilizamos la aplicación wireshark

2. Se genero un icono con el nombre de ucsg.cap



Damos doble Click sobre el Icono UCSG.CAP y nos aparecerá lo siguiente



La figura muestra que se realizaron peticiones de eco a la dirección 10.10.10.1.