c/marzo/ hernández burgos

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL BASADA EN MULTICAST CON MPLS

T E S I S

Que para obtener el Título de
INGENIERO EN TELECOMUNICACIONES

P r e s e n t a

NARCIZO HERNÁNDEZ BURGOS

DIRECTOR DE TESIS: ING. RODOLFO ARIAS VILLAVICENCIO

Marzo 2007

Dedicado a:

Dios, por darme la posibilidad de existir, por ser mi guía espiritual y estar conmigo en las buenas y en las malas, por el refugio que en ti he encontrado y la oportunidad que me das de vivir un día más,

A mis padres Maria Guadalupe Burgos Ramírez y Francisco Hernández Diego, por haberme guiado en mi camino, por darme las herramientas necesarias para llegar a este punto tan importante de mi vida, por enseñarme que las cosas buenas de la vida se logran con esfuerzo y dedicación, por la educación que me han dado, el esfuerzo conjunto en esas madrugadas y esas noches de trabajo, gracias por su amor y comprensión, quiero que sepan que siempre los llevaré en mi mente y en mi corazón,

A mi hermana Edith, por ser mi confidente, mi mejor amiga, y una persona excepcional de la que siempre he aprendido muchas cosas buenas de la vida, porque tengo tantas cosas que aprender de ti, gracias por tu apoyo incondicional,

A mi esposa Verónica, mi compañera de la vida, espero seguir contando con tu motivación y apoyo por siempre, gracias por existir y darme la oportunidad de amar y ser correspondido.

A mis amigos, por compartir conmigo tantos momentos tan agradables e irrepetibles, gracias por su amistad, en fin, años maravillosos imposibles de olvidar.

A Rodolfo Arias, mi asesor de tesis, gracias por aguantarme tanto tiempo, aquí esta el fruto del trabajo realizado, Al fin.....

Narcizo Hernandez Burgos

INDICE

INTRODUCCION

CAPITULO 1 INTRODUCCION

1.1 Antecedentes

La rapidez con que ha aumentado la demanda de acceso a Internet y el consecuente desarrollo de la Intranet, así como la necesidad de comunicarse por este medio, ha propiciado que las empresas requieran un servicio más robusto de interconexión entre dependencias que se encuentran dispersas por toda la geografía o en lugares distantes de la República Mexicana, utilizando el Protocolo de Internet (IP).
Estos factores demandan a las compañías minimizar los costos de conectividad y mantenimiento de red, ofrecer acceso a través de las redes de área local (LAN) y red de área extensa (WAN) a diferentes usuarios que se encuentran alejados territorialmente facilitando así la conectividad a Internet.
La principal consecuencia de este crecimiento es una combinación de interconectividad en la red pública a nivel WAN y la difusión de las interfaces de cliente-servidor (haciendo referencia a los navegadores de Internet), así como el uso de esta tecnología aplicada a la comunicación interna (Intranet). Cada vez con más frecuencia, las empresas trasladan a su LAN diversas aplicaciones y herramientas para cumplir sus objetivos. Dichas redes, por tanto, deben expandirse sobre una WAN para que de esta manera logren comunicarse a distancia entre ellas, con interredes y además con usuarios móviles.
Actualmente las empresas desean aumentar el éxito de su negocio incorporando a sus clientes, proveedores y socios a través de Internet, ya que el tráfico específico de aplicaciones se transmite cada vez con más frecuencia por medio de la tecnología TCP/IP (incluyendo datos, voz y vídeo).
Nuestro objetivo es incorporar estas tendencias a la tecnología de las Redes Privadas Virtuales (VPN's) las cuales proporcionan un servicio robusto y propicio entre la conectividad pública de los sitios de Internet y la retransmisión totalmente controlada de servicios de voz, video y datos.
La oferta se basa en estándares para proporcionar Redes Privadas Virtuales (VPN), basándonos en el protocolo de Multi-envío IP (Multicast), y además en la tecnología de Switcheo por etiquetas (MPLS).

1.2 Planteamiento del problema

El crecimiento constante de las empresas dedicadas a la capacitación de personal, exige una mayor presencia a lo largo del país, por lo que es necesario crear nuevos centros de capacitación, contratar el mobiliario necesario, invertir en la implementación de tecnología, desplazar al personal capacitado, cubrir gastos de viáticos, transporte, alimentos, hospedaje, entre otros factores.
Por tanto, surge la necesidad de optimizar los recursos haciendo uso de los avances tecnológicos a nivel de redes de telecomunicaciones, con el propósito de cubrir mayores áreas del territorio nacional sin la necesidad de desplazar al personal por el interior de la República Mexicana.
En este proyecto de tesis abordamos un tema muy específico, una problemática actual que está relacionada con la expansión de una empresa dedicada a la capacitación de

personal que ya cuenta con la infraestructura necesaria, y además, tiene presencia a lo largo del territorio nacional, en especifico, en aquellas localidades donde se encuentra la mayor concentración de la población, tal es el caso de la CD de México, Guadalajara y Monterrey.

1.3 Objetivo del proyecto de tesis

Implementar una red que aumente la interconectividad entre sitios mediante redes virtuales (VPN), el acceso de múltiples usuarios a información desde diversos puntos de una red con el mínimo uso de los recursos de la misma (Multicast), y una administración adecuada de la información enviada a los usuarios (MPLS). Así mismo y como consecuencia de la implementación de las nuevas tecnologías en la red, disminuir los gastos ocasionados por traslados, hospedajes y alimentación del personal de una empresa dedicada a la capacitación.

1.4 Límites y alcances del trabajo

La interacción de las tecnologías VPN, Multicast y MPLS está encaminada a resolver el problema de implementación, la cual permitirá a los usuarios recibir o transmitir, dependiendo del caso, información de una manera más eficaz y transparente.
Como una consecuencia de la implementación, la empresa podrá tener la capacidad de realizar conferencias a diferentes puntos de la República sin la necesidad de agotar en determinado momento los recursos con los que cuenta su red, esto nos permitirá obtener resultados a corto plazo en cuanto a capacitar a sus empleados, además de la disminución de costos y de recursos, sin tener que cambiar su infraestructura.
La trascendencia de este proyecto traerá consigo para la Empresa beneficios de tipo económico, disminución de los tiempos de aprendizaje de los recursos que se encuentran en provincia y sobre todo, la opción de crecer a futuro con la implementación de estas nuevas técnicas de aprendizaje y de instrucción.
Después de haber analizado las tecnologías que se incluirán en este proyecto, es necesario hacer nuevamente una revisión del objetivo al cuál queremos llegar, de esta manera haremos factible la implementación adecuada a las necesidades planteadas y delimitaremos el problema de una manera eficiente y siguiendo un método de implementación. Después de la implementación de los cambios en la red, viene un punto muy importante el cuál se refiere a dar un seguimiento post-implementación lo que nos permitirá verificar que se cumplió con el objetivo trazado en un principio del proyecto y localizar si en un momento dado existe algún tipo de falla y si es el caso, resolverlo, debido a que la implementación realizada debe ser transparente para el usuario final.

Capítulo 2

DIRECCIONAMIENTO IP

Capítulo 2. DIRECCIONAMIENTO IP

2.1 Introducción

El proceso que nos permite lograr que cada máquina de una red se encuentre enlazada o unida a cualquier otra máquina sobre el Internet se le denomina enrutamiento. Sin éste, la máquina estaría limitada sólo a una red física. El enrutamiento permite al tráfico de una red buscar el camino óptimo a un destino en cualquier lugar del mundo, pasando por supuesto a través de varias redes. Como administrador de redes es necesario asegurar que las rutas del sistema estén correctamente configuradas. El enrutamiento podemos ubicarlo dentro de la capa de red en el modelo ISO/OSI o en la de Internet en el modelo TCP/IP que son las encargadas de las conexiones entre las máquinas a través del protocolo IP. Este puede ser realizado por los hosts (localmente) y especialmente por los enrutadores El modelo OSI (Open System Interconnection) de siete capas fue creado alrededor del año 1979 con el objetivo de facilitar el control, análisis, y administración de los recursos que constituyen el sistema de comunicaciones, además de facilitar el desarrollo de software y hardware que enlazan a redes de trabajo de diferentes proveedores.

A continuación se definirán las siete capas del modelo de referencia OSI, describiendo en forma general la función de las mismas.

- FISICO (1): Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.
- ENLACE (2): Asegura con confiabilidad del medio de transmisión, ya que realiza la
- verificación de errores, retransmisión, control fuera del flujo y la secuenciación de las capacidades que se utilizan en la capa de red.
- RED (3): Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.
- TRANSPORTE (4): Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario. Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica.
- SESIÓN (5): Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.
- PRESENTACIÓN (6): Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.

- APLICACIÓN (7): SE entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.

El TCP/IP es un grupo de protocolos desarrollados para permitir la cooperación entre computadores para compartir recursos a través de una red de trabajo. Este fue desarrollado por un grupo de investigadores del Departamento de Defensa para crear una red de redes de trabajo. El IP es el protocolo más conocido, y es responsable de mover los paquetes de datos desde un nodo a otro, usando para ello la dirección destino compuesta de 4 bytes. En este protocolo ubicado en el nivel Internet (o de red en el modelo ISO/OSI) cada máquina conectada a la red tiene una dirección lógica asignada. Realmente no es cada máquina sino cada interfaz de ésta la que está verdaderamente vinculada a un número de 32 bytes que se conoce como la dirección Internet o número IP, la cual se examina en detalle a continuación, dado que su comprensión es fundamental en nuestra investigación.

2.2 Direccionamiento IP

2.2.1 Direcciones y Redes

Todos los destinos en una red poseen un único identificador que permite a otras máquinas enviar información. Este identificador es llamado usualmente dirección. En algunas tecnologías una dirección identifica una máquina en particular, mientras que en otras, como en el protocolo IP, una dirección identifica un punto de unión a la red, comúnmente llamado interfaz.
Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas, las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz.

2.2.1.2 Definición y estructura de una dirección IP

Las direcciones IP poseen 32 bits de longitud y están divididas en cuatro octetos (8 bits). Una dirección IP puede ser escrita en varias formas: binaria, decimal y hexadecimal. Para escribir una dirección IP en decimal se convierte cada octeto a decimal y se separaran por un punto tal como se muestra en la siguiente figura:

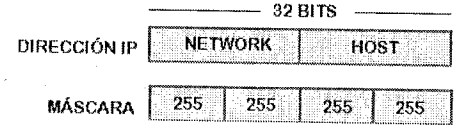


Figura 2.1 Estructura de una Dirección IP

Así 10101100 00011101 00100000 01000010 se puede escribir como 172.29.32.66 La dirección, también puede ser escrita en forma hexadecimal: 0xAC1D2042. Una dirección IP consiste de dos niveles jerárquicos, los cuales son: el identificador de red, y el identificador de máquina, host.

En el protocolo IP el identificador de red representa un número de máquinas que pueden comunicarse entre ellas a través de la capa dos del modelo de referencia OSI. El identificador de máquina representa el número de la máquina dentro de la red.

La dirección IP identifica la máquina de forma única en toda Internet. Las direcciones y rangos de los números IP son asignados por un organismo central en los EU para evitar su duplicación.

2.2.1.3 Números de Red y Máscaras

La división del número de red y de máquina es distinta para cada red. Esto facilita al software de los enrutadores y a las máquinas identificar con facilidad dónde ocurre la división. Cada dirección IP tiene una máscara de red asociada, la cual es representada por un número de 32 bits, donde todos los bits de la porción de red están en 1 y todos los bits de la porción de máquina están en 0. Por ejemplo:
11111111 11111111 00000000 00000000

Los primero 16 bits están asociados al número de red y los 16 restantes al número de la máquina dentro de la red. Las máscaras de redes permiten tener 1 discontinuos, pero esta práctica ha sido eliminada pues tiende a confundir a las personas. Al igual que las direcciones IP, las máscaras se representan con números en forma hexadecimal y una notación adicional llamada dirección base/conteo de bit, como lo señala la tabla siguiente:

FORMATO	VISUALIZACIÓN DE FORMATO
Terminal IP máscara-Formato cuenta de bit	*192.168.2.0/23*
Terminal IP máscara- Formato decimal	*192.168.2.0 255.255.254.0*
Terminal IP máscara-Formato hexadecimal	*192.168.2.0 OXFFFFFE00*

Tabla 2.1 Tabla de Visualizaciones de formatos de Mascaras

2.2.2 *Clases*

Antes de que las máscaras fueran generalizadas, existieron las clases de red, con máscaras implícitas asociadas a dichas clases. Sin embargo esto se fue haciendo obsoleto debido a la generalización de la arquitectura de clases de la cual hablaremos más adelante. Los diseñadores de red no previnieron una red del tamaño de Internet; pensaron que solo necesitarían soportar unas cuantas redes gigantescas (como corporaciones de computadoras, universidades y centros de investigación), un mediano número de redes de tamaño moderado y muchas redes pequeñas. Por esta razón se crearon solo tres tipos de red: clase A para grandes redes, clase B para redes medianas y clase C para redes pequeñas. Se pensó además en hacer los procesos de decisión de enrutamiento fáciles, y codificaron las clases mediante los primeros bits de la dirección IP.

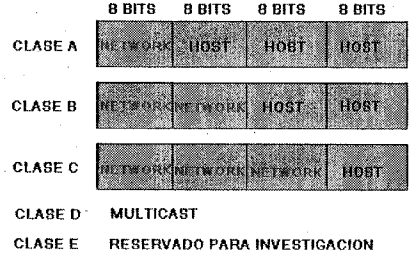


Figura 2.2 Clases de Direcciones IP

Clase A

Las direcciones IP clase A, utilizan el primer octeto (byte) para referirse al número de red. El primer bit comienza en "0". El rango de direcciones para estas redes está entre el 1.x.x.x y el 126.x.x.x y se pueden asignar direcciones hasta 16194277 hosts. La dirección 127.x.x.x está reservada para designar la interfaz local.

Clase B

Las direcciones IP clase B, emplean los dos primeros octetos para referirse al número de red. Los dos primeros bits son "10". El rango de direcciones para estas redes está comprendido entre el 128.0.x.x y el 191.255.x.x, pudiéndose asignar direcciones para 64516 hosts.

Clase C

Las direcciones IP clase C, usan los tres primeros octetos para referirse al número de red. Los tres primeros bits son "110"; y su rango de direcciones de red está comprendido entre el 192.0.0'.x y el 223.255.255.x. A esta clase de red se le pueden asignar direcciones a 254 hosts.

Clase D

Originalmente las direcciones IP clase D eran definidas como las redes con los tres primeros bits en "111"y fueron reservadas para usos futuros. Desde entonces las investigaciones han provocado cambios en la definición de la clase D, considerándose actualmente como las redes que comiencen con "1110". Estas redes no representan una máquina sino una colección que forma parte de un grupo Multicast IP. Comprende las direcciones de red desde la 224.0.0.0 hasta la 239.255.255.255.

Clase E

Las redes clase E, comienzan con sus cinco primeros bits en "11111"y están compuestas por las redes comprendidas desde la 240.0.0.0 hasta la 247.255.255.255. Estas direcciones de red están reservadas para uso futuro y son conocidas como redes reservadas para investigación. Posiblemente una nueva clase podría ser necesaria, así la definición de clase tipo E podría ser modificada por una clase que comience por "111110"y una nueva clase se definiría (y se reservaría para uso futuro) comenzando con "111111". Existen además direcciones IP con un significado especial. Los valores con ceros (0) significan esta red o esta máquina. Los valores con unos (1) representan todas las máquinas en la red indicada. Se descuentan también los octetos compuestos en su totalidad de 0's y 1's que se emplean para Broadcast:

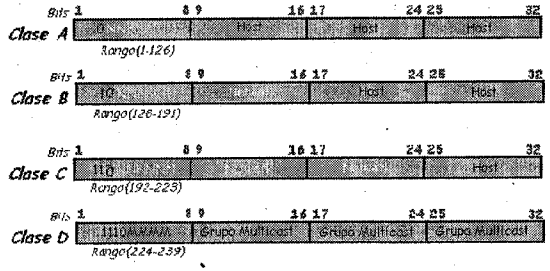
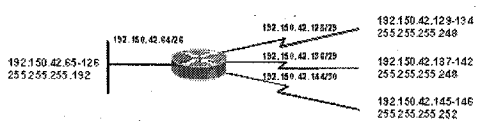


Figura 2.3 Rango de las direcciones IP

2. 2.3 VLSM (Máscara de subred de longitud variable)

El uso de máscaras de subred de longitud variable (VLSM) permite optimizar el espacio de direcciones disponible mediante la división de una red en subredes de diferente tamaño. Las máscaras de longitud variable pueden utilizarse, por ejemplo, en los enlaces WAN punto a punto que tienen sólo dos equipos (un enrutador en cada extremo).



# subredes	máscara de subred	# hosts
1	/24 255.255.255.0	254
2	/26 255.255.255.192	62
6	/27 255.255.255.224	30
14	/28 255.255.255.240	14
30	/29 255.255.255.248	6
62	/30 255.255.255.252	2

Figura 2.4 Mascara de subred de longitud variable

Si se hace uso de la técnica de VLSM, el rango de direcciones IP posibles es administrado con mayor eficiencia. Esta técnica consiste en la inclusión del campo subred en el registro de una dirección IP. Su función es definir la subred de una red.
El método más utilizado para determinar la subred de una red es haciendo uso de un registro conocido con el nombre de "máscara de una subred " y al efectuar la operación booleana AND entre una dirección IP y la "máscara de la subred " se determina la subred de una red.
En el ejemplo de la figura siguiente se define una dirección IP clase B, cuya red está definida por el número: 140.120.x.x y máscara 255.255.0.0.
La máscara de las subredes es 255.255.255.0. Lo cuál nos dice que existen 255 subredes, además de que hay 255 computadoras por subred.
Es importante mencionar que el número de bit del campo subred puede variar dependiendo del número necesario de computadoras por subred. Por ejemplo, dada la red clase B: 130.130.0.0, dicha red podría ser dividida por uno de los siguientes arreglos de subredes:

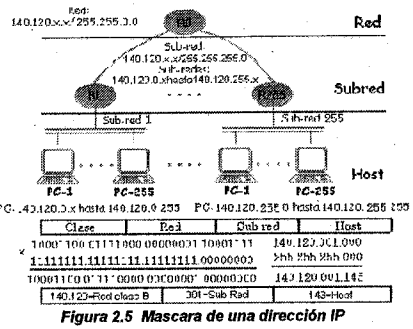


Figura 2.5 Mascara de una dirección IP

Esta técnica se conoce con el nombre de máscara de subred de longitud variable (VLSM) y su función es definir subredes que se adapten con mayor facilidad al número de computadoras por subred. Para hacer aún más explícita esta técnica analizamos el siguiente ejemplo. Una organización se le ha asignado la red Clase C número 194.120.14.x/255.255.255.0. Dicha organización está compuesta por los departamentos: A, B, C; cada departamento requiere el siguiente número de computadoras: 98, 48 y 50 respectivamente.

Red: 130.130.0.0		
Máscara de la subred: 255.255.255.0 No. subredes: 255 Computadoras/Subred: 255	*Máscara de la subred: 255.255.255.240 No. de subredes: 17 Computadoras/subred: 16*	*Máscara de la subred: 255.255.255.252 No. de subredes: 65 Computadoras/Subred: 4*
130.130.0.0	130.130.0.0	130.130.0.0
130.130.1.0	130.130.0.16	130.130.0.4
130.130.2.0	130.130.0.32	130.130.0.8
130.130.3.0	130.130.0.48	130.130.0.12
130.130.4.0		
130.130.5.0		
130.130.6.0		
130.130.251.0	130.130.207.176	130.130.239.236
130.130.252.0	130.130.223.192	130.130.243.240
130.130.253.0	130.130.239.208	130.130.247.244
130.130.254.0	130.130.255.224	130.130.251.248
130.130.255.0	130.130.255.240	130.130.255.252

Tabla 2.2 Tabla de los arreglos de las subredes

El crecimiento en 2 años de cada departamento está previsto que sea del 20% para el departamento A, del 18% para el departamento B y del 10% para el departamento C. Sobre la base de esta información la máscara de cada subred y el número de direcciones IP de cada computador es la siguiente:

- Departamento A subred: 194.120.14.0
- Mascara de la subred: 255.255.255.128
- Rango de direcciones IP: 194.120.14.0 hasta 194.120.14.127
- **Rango de direcciones IP válidas para host: 194.120.14.1 hasta 194.120.14.126**
- Rango de direcciones IP a utilizar inicialmente: 194.120.14.1 hasta 194.120.14.98
- **Rango de direcciones IP a utilizar en dos años: 194.120.14.1 hasta** 194.120.14.116
- Rango de direcciones IP de reserva: 194.120.14.117 hasta 194.120.14.126
- Departamento B subred: 194.120.14.128
- Mascara de la subred: 255.255.255.192
- Rango de direcciones IP: 194.120.14.128 hasta 194.120.14.191
- **Rango de direcciones IP válidas para host: 194.120.14.128 hasta** 194.120.14.191
- Rango de direcciones IP a utilizar inicialmente: 194.120.14.129 hasta 194.120.14.177
- **Rango de direcciones IP a utilizar en dos años: 194.120.14.129 hasta** 194.120.14.186
- Rango de direcciones IP de reserva: 194.120.14.187 hasta 194.120.14.190
- Departamento C subred: 194.120.14.192
- Mascara de la subred: 255.255.255.192
- Rango de direcciones IP: 194.120.14.192 hasta 194.120.14.255
- **Rango de direcciones IP válidas para host: 194.120.14.193 hasta** 194.120.14.243
- Rango de direcciones IP a utilizar inicialmente: 194.120.14.193 hasta 194.120.14.243
- **Rango de direcciones IP a utilizar en dos años: 194.120.14.193 hasta** 194.120.14.248
- Rango de direcciones IP de reserva: 194.120.14.249 hasta 194.120.14.254

Para esto, las reglas seguidas son que cada uno de los bits que conforman al campo de una dirección IP no puede tener el valor 0 ó 1. Ya que si todos los bits son iguales a 0 se estaría definiendo a la subred. Y si todos los bits del campo computador son iguales a 1 se estaría definiendo a la dirección broadcast de la subred.

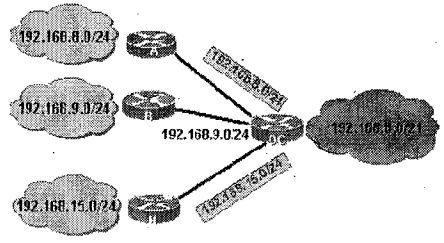
Si aplicamos este esquema de direccionamiento a una organización que está dividida en *n* departamentos es importante resaltar que:

- El campo subred incluido en el registro de una dirección IP es el que define a la red de un departamento y por ende, el número de redes no es directamente proporcional al número de departamentos.

- El número de computadoras que pueden ser definidas en una subred se adapta con mayor facilidad al número de computadoras por departamento, y el rango de direcciones IP posibles es administrado con mayor eficiencia.
- Un nuevo nivel jerárquico es incluido de manera implícita en el sistema de direccionamiento IP

2.2.4 CIDR (Classless Inter - Domain Routing)

Asignar muchas direcciones tipo C en vez de una sola tipo B conserva los números tipo B y resuelve el problema inmediato de la terminación de espacio para direcciones de este tipo. Sin embargo, crea un nuevo problema: la información que los ruteadores almacenan e intercambian aumenta dramáticamente. Una técnica conocida como CIDR resuelve el problema. Conceptualmente CIDR colapsa un grupo de direcciones tipo C contiguas (o de cualquier otro tipo) en un solo registro representados por dos datos: (dirección de red, conteo de bits para la máscara) Por ejemplo Redes de la 192.168.8.0/24 hasta la 192.168.15.0/24 pueden ser sumadas en un solo anuncio: 192.168.8.0/21.



Redes de la 192.168.8.0/24 hasta la 192.168.15.0/24 son sumarizadas por OC en un solo anuncio : 192.168.8.0/21

Figura 2.6 Ejemplo de la utilización de CIDR

En la práctica, CIDR no restringe los números de red sólo a direcciones tipo C, ni utiliza un conteo de números enteros para especificar el tamaño de un grupo. Mas bien requiere que cada grupo de direcciones sea contiguo y una potencia de dos utilizando una máscara de bit para identificar el tamaño del grupo. Por ejemplo, suponga que tiene asignado un grupo de 2048 direcciones contiguas, comenzando en la dirección 234.170.168.0, se calculan los valores binarios de las direcciones en dicho rango.

Notación decimal con puntos	Notación decimal con puntos	Equivalencia binaria de 32 bits
más baja	234.170.168.0	101010 10101010 101010 00000000
más alta	234.170.175.255	101010 10101010 101011 11111111

Tabla 2.3 Tabla de equivalencias en CIDR

CIDR requiere que dos valores especifiquen el rango: la dirección más baja y una máscara que operé como un estándar de subred al delimitar el fin del prefijo. Para el rango mostrado, la máscara CIDR tiene el grupo de 21 bits 11111111 11111111 11111000 00000000 que puede ser denotada en notación decimal como 255.255.248.0.
La notación en CIDR para el rango trabajado con su respectiva máscara será la siguiente: 234.170.168.0 / 21. En vez de ser limitados a identificadores de red (o "prefijos") de 8, 16 o 24 bits, CIDR actualmente usa prefijos que van de 13 a 27 bits.
De este modo se pueden asignar bloques de direcciones para redes pequeñas de 32 hosts hasta redes con más de 50000 hosts permitiendo la asignación de direcciones que se ajusten a las necesidades específicas de las organizaciones.

Prefijo de bloque CIDR	# Equivalente de clase C	# de direcciones de hosts
/27	un 1/8 de clase C	32 hosts
/26	un ¼ de clase C	64 hosts
/25	un ½ de clase C	128 hosts
/24	1 clase C	256 hosts
/23	2 clase C	512 hosts
/22	4 clase C	1024 hosts
/21	8 clase C	2048 hosts
/20	16 clase C	4096 hosts
/19	32 clase C	8192 hosts
/18	64 clase C	16384 hosts
/17	128 clase C	32768 hosts
/16	256 clase C (= 1 clase B)	65536 hosts
/15	512 clase C	131072 hosts
/14	1024 clase C	262144 hosts
/13	2048 clase C	524288 hosts

Tabla 2.4 Tabla completa de CIDR

2 .3 Direccionamiento IP USADO para Multicast

2.3.1 Protocolo de Internet (IP) Multicast

IP Multicast es una tecnología que reduce el tráfico sobre la red entregando un solo flujo de información simultáneamente a los miles de destinatarios corporativos y casas. De las aplicaciones que se aprovechan de Multicast se incluyen las videoconferencias, comunicaciones corporativas, educación a distancia, distribución de software, y noticias. IP Multicast entrega tráfico de la fuente a los receptores múltiples sin agregar cualquier carga adicional en la fuente o los receptores mientras usa el menor ancho de banda de la red En la red, los ruteadores reproducen paquetes de IP Multicast con el protocolo PIM (Protocol Independent Multicast) para un envío eficaz de la información a los múltiples receptores posibles. Como algo forzoso para transmisiones IP sin Multicast, el host debe enviar una copia de los datos a cada receptor destino, para este caso pongamos un ejemplo, si se quisiera enviar a miles de receptores- destino un paquete de datos que utilicen un ancho de banda grande como videos MPEG, el envío de la información sería complicado pues esta aplicación utiliza una gran porción del ancho de banda disponible para un solo envío. En estas aplicaciones la única manera de enviar simultáneamente a más de un receptor es usando IP Multicast. El IP Multicast provee a los múltiples receptores del tráfico de la fuente sin saturar a la fuente o a los receptores mismos, esto utilizando un mínimo del ancho de banda. Los paquetes de IP Multicast son copiados en la red en el punto donde los enlaces divergen en los ruteadores, los cuáles están habilitados con PIM (Protocol Independent Multicast) y otros protocolos de Multicast que sirven como apoyo para el PIM. La figura muestra como los datos de una fuente se entregan a varios destinatarios utilizando IP Multicast.

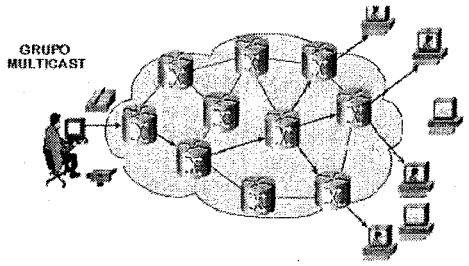


Figura 2.7 Transmisión de Multicast: La fuente envía solo un paquete del Multicast el cuál es dirigido a todos los destinatarios

2.3.2 Concepto de Grupo Multicast

Multicast esta basado en el concepto de un grupo, el cual es un grupo arbitrario de receptores que reciben un arroyo de datos en particular. Este grupo no tiene límite físico o geográfico. Los hosts que están interesados en unirse a un grupo en particular (es decir en convertirse en receptores de datos que fluyen a un grupo particular) deben hacerlo mediante una solicitud de membresía de IGMP (Internet Group Management Protocol). Los hosts deben ser un miembro del grupo para recibir el flujo de datos.

2.3.3 Direcciones IP Multicast

Las direcciones de Multicast especifican un grupo arbitrario de receptores IP que se han metido en el grupo y han deseado recibir tráfico enviado a este grupo.

2.3.3.1 Clases IP, las Direcciones de D

El IANA ha asignado la vieja Clase D para ser usado por IP Multicast. Esto significa que todo el grupo de direcciones IP Multicast se desplomarán de este rango:
224.0.0.0 - 239.255.255.255. Note que este rango de dirección sólo es para la dirección de grupo o dirección del destino de IP del tráfico de Multicast. La dirección de la fuente para los diagramas de datos de Multicast siempre es la dirección de fuente de unicast.

2.3.3.2 Mapeo de direcciones IP Multicast con direcciones MAC

Históricamente, las tarjetas de interfase de red (NIC's) en un segmento de la red LAN pueden recibir solo paquetes destinados a sus direcciones MAC propiamente. En el direccionamiento IP con Multicast, algunos host necesitan para la recepción una cadena simple de datos con una misma dirección MAC de destino. Algunos medios tuvieron que ser inventados para que los múltiples host pudieran recibir el mismo paquete y así poder diferenciar entre varios grupos del Multicast.

Un método para poder realizar esto, es mapear las direcciones IP Multicast de la clase D directamente a la dirección del MAC. Hoy, usando este método, las NIC's puede recibir paquetes destinados a muchas direcciones diferentes MAC de su propio Unicast, Broadcast y a un rango determinado de direcciones del Multicast Las especificaciones de IEEE sobre LAN aportaron técnicas para la transmisión de paquetes de broadcast y paquetes de Multicast.
En el estándar 802.3, el bit cero del primer octeto es usado para indicar si se trata de una trama de broadcast o una trama de Multicast. La siguiente figura muestra la ubicación del bit de broadcast o de Multicast en una trama de Ethernet.

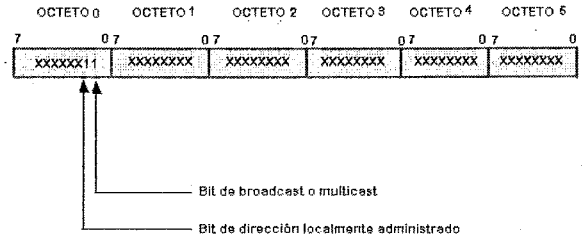


Figura 2.8 Formato de dirección MAC del estándar 802.3

Este bit indica que la trama esta destinada para un grupo de hosts o para todos los hosts que se encuentran en la red (en este caso de la dirección de broadcast: 0xFFFF.FFFF.FFFF). El direccionamiento IP Multicast hace uso de esta capacidad para enviar paquetes de IP a un grupo de hosts en un segmento de LAN.
El IANA posee un bloque direcciones de MAC de Ethernet que empiezan con 01:00:5E en forma hexadecimal. La mitad de este bloque se asigna para las direcciones del Multicast El rango de 0100.5e00.0000 hasta el 0100.5e7f.ffff, es el rango disponible de las direcciones MAC de Ethernet para el direccionamiento Multicast IP.
Esta asignación permite para 23 bits en la dirección de ethernet corresponder al Multicast de la dirección de grupo IP. El mapeo coloca los 23 bits más bajos del grupo de direccionamiento IP de Multicast en los 23 bits disponibles en la dirección de Ethernet, como se muestra en la siguiente figura:

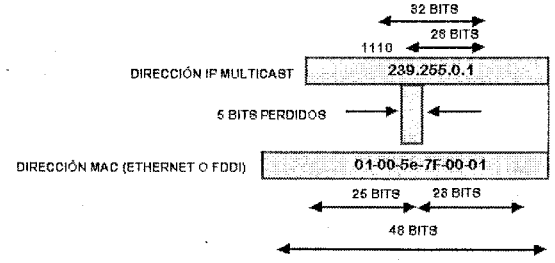


Figura 2.9 IP Multicast para Ethernet o mapeo de direcciones MAC

Debido a que los cinco bits más altos de la dirección IP Multicast caen dentro del mapeo, las direcciones resultantes no son únicas, de hecho, 32 grupos diferentes de ID's Multicast caen a la misma dirección MAC, como se muestra en la siguiente figura:

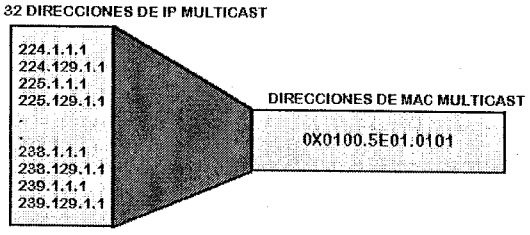


Figura 2.10 Ambigüedades del direccionamiento MAC

Los administradores de red pueden considerar este hecho cuando asignan direcciones IP Multicast. Por ejemplo 224.1.1.1 y 225.1.1.1 caen dentro de la misma dirección MAC **Multicast en un switch de capa 2 Si un usuario se subscribe al grupo** A (designado por **224.1.1.1) y otros usuarios están subscritos en el grupo B (designado por 225.1.1.1), quizás recibirán ambas tramas. Esta situación limita la** efectividad de Multicast en capa dos, la cual se puede solucionar asignando cuidadosamente las direcciones IP para cada grupo a usarse, evitando el enlace en capa 2.

Capítulo 3

ENRUTAMIENTO IP

Capitulo 3 ENRUTAMIENTO IP

3.1 Enrutamiento (Routing)

Enrutamiento es el proceso de dirigir a los paquetes por vías alternativas hasta su destino, siendo realizado por los hosts (localmente) y especialmente, por los enrutadores. El problema del enrutamiento es el de decidir la vía óptima para alcanzar algún nodo destino, la cuál puede estar definida por:

- El Tiempo de transmisión.
- El número de saltos.
- El máximo ancho de banda.
- El mínimo retardo.
- La menor ocupación de enlaces.
- La confiabilidad de los enlaces.

Normalmente, existe más de un camino por el cuál enviar paquetes de información entre un punto de origen y el punto de destino. Cuando hay varias opciones a elegir, el enrutador es el elemento que se encarga de elegir la ruta de envío de dichos paquetes de información. Para esto, debemos considerar algunos factores, por ejemplo, la longitud de las rutas a seguir. La elección de dichas rutas se logra asignando valores a los enlaces los cuáles a su vez, en conjunto, determinan la longitud de la ruta. Por consecuencia, elegiremos la ruta más corta.
El término "ruta mas corta", en este contexto, puede significar dos cosas dependiendo del protocolo, en algunos casos, significa la ruta que requiere el número más pequeño de retransmisiones o saltos, en otros casos, significa la ruta más rápida, económica, más fiable, más segura o la mejor cualidad que se puede establecer sobre un enlace concreto (o combinación de enlaces) y que sea más atractiva que otra. Normalmente esta terminología de "ruta más corta", suele hacer referencia a una combinación de todas las ventajas descritas anteriormente.

3.2 Conceptos generales

3.2.1 Tiempo de vida

Una vez que el enrutador a elegido un camino, pasa el paquete al siguiente enrutador situado en el camino y se olvida de él. El siguiente enrutador, sin embargo, puede elegir el mismo camino o puede decidir que existe un camino diferente más corto y retransmitir el paquete al siguiente enrutador en esa dirección. Esta separación de responsabilidades permite a cada enrutador contener la mínima lógica necesaria, haciendo que la cantidad de información de control que debe contener un paquete sea la mínima y permite que el ajuste de la ruta se base en las apreciaciones de última hora de cada enlace. También crea la posibilidad de que un paquete entre en un bucle o

entre en una situación en la que el paquete se pasa enrutador a enrutador sin que nunca alcance su destino. La situación en la que un paquete pasa de un enrutador a enrutador sin alcanzar el destino puede ocurrir cuando el enrutador actualiza su tabla de enrutamiento y retransmite un paquete de acuerdo a los nuevos caminos antes de que el enrutador que recibe haya actualizado el suyo propio. El problema creado por los bucles o los rebotes no es principalmente que los paquetes se pierdan; las funciones del nivel de enlace de datos del emisor y del receptor de la transmisión informarán de la pérdida de tramas y las reemplazarán con nuevas copias. El problema es que el procesamiento eterno de los paquetes que entran en un bucle utiliza recursos de red e incrementa la congestión. Los paquetes que entran en un bucle deben ser identificados y destruidos para liberar los enlaces y dejarlos para tráfico legítimo. La solución se basa en añadir un campo denominado tiempo de vida del paquete (TTL). Cuando se genera un paquete se marca con un tiempo de vida, normalmente el número de saltos que se permiten antes de que un paquete se considere como perdido. Cada enrutador, cuando recibe un paquete, resta una unidad al tiempo de vida antes de pasarlo. Cuando el tiempo de vida llega a cero, el paquete es destruido.

3.2.2 Tabla de enrutamiento.

En las tablas de enrutamiento se encuentran identificadas las redes, las trayectorias para llegar a ellas y la eficiencia relativa de las trayectorias. Los enrutadores no usan las tablas para encontrar la dirección específica de un dispositivo en otra red, sino que se hace para seleccionar la mejor ruta hacia este. El enrutador recibe paquetes ya sean de una estación final (dirección fuente) o por otro enrutador. Basado en la dirección de red que mejor se ajuste en la tabla de enrutamiento con respecto al destino final contenido en el paquete, el enrutador determina a cual estación o nodo de red debe enviar el paquete, dándose así el proceso de enrutador de salto en salto.

La tabla de enrutamiento IP incluye información en las columnas siguientes:

- Destino: El destino es el host, la dirección de subred, la dirección de red o la ruta de default. La ruta de default es 0.0.0.0.

- Máscara de red: La máscara de red se utiliza en conjunción con el destino para determinar cuándo se utiliza una ruta. Por ejemplo, una ruta de host tiene una máscara 255.255.255.255, la ruta de default tiene una máscara 0.0.0.0 y una ruta de red o de subred tiene una máscara comprendida entre estos dos extremos.La máscara 255.255.255.255 significa que sólo utilizará esta ruta un destino que coincida exactamente. La máscara 0.0.0.0 significa que cualquier destino puede utilizar esta ruta. Si una máscara se escribe en binario, un 1 es significativo (debe coincidir) y un 0 no lo es (no es necesario que coincida). Por ejemplo, un destino 172.16.8.0 con una máscara de red 255.255.248.0. Esta máscara indica que los dos primeros octetos tienen que coincidir exactamente, los primeros 5 bits del tercer octeto tienen que coincidir (248=11111000) y que el último octeto no es relevante. El tercer octeto de 172.16.8.0 (es decir, 8) es igual a **00001**000 en binario. Sin cambiar los primeros 5 bits (la parte sin máscara que se muestra en **negrita**), puede llegar hasta 15 ó **00001**111 en binario. Así pues, una ruta con un destino 172.16.8.0 y una

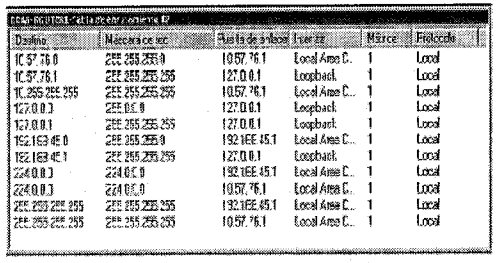
máscara 255.255.248.0 se aplica a todos los paquetes destinados a 172.16.**8**.0 hasta 172.16.**15**.255.

- Puerta de enlace o salto siguiente: La puerta de enlace o salto siguiente es la dirección IP del siguiente enrutador al que se debe enviar un paquete. En el caso de una interfaz de marcado a petición, la dirección IP de puerta de enlace no es configurable.

- Interfaz : La interfaz indica la interfaz LAN o WAN que se va a utilizar para alcanzar el siguiente enrutador

- Métrica: La métrica indica el costo relativo por utilizar la ruta para alcanzar el destino. Una métrica típica son los saltos, o número de enrutadores que se atraviesan para alcanzar el destino. Si existen varias rutas al mismo destino, la ruta con menor métrica es la ruta más adecuada.

- Protocolo: El protocolo muestra cómo se aprendió la ruta. Si en la columna *Protocolo* se enumeran los protocolos RIP o OSPF (o cualquier otro que no sea Local), el enrutador está recibiendo las rutas desde otro dispositivo.



Destino	Máscara de red	Puerta de enlace	Interfaz	Métrica	Protocolo
10.57.76.0	255.255.255.0	10.57.76.1	Local Area C...	1	Local
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Local
10.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.45.0	255.255.255.0	192.168.45.1	Local Area C...	1	Local
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Local
224.0.0.0	224.0.0.0	192.168.45.1	Local Area C...	1	Local
224.0.0.0	224.0.0.0	10.57.76.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.45.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	10.57.76.1	Local Area C...	1	Local

Figura 3.1 Ejemplo de Tabla de Enrutamiento

Para mantener la tabla de enrutamiento se conocen dos métodos generales. El primero es el enrutamiento estático en donde el administrador llena los registros de la tabla de forma manual, para lo cual debe conectarse al enrutador a fin de modificar la información necesaria para acceder a cada red. Si existe un cambio en la topología de la red, el o los administradores deben cambiar las rutas manualmente según los cambios ocurridos. La desventaja de este tipo de enrutamiento es que sólo toma en cuenta una ruta sin importar la existencia de una ruta alterna más conveniente. Para solventar estas deficiencias se buscó un proceso para actualización automática de las tablas de enrutamiento, dando origen a la aparición del segundo método de enrutamiento llamado dinámico, que funciona gracias al intercambio de información entre los diferentes enrutadores. Los enrutadores intercambian información con sus vecinos acerca de las rutas que ellos conocen, de manera tal que todos los enrutadores

tengan sus tablas al día. El enrutamiento se puede clasificar entonces en dinámico y estático.

3.2.3 Protocolos de Enrutamiento

Los protocolos son el lenguaje o las normas de comunicación entre los dispositivos en una red. Todos los dispositivos en una red generalmente ejecutan el mismo protocolo de enrutamiento, que es similar a un lenguaje común, para poder comunicarse.

Los protocolos de enrutamiento son los protocolos que utilizan los enrutadores para comunicarse entre sí a fin de intercambiar información de forma dinámica acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles. Los paquetes de los protocolos de enrutamiento ocupan ancho de banda y operan independientemente de los paquetes de datos enrutados que atraviesan la red. Los enrutadores se envían entre sí periódicamente información acerca de las rutas (tablas de enrutamiento), de modo que cuando reciben un paquete de protocolo enrutado (como IP) saben a dónde deben enviarlo. En general, existen dos tipos de protocolos de enrutamiento: los protocolos interiores y los protocolos exteriores.

Los protocolos de enrutamiento interiores se utilizan dentro de una red privada. Por ejemplo, una empresa puede tener varias LAN en distintas ubicaciones geográficas, conectadas por enrutadores y por enlaces de WAN dedicados (como T1 o Frame Relay). Si todos esos enrutadores están bajo un sistema de administración común o autónomo (que no está conectado a través de Internet), entonces deben utilizar un protocolo de enrutamiento interior. Los protocolos de enrutamiento interior pueden clasificarse de la siguiente manera:

- Vector distancia
- Estado de enlace.

Estos dos tipos se distinguen en las métricas que emplean para seleccionar rutas y en la forma de que se almacenan y se intercambian las actualizaciones de tabla de enrutamiento. Ejemplos: RIP, IGRP, EIGRP, OSPF.

Los protocolos de enrutamiento exteriores se utilizan para las comunicaciones entre sistemas autónomos y a través de Internet. Entre los ejemplos de protocolos exteriores se incluyen el Protocolo de Gateway Fronterizo (BGP) y el Protocolo de Gateway Exterior (EGP). BGP es el protocolo de enrutamiento exterior más común y su versión más reciente es BGP4.

3.3 Enrutamiento Estático

Se denomina enrutamiento estático a la ruta que se ha configurado e introducido explícitamente en una tabla de enrutamiento. Las rutas estáticas son fijas y tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico, la

decisión de qué ruta tomar desde el principio al final de una tabla de enrutamiento se calcula por adelantado, fuera de línea y, se cargan en los enrutadores al iniciar el proceso de enrutamiento dentro de una red.

La desventaja de este tipo de esquema es que no es posible responder a situaciones cambiantes como por ejemplo saturación, exceso de tráfico o fallo en una línea. En un conjunto de redes complejas, se necesita cierto grado de cooperación dinámica entre los dispositivos de enrutamiento. En particular se deben evitar aquellas porciones de red que sufren congestión, entendiéndose esto como aquella situación donde hay demasiados paquetes en alguna parte de la subred, y como consecuencia el rendimiento de ésta baja.

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de red, que lo introduce en la configuración de un enrutador como mencionamos anteriormente. El administrador debe actualizar manualmente cada entrada de ruta estática siempre que un cambio en la topología de la red requiera una actualización. Los enrutadores no tienen que descubrir ni propagar nuevas rutas a través de la red. Existe una relación entre la dirección destino de un paquete y el interfaz por el cual debe de ser enviado dicho paquete. Esta relación es la que se programa de forma estática en los enrutadores, y no se modificará con el paso del tiempo.

El enrutamiento estático posee varias ventajas.

- Cuando se puede acceder a una red a través de un solo camino, una ruta estática hacia la red puede ser suficiente. Este tipo de red se denomina red de conexión única. La configuración del enrutamiento estático para una red de conexión única evita el gasto que implica el enrutamiento dinámico.
- Es el que menos recursos del enrutador y de la red consume: ahorra ancho de banda en cada uno de sus enlaces al no necesitar información proveniente de la red para construirse las tablas de enrutamiento, ahorra tiempo de CPU y memoria en el enrutador porque no tiene que calcular rutas.
- Ayuda a crear redes más seguras puesto que solo existe un camino para entrar o salir de este tipo de redes, por lo que se hace más fácil el monitoreo en previsión de ataques, o el rastreo una vez se han producido dichos ataques.

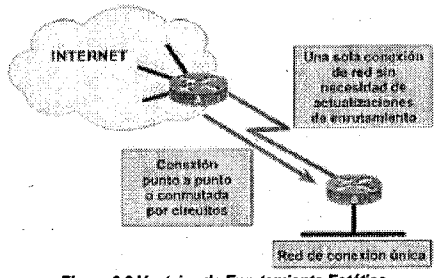


Figura 3.2 Ventajas de Enrutamiento Estático

El enrutamiento estático también posee varias desventajas:

- La ausencia de tolerancia a fallos. Si existiera una caída en cualquier parte de la red, esta no sería capaz de reaccionar y automáticamente dirigir los paquetes por otro camino, ya que solo tienen una única ruta para hacerlo.
- La cantidad de rutas estáticas que habría que configurar en redes grandes y complejas. La imposibilidad de reparto de tráfico entre varios caminos posibles (balanceo de carga).

La distancia administrativa es una calificación para determinar la confiabilidad de una fuente de información de enrutamiento, expresada por un valor numérico de 0 a 255. Cuanto mayor sea el número, menor será la calificación de confiabilidad. Los valores de distancia administrativa introducidos manualmente para las rutas estáticas son generalmente números bajos (1 es el valor por defecto). Las actualizaciones de enrutamiento no se envían a través de un enlace si sólo se encuentran definidas por una ruta estática, por lo tanto, conservan el ancho de banda. Las rutas por defecto mantienen las tablas de enrutamiento más cortas. Cuando no existe una entrada para una red destino en una tabla de enrutamiento, el paquete se envía a la red por defecto. La figura muestra el uso de una ruta por defecto: una entrada en la tabla de enrutamiento que dirige los paquetes hacia el salto siguiente, cuando este salto no se encuentra explícitamente determinado en la tabla de enrutamiento. Se pueden establecer rutas por defecto como parte de la configuración estática.

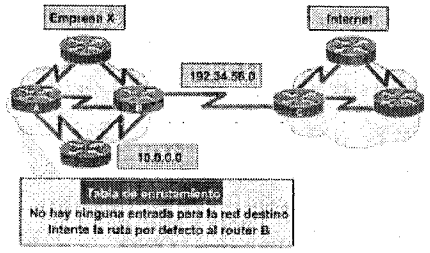


Figura 3.3 Ruta por Defecto

En este ejemplo, los enrutadores de la empresa X poseen un conocimiento específico de la topología de la red de la empresa X, pero no de las demás redes. Mantener el conocimiento de cada una de las demás redes accesibles a través de la nube de Internet es totalmente innecesario y poco razonable, si no imposible.
En lugar de mantener un conocimiento específico de cada red, se informa a cada enrutador de la empresa X la ruta por defecto que puede utilizar para llegar a cualquier destino desconocido direccionando el paquete hacia Internet.
Veamos el siguiente ejemplo: La asignación de una ruta estática para alcanzar la red de conexión única 172.16.1.0 es adecuada para A porque sólo existe una forma de alcanzar esa red. La asignación de una ruta estática desde B a las redes de la nube también es posible. Sin embargo, se requiere una asignación de ruta estática para cada red destino, en cuyo caso sería más apropiada una ruta por defecto.

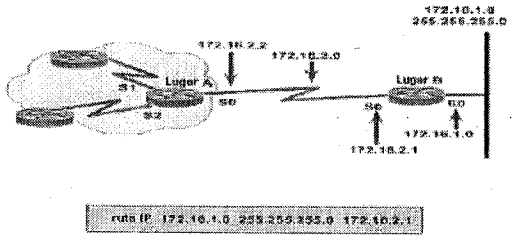


Figura 3.4 Aplicación de las Rutas por Defecto

3.4 Enrutamiento Dinámico

El conocimiento de las rutas de forma dinámica funciona de manera diferente. Después de que un administrador de red introduce comandos de configuración para empezar el

enrutamiento dinámico, el conocimiento de la ruta se actualiza automáticamente a través de los protocolos de enrutamiento. Los cambios en el enrutamiento dinámico intercambian entre enrutadores como parte del proceso de actualización. La red que aparece en la figura se adapta de forma diferente a los cambios de topología, según si usa la información de enrutamiento configurada de forma estática o dinámica.

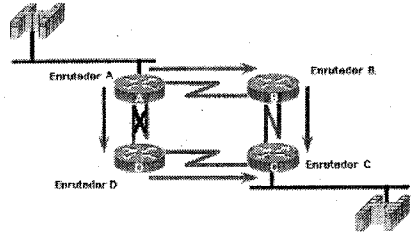


Figura 3.5 Enrutamiento Dinámico

El enrutamiento estático permite que los enrutadores actúen correctamente sobre un paquete desde una red a otra tomando como base la información configurada. El enrutador consulta su tabla de enrutamiento y utiliza el conocimiento estático que reside allí para transferir el paquete hacia el Enrutador D. El Enrutador D hace lo mismo y transfiere el paquete al Enrutador C. El Enrutador C entrega el paquete al host destino. Si la ruta entre el Enrutador A y el Enrutador D falla, el Enrutador A no podrá transferir el paquete al Enrutador D utilizando esa ruta estática. Hasta que el Enrutador A se reconfigure manualmente para enviar paquetes a través del Enrutador B, la comunicación con la red destino es imposible. El enrutamiento dinámico ofrece más flexibilidad.
Según la tabla de enrutamiento generada por el Enrutador A, un paquete puede llegar a destino por la ruta preferida a través del Enrutador D. Sin embargo, una segunda ruta hacia el destino está disponible a través del Enrutador B. Cuando el Enrutador A reconoce que el enlace al Enrutador D está caído, ajusta su propia tabla de enrutamiento, haciendo que la ruta a través del Enrutador B se convierta en la ruta preferida hacia el destino.
Los enrutadores siguen enviando paquetes a través de este enlace. Cuando se restaura la ruta entre los Enrutadores A y D, el Enrutador A puede nuevamente cambiar su tabla de enrutamiento para indicar una preferencia por la ruta orientada en dirección contraria a la de las agujas del reloj a través de los Enrutadores D y C hacia la red destino. Los protocolos de enrutamiento dinámico también pueden dirigir el tráfico de una misma sesión a través de distintas rutas de una red para lograr un mejor rendimiento. Esto se conoce como carga compartida. El éxito del enrutamiento dinámico depende de dos funciones básicas del enrutador:

- El mantenimiento de una tabla de enrutamiento
- La distribución oportuna del conocimiento, bajo la forma de actualizaciones de
- Enrutamiento, hacia otros enrutadores

El enrutamiento dinámico se basa en un protocolo de enrutamiento para compartir el conocimiento entre los enrutadores. Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un enrutador cuando se comunica con los enrutadores vecinos. Por ejemplo, un protocolo de enrutamiento describe:

- Cómo enviar actualizaciones
- Qué conocimiento contienen esas actualizaciones
- Cuándo enviar ese conocimiento
- Cómo ubicar a los destinatarios de las actualizaciones

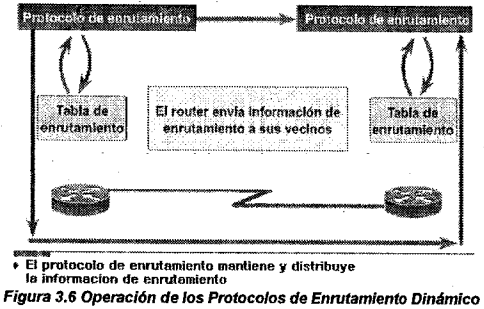


Figura 3.6 Operación de los Protocolos de Enrutamiento Dinámico

Cuando un algoritmo de enrutamiento actualiza una tabla de enrutamiento, su objetivo principal es determinar cuál es la mejor información que debe incluir en la tabla. Cada algoritmo de enrutamiento interpreta lo que es mejor a su manera. El algoritmo genera un número, denominado métrica, para cada ruta a través de la red. Normalmente, cuanto menor sea la métrica, mejor será la ruta. Se pueden calcular las métricas tomando como base una sola característica de la ruta. Se pueden calcular métricas más complejas combinando varias características. Las métricas utilizadas con mayor frecuencia por los enrutadores son las siguientes:

- ancho de banda: capacidad de transmisión de datos de un enlace; (normalmente, se prefiere un enlace Ethernet de 10 Mbps a una línea arrendada de 64 kbps)
- retardo: cantidad de tiempo requerido para transportar un paquete por cada enlace desde el origen hacia el destino
- carga: cantidad de actividad en un recurso de red tal como un enrutador o un enlace
- confiabilidad: generalmente se refiere al índice de error de cada enlace de red
- número de saltos: cantidad de enrutadores que un paquete debe atravesar antes de llegar a su destino

Una ruta dinámica es construida por información intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información que dinámicamente ajustan las rutas reflejadas en las condiciones de la red. Los protocolos de enrutamiento manejan complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacerlo.
Los protocolos de enrutamiento no sólo están diseñados para cambiar a una ruta de respaldo cuando la ruta primaria se vuelve inoperante sino que ellos también evalúan y deciden cual es la mejor ruta para un destino. Una red con múltiples caminos a un mismo destino puede utilizar enrutamiento dinámico.

- Al interior de un Sistema Autónomo: Interior Gateway Protocol (IGP)
- Entre Sistemas Autónomos: Border Gateway Protocol (BGP)

3.4.1 Protocolos IGP´s y EGP's.

Dejar el trabajo de actualización a los enrutadores implicó crear protocolos para que estos pudieran intercambiar información. Estos son los protocolos de enrutamiento dinámico, que pueden ser de dos tipos:

3.4.2 Protocolos EGP

Protocolos entre gateways (entradas) exteriores (Exterior Gateway Protocol EGP) los cuáles son utilizados para enrutar entre diferentes sistemas autónomos donde cada enrutador es responsable de la información de su propio sistema autónomo. Como ejemplo de este protocolo podemos citar al BGP (Border Gateway Protocol).

3.4.3 Protocolos IGP

Los IGP's (Interior Gateway Protocol) son usados para intercambiar información de enrutamiento entre enrutadores dentro de un sistema autónomo. Un sistema autónomo es un grupo de enrutadores intercambiando información a través de un protocolo de enrutamiento común. Generalmente se le conoce por sus siglas en inglés AS (Autonomous System). Cada sistema autónomo a la vez puede constituirse de un conjunto de hosts y enrutadores. También lo usan los enrutadores que ejecutan protocolos de enrutamiento exterior para recoger información de accesibilidad de la red para el AS. Los IGP más usados son, RIP (Routing Information Protocol), y el protocolo OSPF (Open Shortest Path First).

Antes de seguir adelante se debe establecer la diferencia entre enrutamiento y protocolos de enrutamiento. Enrutamiento es el acto de reenviar paquetes basados en la información de las tablas de enrutamiento. Los protocolos de enrutamiento se encargan de intercambiar la información usada para construir las tablas de enrutamiento. A continuación se muestran los detalles de los protocolos de enrutamiento.

3.4.4 Protocolos de Vector de Distancia

El término *Vector-Distancia se refiere* a una clase de algoritmos que usan los enrutadores para actualizar su información de enrutamiento. Cada enrutador comienza con un conjunto de rutas para aquellas con las que está directamente conectado, y posiblemente algunos enrutadores adicionales a otras redes o hosts si la topología de la red es tal que el protocolo de enrutamiento no es capaz de producir el enrutamiento deseado. Esta lista se guarda en una tabla de enrutamiento, en la que cada entrada identifica una red o host de destino y a la distancia a ella. Esta distancia se denomina *métrica* y se mide típicamente en saltos.
Periódicamente, cada enrutador envía una copia de su tabla de enrutamiento a cualquier otro enrutador que pueda alcanzar directamente. Cuando un informe le llega al enrutador B del A, B examina el conjunto de destinos que recibe y la distancia a cada uno. B actualizará su tabla de enrutamiento si:

- A conoce un camino más corto a cada destino.
- A lista un destino que B no tiene en su tabla.
- La distancia de A a un destino desde B pasando por A ha cambiado.

Esta clase de algoritmo es fácil de implementar, pero tiene un número de desventajas; cuando las rutas cambian rápidamente, es decir, aparece una nueva conexión o falla una vieja, la topología de enrutamiento puede no estabilizar la topología cambiada debido a que la información se propague lentamente y mientras se esté propagando, algunos "enrutadores" tengan información de enrutamiento incorrecta.
Otra desventaja es que cada "enrutador" tiene que enviar una copia de toda su tabla de enrutamiento a cada vecino a intervalos regulares. Por supuesto, se pueden usar intervalos más largos para reducir la carga de la red pero eso introduce problemas relacionados con la respuesta de la red a cambios en la topología.
Los algoritmos vector-distancia que usan la cuenta de saltos como métrica no tienen en cuenta la velocidad o la fiabilidad del enlace.
La tarea más difícil en uno de estos algoritmos es prevenir la inestabilidad

3.4.5 Protocolos de estado de Enlace

Los protocolos de estado de enlace crean una vista coherente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero por otro lado para lograr esto deben sufrir dificultades informáticas relativamente mayores y un tráfico más disperso (comparado con los protocolos de enrutamiento por vector distancia).

El concepto de este algoritmo es sencillo y puede describirse en cinco partes. Cada enrutador debe:

1. Descubrir a sus vecinos y conocer sus direcciones de red.
Al ponerse en operación un enrutador, su primera tarea es averiguar quiénes son sus vecinos; esto se logra enviando un paquete de saludo por cada línea punto a punto. Se espera que el enrutador del otro extremo envíe de regreso su dirección única.

Al conectarse dos o más enrutadores mediante una LAN, la situación es ligeramente más complicada.

2. Medición del costo de la línea.
El algoritmo de enrutamiento por estado de enlace requiere que cada enrutador sepa, o cuanto menos tenga una idea razonable del estado de cada uno de sus vecinos. La manera más directa de determinar este retardo es enviar un paquete especial a través de la línea, el cual debe enviar de regreso inmediatamente el otro lado. Si mide el tiempo de ida y vuelta y lo divide entre dos, el enrutador transmisor puede tener una idea razonable del retardo.

3. Construcción de los paquetes de estado de enlace.
Una vez que se ha recabado la información necesaria para el intercambio, el siguiente paso es que cada enrutador construya un paquete con todos los datos. Este paquete comienza con la identidad del transmisor, seguida de un número de secuencia, una edad y una lista de vecinos. Para cada vecino, se coloca el retardo a ese vecino.
Es fácil construir los paquetes de estado de enlace, la parte difícil es determinar cuándo construirlos. Una posibilidad es construirlos periódicamente, es decir, a intervalos regulares. Otra posibilidad es al ocurrir un evento significativo, como la caída o reactivación de una línea o de un vecino, o el cambio de sus propiedades.

4. Distribución de los paquetes de estado de enlace.
La parte mas complicada del algoritmo es la distribución confiable de los paquetes de estado de enlace. A medida que se distribuyen e instalan los paquetes, los enrutadores que reciban los primeros cambiarán sus rutas. En consecuencia, los distintos enrutadores podrían estar usando versiones diferentes de la topología, lo que puede conducir a inconsistencias, ciclos, máquinas inalcanzables, y otros problemas. El algoritmo que se utiliza para la distribución de los paquetes de estado de enlace seria inundación.

5. Cálculo de nuevas rutas.
Una vez que un enrutador ha acumulado un grupo completo de paquetes, puede construir la tabla de la subred completa porque todos los enlaces están representados. De hecho, cada enlace se representa dos veces, para cada dirección. Los dos valores pueden promediarse o usarse por separado. Ahora puede ejecutarse localmente el algoritmo de la trayectoria más corta posible a todos los destinos. Los resultados de este algoritmo pueden instalarse en las tablas de enrutamiento, y reiniciarse la operación normal. Para una subred con n enrutadores, cada uno de los cuales tiene k vecinos, la memoria requerida para almacenar los datos de entrada es proporcional a nk. En las subredes grandes este puede ser un problema, sin embargo en muchas situaciones prácticas, el enrutamiento por estado de enlace funciona bien. Se usa ampliamente en redes actuales, algunos protocolos que lo usan son: el protocolo OSPF y el IS-IS (sistema intermedio - sistema intermedio).
Enseguida se muestra una breve descripción de cómo opera cada protocolo de enrutamiento, refiriéndonos con esto a los dos tipos de protocolo, con sus respectivas clases de vector distancia y vector enlace.

Tipo de protocolo	Vector distancia	Estado enlace
IGPs	GGP Hello RIP IGRP	OSPF Integrated IS-IS SPF
EGPs	EGP BGP	IDRP

Tabla 3.1 Protocolos de vector distancia y estados de enlace

3.5 BGP (Protocolos de enlace exterior)

BGP (Border Gateway Protocol) representa un intento para dirigir los problemas más serios de EGP. El BGP es un protocolo de Sistema Inter Autónomo creado para uso en la Internet. A diferencia de EGP, BGP fue diseñado para detectar lazos de enrutamiento.

3.5.1 Tecnologías Básicas

Aunque BGP fue diseñado como un protocolo AS, éste puede ser usado entre y dentro del mismo. Dos BGP vecinos comunicándose entre Sistemas Autónomos deben residir en la misma red física. Los enrutadores BGP dentro del mismo Sistema Autónomo se comunican con algún otro para asegurar que ellos tienen una vista consistente del Sistema Autónomo y para determinar cual enrutador BGP servirá como punto de conexión para o de cierto sistema Autónomo externo. Algunos SA son meramente canales a través de los cuales pasa el tráfico de la red. Esto es, algunos AS transmiten el tráfico de red que no se originó dentro del mismo y no es destinado para el sistema autónomo. BGP debe interactuar con todos los protocolos de enrutamiento que transitan en este paso a través del AS. La actualización de mensajes de BGP consiste de pares de rutas de redes número/AS. La ruta del AS contiene la trama de los AS a través de los cuales la determinada red ha llegado. Estas actualizaciones de mensajes son enviadas sobre el protocolo de mecanismo de transporte TCP para asegurar la entrega confiable. El intercambio inicial de datos entre dos enrutadores mantiene intacta la tabla de enrutamiento BGP. Las actualizaciones son enviadas para el cambio de la tabla de enrutamiento. A diferencia de algunos otros protocolos de enrutamiento, BGP no requiere un período de refrescamiento de la tabla de enrutamiento. En lugar de esto, los enrutadores de BGP retienen la última versión de la tabla de enrutamiento. Aunque BGP mantiene una tabla de enrutamiento con todas las rutas factibles para una red particular, éste anuncia solamente la ruta primaria (optima) en sus mensajes de actualización.
La métrica BGP es una unidad de número arbitrario especificando el grado de preferencia de una ruta particular. Estas métricas son típicamente asignadas por el administrador de red a través de archivos de configuración. Los grados de preferencia pueden ser basados en algún número de criterios incluyendo contadores de AS (rutas

con el contador AS más pequeño son generalmente mejores), tipo de enlace (es el enlace estable, rápido, confiable) y otros factores.

3.5.2 Formato del Paquete de Datos

El formato de los paquetes BGP es el siguiente:

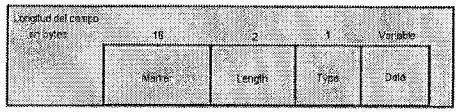


Figura 3.7 Formatos de los paquetes BGP

Los paquetes BGP tienen un header común de 19 bytes que consisten de tres campos. El *Marker,* que contiene un valor que el receptor del mensaje puede predecir. Este campo es usado para autentificación. El campo *Length*, contiene la total longitud total del mensaje, en bytes y por último el campo *Type*, que especifica el tipo de mensaje. Cuatro tipos de mensajes son especificados para el formato BGP:

- Open
- Update
- Notification
- Keepalive

Los mensajes con su función específica se muestran a continuación:

Open
Después que una conexión de protocolo de transporte es establecida, el primer mensaje mandado para cada lado son unos mensajes open. Si el mensaje open es aceptable para el receptor, un mensaje de keepalive, confirmando los mensajes open, es devuelto. Sobre una confirmación exitosa de los mensajes open, updates, keepalives y notifications pueden ser ejecutadas. En adición al header común del paquete, el mensaje open define varios campos. El campo *versión* provee un número de versión BGP, y permite que el receptor cheque que esta corriendo la misma versión del emisor. El campo *autonomous system* provee el número del AS del emisor. El campo *hold-time* indica el número máximo de segundos que pueden transcurrir sin recepción de un mensaje antes de que el transmisor es asumido como muerto. El campo *authentication code* indica que tipo de autentificación está siendo usado. El campo *authentication data* contiene datos de autentificación actual.

Update
Los mensajes update de BGP proveen actualizaciones de enrutamiento a otros sistemas BGP. Información en estos mensajes es usada para construir un grafo describiendo las interrelaciones de varios AS. In adición al header común BGP,

mensajes updates tienen varios campos adicionales. Estos campos proveen información de enrutamiento listando atributos de rutas correspondientes a cada red. BGP actualmente define cinco atributos:

- *Origin:* Puede tomar uno de los tres valores: *IGP*, *EGP*, o *incomplete*. El atributo IGP significa que la red es parte de un SA. El atributo EGP significa que la información fue originalmente aprendida del EGP. Implementaciones de BGP podrán estar inclinadas a preferir enrutadores IGP sobre enrutadores EGP debido a que esta tecnología falla en presencia de lazos de enrutamiento.
- *AS path:* Provee la lista actual de AS en la ruta de l destino
- *Next hop*: Provee la dirección IP del enrutador que podría ser usado como el próximo hop a las redes listadas en el mensaje update.
- *Unreachable*: Si está presente, indica que una ruta no es alcanzable.
- *Inter-AS metric*: Provee una manera para un enrutador BGP de avisar su costo al destino dentro de su propio SA. Esta información puede ser usada por enrutadores externos para los SA anunciantes para seleccionar una ruta óptima dentro del SA a un destino particular.

Notification

Mensajes Notification son enviados cuando una condición de error ha sido detectada, y un enrutador desea decirle a algún otro porque está cerrando la conexión entre ellos. Aparte del header común BGP, los mensajes de notificación tienen un campo de *error code*, un campo de *error subcode* y un campo *error data*. El campo error indica el tipo de falla, y puede ser uno de los siguientes:

- *Message header error*: Indica un problema con el header del mensaje en sí, un mensaje de length inaceptable, un valor del campo marker inaceptable, o un tipo de mensaje inaceptable.
- *Open message error*: Indica un problema con un mensaje open como tal, un version number no soportada, un número AS o dirección IP inaceptable, o un authentication code no soportada.
- *Update message error*: Indica un problema con los mensajes de actualización. Ejemplos incluyen una lista de atributos mal formados, una lista de errores de atributos, y un atributo de next-hop inválido.
- *Hold time expired*: Indica una expiración del hold-time, después del cual un nodo BGP puede ser declarado fuera de funcionamiento.

Keepalive

Mensajes keepalive no contienen ningún campo adicional más allá de aquellos en el encabezado (header) común de BGP. Estos mensajes son enviados bastante frecuente para resguardar el tiempo de expiración del hold-time.

3.6 IGP (Protocolos de enlace interior)

Los protocolos IGP (Interior gateway protocol) se utilizan para intercambiar información de enrutamiento entre enrutadores con un sólo sistema AS (Autonomous System).

También lo usan los enrutadores que ejecutan protocolos de enrutamiento exterior para recoger información de accesibilidad de la red para el AS. Los IGP más usados son, RIP (Routing Information Protocol), y el protocolo OSPF (Open Shortest Path First). Como se había comentado anteriormente, los protocolos se clasifican en protocolos de vector de distancias y de estado de enlace. El término Vector-Distancia se refiere a una clase de algoritmos que usan los enrutadores para actualizar su información de enrutamiento. Cada enrutador comienza con un conjunto de rutas para aquellas con las que está directamente conectado Esta lista se guarda en una tabla de enrutamiento, en la que cada entrada identifica una red o host de destino y la distancia a dicha red o host de destino. Esta distancia se denomina métrica y se mide típicamente en saltos (hops). Periódicamente, cada enrutador envía una copia de su tabla de enrutamiento a cualquier otro enrutador que pueda ser alcanzado directamente. Por ejemplo, Cuando un informe le llega a un enrutador B de parte de un enrutador A, B examina el conjunto de destinos que recibe y la distancia a cada uno. B actualizará su tabla de enrutamiento sí el enrutador A conoce un camino más corto a cada destino, o el enrutador A enlista un destino que B no tiene en su tabla de enrutamiento.

Esta clase de algoritmo es fácil de implementar, pero tiene un número de desventajas, por ejemplo, cuando las rutas cambian rápidamente, es decir, aparece una nueva conexión o falla una vieja conexión, la topología de enrutamiento puede no estabilizar la topología cambiada debido a que la información se propague lentamente, y mientras se esté propagando, algunos enrutadores tengan información de enrutamiento incorrecta. Otra desventaja es que cada enrutador tiene que enviar una copia de toda su tabla de enrutamiento a cada vecino a intervalos regulares. Por supuesto, se pueden usar intervalos más largos para reducir la carga de la red pero eso introduce problemas relacionados con la respuesta de la red a cambios en la topología. La tarea más difícil en uno de estos algoritmos es prevenir la inestabilidad. Existen distintas soluciones:

- Cuando las rutas cambian rápidamente, es decir, aparece una nueva conexión o falla una anterior, la topología de enrutamiento puede no concordar con la topología cambiada debido a que la información se propaga lentamente y mientras se esté propagando, algunos enrutadores tendrán información de enrutamiento incorrecta.
- Otra desventaja es que cada enrutador tiene que enviar una copia de toda su tabla de enrutamiento a cada vecino a intervalos regulares. Por supuesto, se pueden usar intervalos más largos para reducir la carga de la red pero eso introduce problemas relacionados con la respuesta de la red a cambios en la topología.
- Los algoritmos vector-distancia que usan la cuenta de saltos como métrica no tienen en cuenta la velocidad o la confiabilidad del enlace.

3.6.1 IGRP (Interior Gateway Routing Protocol)

La implementación inicial de IGRP fue montada sobre interconexión de redes usando IP. (IGP) trabaja con vector de distancias. El protocolo de enrutamiento de vector de distancias consiste en que cada enrutador manda toda o una porción de su tabla de enrutamiento en mensajes de update (actualización) en intervalos regulares a cada uno

de sus enrutadores vecinos. Como la información se prolifera a través de la red, los enrutadores pueden calcular distancias para todos los nodos dentro de la interconexión. IGRP usa combinaciones de métricas. Internetwork delay, bandwith, reliability y load son hechos tomados en cuenta para la decisión de enrutamiento. Los administradores de red pueden colocar el factor de peso para cada una de esas métricas, IGRP las utiliza ya sea que estén colocadas por el administrador o por default, para automáticamente calcular las rutas óptimas. Además IGRP provee un fino rango para sus métricas, lo cual permite mediciones satisfactorias en redes con pequeñas variaciones en sus características de desempeño. Además los componentes de las métricas son combinadas en algoritmos definidos por el usuario. Como resultado el administrador puede tener influencia en la selección de rutas en una manera intuitiva. Para proveer flexibilidad adicional, IGRP permite enrutamiento multitrayectoria. Líneas duales de igual ancho de banda pueden transmitir una cadena simple de tráfico en round-robin, con cambio automático a la segunda línea si una cae. También, múltiples caminos pueden ser usados si las métricas para ellos son diferentes.

3.6.2 Características de Estabilidad

IGRP provee un número de características que son diseñadas para aumentar su estabilidad. Estas incluyen hold-downs, split horizons y poison reverse updates.
Hold-downs son usadas para prevenir mensajes update (de actualizacÿÿn) regulares de restitución inapropiada de una ruta que puÿÿla cueÿÿvenido mal. Cuando un enrutador cae, los enrutadores vecinos detectan esto a través de la escasez de mensajes update regularmente. Estos enrutadores calculan entonces nuevas rutas y mandan mensajes update para informar a sus vecinos del cambio de rutas. Esta actividad comienza una onda de actualizaciones disparadas que se filtran a través de la red. Estas actualizaciones disparadas no llegan instantáneamente a cada dispositivo de la red, por lo que es posible que un dispositivo que no haya sido todavía informado del fallo de la red mande un mensaje update regular a un dispositivo que ha sido notificado del fallo. en este caso, el último dispositivo podría contener información incorrecta de enrutamiento. Hold-downs es un intervalo de tiempo durante el cual los enrutadores moderan .Cualquier cambio que podría afectar rutas para algún período de tiempo. El período hold-down es usualmente calculado para ser más grande que el período de tiempo necesario para actualizar la red completa con un cambio de enrutamiento. Split horizons deriva del hecho de que nunca es útil mandar información sobre una ruta de regreso en la dirección de la cual este viene. Por ejemplo consideremos la siguiente figura:

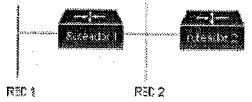


Figura 3.8 Split Horizons

El enrutador 1 (R1) inicialmente anuncia que tiene una ruta a la red A. No hay razón para que el enrutador 2 (R2) incluya esta ruta en su actualización de regreso a R1. La regla de split-horizon dice que R2 debería perder esta ruta de cualquier actualización que mande a R1.La regla de split-horizon ayuda a prevenir lazos de enrutamiento. Por ejemplo consideremos el caso donde la interfase de R1 a la red A cae. Sin split horizons, R2 continúa informando a la red A a través de R1. Si R1 no tiene suficiente inteligencia, este puede actualmente tomar la ruta de R2 como una ruta alternativa para su fallo de conexión directa, causando un lazo. Aunque hold-dows podría prevenir esto, split horizons son implementados en IGRP debido a que este provee algoritmo extra de estabilidad.

Poison Reverse Updates

Mientras split horizons podría prevenir lazos entre enrutadores adyacentes, poison reverse updates son destinado para vencer lazos de enrutamiento mas grandes. Incremento en las métricas de enrutamiento generalmente indica lazos. Poison reverse updates son entonces mandados para remover la ruta y colocarlo en hold-down.

Timers

IGRP mantiene un número de temporizadores y variables que contienen intervalos de tiempo. Esto incluye un temporizador de update, de inválido, de periodo hold-down, y flush timer.

Tipos de paquetes

IGRP Aumentado usa los siguientes tipos de paquetes:

- *Hello* and *acknowledgment: Paquetes* Hello son Multicast para el descubrimiento y recuperación de vecinos y no requiere acknowledgment. Un paquete *acknowledgment* es un paquete hello que no contiene data. Paquetes Acknowledgment contiene un número diferente de cero, y son siempre enviados con dirección unicast.
- *Update*: Paquetes update son usados para convenir alcanzabilidad de destinos. Cuando un vecino es descubierto, paquetes update unicast son enviados, por lo que el vecino puede construir su tabla de topología. En otro caso, los updates son Multicast.
- *Query* and *reply*: Paqutes Query and reply son enviados cuando un destino no posee sucesores factibles. Paquetes Query son siempre Multicast. Paquetes Reply son enviados en respuesta a paquetes query para indicar al emisor que no es necesario recalcular la ruta porque hay sucesores factibles. Paquetes Reply son unicast al emisor del query.
- *Request*: Paquetes Request son usados para obtener información específica de uno o más vecinos. Paquetes Request packets son usados en rutas servidor aplicaciones y pueden ser multi o unicast.

3.6.3 Tabla de Vecinos

Cuando un enrutador descubre a un vecino, este registra la dirección e interfaces de este vecino como una entrada en la tabla de Vecinos. Hay una tabla para cada modulo

dependiente del protocolo. Cuando un vecino manda un paquete Hello, este anuncia un hold time.

3.6.4 Tablas de Topología

La tabla de topología contiene todos los destinos avisados por los enrutadores vecinos. Cada entrada en la tabla incluye la dirección destino y una lista de vecinos que han anunciado este destino. Para cada vecino, la entrada registra las métricas anunciadas, las cuales guarda el vecino en su tabla de enrutamiento.

3.7 RIP (Routing Information Protocol)

RIP es una implementación directa del enrutamiento vector-distancia para LANs. RIP opera en uno de dos modos: activo (normalmente usado por enrutadores) y pasivo (normalmente usado por hosts). La diferencia entre los dos se explica más adelante.Los mensajes RIP se envían en diagramas de datos UDP y cada uno contiene hasta 25 pares de números como se mustra en la figura siguiente:

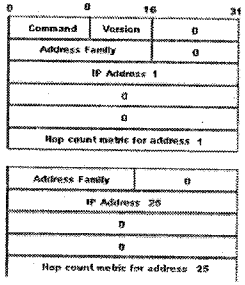


Figura 3.9 Mensaje RIP

En un mensaje RIP se pueden enlistar entre 1 y 25 rutas. Con 25 rutas el mensaje tiene 504 bytes (25x20+4) que es el tamaño máximo que se puede transmitir en un datagrama UDP de 512 bytes.Para describir el datagrama se tiene que:

- *Command* es 1 para una petición RIP o 2 para una respuesta,
- *Version* es 1,
- *Address Family* es 2 para direcciones IP,
- *IP address* es la dirección IP de para esta entrada de enrutamiento: un host o una subred(caso en el que el número de host es cero),
- *Hop count metric es* el número de saltos hasta el destino. La cuenta de saltos para una interfaz conectada directamente es de 1, y cada enrutador intermedio la incrementa en 1 hasta un máximo de 15, con 16 indicando que no existe ruta

hasta el destino. Tanto el modo activo como el pasivo escuchan todos los mensajes de broadcast y actualizan su tabla de enrutamiento según el algoritmo vector-distancia descrito antes.

3.7.1 Operaciones básicas

Cuando RIP se inicia envía un mensaje a cada uno de sus vecinos pidiendo una copia de la tabla de enrutamiento del vecino, este mensaje es una solicitud (el campo command se pone a 1) con address family a 0 y metric a 16. Los enrutadores vecinos devuelven una copia de sus tablas de enrutamiento. Cuando RIP está en modo activo envía toda o parte de su tabla de enrutamiento a todos los vecinos (por broadcastadcast) y/o con enlaces punto a punto. Esto se hace cada 30 segundos. La tabla de enrutamiento se envía como respuesta (command vale 2), aun que no haya habido petición). Cuando RIP descubre que una métrica ha cambiado, la difunde por broadcast a los demás enrutadores. Cuando RIP recibe una respuesta, el mensaje se valida y la tabla local se actualiza si es necesario. Para mejorar el rendimiento y la fiabilidad, RIP especifica que una vez que un enrutador (o host) a aprendido una ruta de otro, debe guardarla hasta que conozca una mejor (de costo estrictamente menor). Esto evita que los enrutadores oscilen entre dos o más rutas de igual costo. Cuando RIP recibe una petición, distinta de la solicitud de su tabla, se devuelve como respuesta la métrica para cada entrada de dicha petición fijada al valor de la tabla local de enrutamiento. Si no existe ruta en la tabla local, se coloca en 16. Las rutas que RIP aprende de otros enrutadores expiran a menos que se vuelvan a difundir en 180 segundos (6 ciclos de broadcast). Cuando una ruta expira, su métrica se pone a infinito, la invalidación de la ruta se difunde a los vecinos, y 60 segundos más tarde, se borra de la tabla.

3.7.2 Limitaciones

RIP no está diseñado para resolver cualquier posible problema de enrutamiento. Entre los posibles candidatos están OSPF (Open Shortest Path First Protocol) y el IS-IS (Intermediate System to Intermediate System). Sin embargo, RIP tiene limitaciones, por ejemplo, el costo máximo permitido en RIP es 16, que significa que la red es inalcanzable. De esta forma, RIP es inadecuado para redes grandes(es decir, aquellas en las que la cuenta de saltos puede aproximarse perfectamente a 16), además RIP no soporta máscaras de subred de longitud variable (VLSM). En un mensaje RIP versión 1 no hay ningún modo de especificar una máscara de subred asociada a una dirección IP. RIP carece de servicios para garantizar que las actualizaciones proceden de enrutadores autorizados. Es un protocolo inseguro además que sólo usa métricas fijas para comparar rutas alternativas. No es apropiado para situaciones en las que las rutas necesitan elegirse basándose en parámetros de tiempo real tales como el retardo, la confiabilidad o la carga. El protocolo depende de la cuenta hasta infinito para resolver algunas situaciones inusuales.
Como se describió antes, la resolución de un bucle requeriría mucho tiempo (si la frecuencia de actualizaciones fuese limitada) o mucho ancho de banda (si las actualizaciones se enviasen por cada cambio producido).

A medida que crece el tamaño del dominio, la inestabilidad del algoritmo vector-distancia de cara al cambio de topología se hace patente. RIP especifica mecanismos para minimizar los problemas con la cuenta hasta infinito que permiten usarlo con dominios mayores, pero eventualmente su operatividad será nula. No existe un límite superior prefijado, pero a escala práctica este depende de la frecuencia de cambios en la topología, los detalles de la topología de la red, y lo que se considere como un intervalo máximo de tiempo para que la topología de enrutamiento se estabilice.

3.7.3 Split horizon con poisoned reverse

Consideremos una red, por ejemplo la de conteo hasta infinito, como se muestra en la siguiente figura:

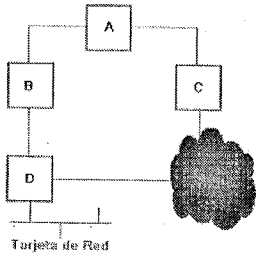


Figura 3.10 Problemas de la cuenta hasta infinito

Como se describió en la técnica de vector distancia, el problema lo causaba el hecho de que A y C se descartan mutuamente. Cada uno afirma ser capaz de alcanzar a D a través del otro. Este hecho se puede evitar siendo más cuidadoso con el destino de la información. En particular, nunca es útil afirmar la accesibilidad a una red de destino a través del vecino del que se aprendió la ruta. El método split horizon con poisoned reverse incluye las rutas en las actualizaciones enviadas al enrutador al que se aprendieron, pero pone sus métricas a infinito. Si dos enrutadores tienen rutas apuntándose recíprocamente, al anunciar las rutas en bucle con métrica de 16 romperá el bucle inmediatamente.
Si simplemente no se anuncian estas rutas (esquema conocido como simple split horizon), las rutas erróneas tendrán que ser eliminadas tras un tiempo fuera. Poisoned reverse tiene una desventaja: incrementa el tamaño de los mensajes de enrutamiento.

3.7.4 Triggered Updates

Split horizon con poisoned reverse evita cualquier bucle que implique sólo dos pasarelas. Sin embargo, aún es posible acabar con situaciones de este tipo. Por ejemplo, A puede creer que tiene una ruta a través de B, B a través de C, y C a través

de A. Esto no se puede solucionar con el método split horizon. Este bucle sólo se arreglará cuando la métrica alcance infinito y la red o el host implicados se declaren inaccesibles. El método triggered updates es un intento de acelerar esta convergencia. Siempre que un enrutador cambia la métrica de una ruta, se le requiere que envía mensajes casi inmediatamente, incluso aunque no sea el momento de una actualización (RIP especifica un pequeño intervalo, entre 1 y 5 segundos, con el fin de evitar que estas actualizaciones generen un tráfico de red excesivo).

3.8 RIP2 (Routing Information Protocol Versión 2)

RIP-2 tiene las ventajas de una fácil implementación y menores factores de carga. La intención de RIP-2 es proporcionar una sustitución directa de RIP que se pueda usar en redes pequeñas y medianas, en presencia de subredes variables(VLSM) o (CIDR) y, sobre todo, que pueda interactuar con RIP-1. RIP-2 aprovecha que la mitad de los bytes de un mensaje RIP están reservados (deben ser cero) y que la especificación original estaba diseñada con las mejoras en la mente de los desarrolladores, particularmente en el uso del campo de versión. Un área notable en la que este no es el caso es la interpretación del campo de métrica. RIP-1 lo especifica con un valor de 0 a 16 almacenado en un campo de 4 bytes. Por compatibilidad, RIP-2 preserva esta definición, lo que significa en que interpreta 16 como infinito, y desperdicia la mayor parte del rango de este campo. Ni RIP-1 ni RIP-2 son adecuados para ser usados como IGP en un AS en el que el valor de 16 sea demasiado bajo para ser considerado infinito, ya que los valores altos del infinito aumentan el problema de la cuenta hasta infinito.
El protocolo estado del enlace, más sofisticado, usado en OSPF y en IS-IS proporciona una solución de enrutamiento mucho mejor cuando el AS es lo bastante largo para tener una cuenta de saltos cercana a 16.
El formato del mensaje RIP-2 se muestra en la siguiente figura:

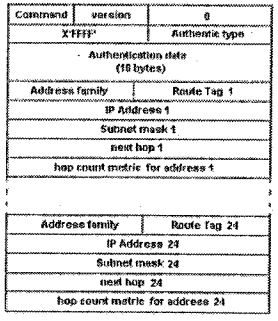


Figura 3.11 Mensaje RIP versión 2

La primera entrada del mensaje puede ser una entrada de autentificación, como se muestra en la figura, o una ruta como en el mensaje RIP. Si la primera entrada es de autentificación, sólo se pueden incluir 24 rutas en el mensaje; de otro modo, el máximo es 25, como en RIP. Los campos del mensaje RIP-2 son los mismos que en RIP excepto los siguientes:

- Versión: es 2. Le dice al "enrutador" RIP-1 que ignore los campos reservados, los que deben ser cero (si el valor es 1, los enrutadores deben desechar los mensaje con valores distintos de cero en estos campos, ya que los originó un enrutador que dice ser RIP, pero que envía mensajes que no cumplen el protocolo).
- Address Family: puede ser X'FFFF' sólo en la primera entrada, indicando que se trata de una entrada de autentificación.
- Authentication Type: Define como se han de usar los restantes 16 bytes. Los únicos tipos definidos son 0, indicando ninguna autentificación, y 2 indicando que el campo contiene datos de password.
- Authentication Data: el password es de 16 bytes, texto ASCII plano, alineado a la izquierda y rellenado con caracteres nulos ASCII (X'00').
- Route Tag: es un campo dirigido a la comunicación de información acerca del origen de la información de enrutamiento. Está diseñado para la interoperabilidad entre RIP y otros protocolos de enrutamiento. Las implementaciones de RIP-2 deben conservarlo, aunque RIP-2 no especifica como se debe usar.
- Subnet Mask: la máscara de subred asociada con la subred a la que se refiere esta entrada.
- Next Hop Una recomendación acerca del siguiente salto que el "enrutador" debería usar para enviar datagramas a la subred o al host dado en la entrada.

- Para asegurar una interoperabilidad segura con RIP se debe de cumplir con las siguientes restricciones para los enrutadores RIP-2 que transmiten sobre una interfaz de red en la que un enrutador RIP puede escuchar y operar con mensajes RIP.

- La información interna a una red nunca se debe anunciar a otra red.
- La información acerca de una subred más específica no se debe anunciar donde los enrutadores vean una ruta de host.
- Las rutas a superredes (rutas con una máscara de subred más corta que la máscara natural de la red) no se deben anunciar en los sitios en los que puedan ser malentendidas por los enrutadores RIP.
- RIP versión 2 soporta además el Multicast con preferencia al broadcast. Esto puede reducir la carga de los host que no están a la escucha de mensajes RIP-2. Esta opción es configurable para cada interfaz para asegurar un uso óptimo de los servicios RIP-2 cuando un enrutador conecta redes mixtas RIP-1/RIP-2 con redes RIP-2. Similarmente, el uso de la autentificación en entornos mixtos se puede configurar para adecuarse a los requerimientos locales.

3.9 Open Shortest Path First (OSPF)

OSPF tiene dos características primarias. La primera es que es abierto, en que su especificación esta en el dominio público. La segunda característica principal es que está basado en el algoritmo SPF.
El algoritmo de enrutamiento SPF es la base de la operación para OSPF. Cuando un enrutador SPF es encendido, este inicializa su estructura de datos del protocolo de enrutamiento y entonces espera las indicaciones de protocolos de capas inferiores para que sus interfaces sean funcionales. Una vez que un enrutador esta seguro que sus interfaces están funcionando, este usa el protocolo OSPF para adquirir vecinos. Los vecinos son enrutadores con interfaces a una red común. El enrutador envía paquetes de saludo a sus vecinos y reciben sus paquetes de saludo. En redes multi-acceso (redes que soportan mas de 2 enrutadores), el protocolo Hello elige un enrutador designado y un enrutador designado suplente. El enrutador designado es responsable, entre otras cosas, de generar los LSA de la red multi-acceso entera. El enrutador designado permite una reducción en el tráfico de red y en el tamaño de la base de datos topológica. Cuando la base de datos del estado de enlace de dos enrutadores vecinos es sincronizada, los enrutadores se dicen adyacentes. En redes multi-acceso, el enrutador designado determina cuales enrutadores deberían convertirse en adyacentes. Las bases de datos son sincronizadas entre enrutadores adyacentes. Adyacencias controla la distribución de paquetes del protocolo de enrutamiento. Estos paquetes son enviados y recibidos solamente en adyacencias.
Cada enrutador, periódicamente, manda un LSA. Los LSA son también enviados cuando el estado de un enrutador cambia. Los LSA incluyen información en las adyacencias de los enrutadores. Por comparación establecida entre adyacencias y estados de enlaces, fallas en los enrutadores pueden ser detectadas más rápidamente y la topología de la red ser alterada apropiadamente.

3.9.1 Tecnologías Básicas

OSPF es un protocolo de enrutamiento de estado de enlace. Así, este manda un anuncio de estado de enlace (LSA) a todos los otros enrutadores dentro de la misma área jerárquica. Información de interfaces adheridas, métricas usadas, y otras variables son incluidas en los LSA de OSPF. Como los enrutadores OSPF acumulan información de los estados de enlace, ellos usan el algoritmo SPF para calcular el camino más corto a cada nodo. Como un protocolo de enrutamiento con estado de enlace, OSPF contrasta con *Routing Information Protocol (RIP)* y IGRP, los cuales utilizan algoritmos de enrutamiento tipo *vector de distancia*.

3.9.2 Jerarquía de enrutamiento

A diferencia de RIP, OSPF puede operar dentro de una jerarquía. La entidad más grande dentro de la jerarquía es el sistema autónomo (AS). Un sistema autónomo es una colección de redes bajo una administración común, compartiendo una misma

estrategia de enrutamiento. OSPF es un protocolo intra-AS (gateway interior), aunque es capaz de recibir y de enviar rutas a otros AS.

Un AS puede ser dividido en un número de áreas. Un área es un grupo de redes contiguas y hosts adjuntos. Los enrutadores con múltiples interfaces pueden participar en múltiples áreas. Estos enrutadores, mantienen bases de datos topológicas separadas para cada área. Una *Base de datos topológica* es esencialmente un dibujo total de la redes en interrelación con los enrutadores. La base de datos topológica contiene la colección de LSA recibidos de todos los enrutadores en la misma área. Debido a que los enrutadores dentro de la misma área comparten la misma información, ellos tienen bases de datos topológicas idénticas. El termino *dominio* es algunas veces usado para describir una porción de la red en la cual todos los enrutadores tienen idénticas bases de datos topológicas. El dominio es frecuentemente usado intercambiablemente con AS.

La topología de un área es invisible para las entidades fuera de ésta. Guardando topologías de áreas separadas, OSPF pasa menos trafico de enrutamiento que si el AS no fuera particionado. Particionar en áreas crea dos tipos diferentes de enrutamiento OSPF, dependiendo de sí la fuente y el destino están en la misma o en diferentes áreas. Enrutamiento intra-área ocurre cuando la fuente y el destino están en la misma área; enrutamiento Inter-área ocurre cuando ellos están en áreas diferentes. Un área principal, o backbone OSPF es responsable de la distribución de la información de enrutamiento entre áreas. Esto consiste de todos los enrutadores llamados enrutadores de frontera, los cuales interconectan a varias redes. La figura siguiente muestra un ejemplo de una red interconectada con varias áreas.

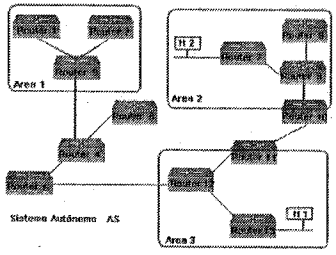


Figura 3.12 Red interconectada con varias áreas

En esta figura, los enrutadores 4, 5, 6, 10,11 y 12 conforman el backbone. Si el host H 1 que se encuentra en el área 3 desea mandar un paquete al host H2 in el área 2, el paquete es enviado al enrutador 13, el cual adelanta el paquete al enrutador 12, quien lo manda al enrutador 11. Este último lo manda a lo largo del backbone al enrutador 10, el cual envía el paquete a través de dos enrutadores intra-área (9 y 7) para ser enviado al host H2. El backbone en si mismo es un área OSPF, por lo tanto todos los enrutadores en él usan los mismos procedimientos y algoritmos para mantener la información de enrutamiento dentro de este. La topología del backbone es invisible a todos los enrutadores intra-área.

3.9.3 Formato del paquete

Todos los paquetes comienzan con un encabezado de 24 bytes, como es mostrado en la figura.

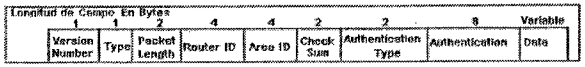


Figura 3.13 Formato de encabezado OSPF

Los campos del encabezado OSPF son los siguientes:

1) *Version number*: Identifica la implementación particular de OSPF que esta siendo usada.
2) *Type*: Especifica uno de los cinco tipos de paquetes OSPF:

- *Hello*: Mandada en intervalos regulares para establecer y mantener las interrelaciones con sus vecinos.
- *Database description*: Describe el contenido de la base de datos topológica. y son intercambiadas cuando una adyacencia esta siendo inicializada.
- *Link state request*: Peticiona piezas de la base de datos topológica de su vecino, Ellos son intercambiados después que un enrutador ha descubierto (a través de la inspección de los paquetes de la base de datos) que partes de su base de datos topológica esta fuera de fecha.
- *Link state update*: Responde a la petición de paquetes de estado de enlace. Ellos son también usados para la dispersión de los LSA. Varios LSA pueden ser incluidos dentro de un paquete simple.
- *Link state acknowledgment*: Reconocimiento de paquetes de actualizaciones de estados de enlace. Los paquetes de actualizaciones de estados de enlace deben ser explícitamente reconocidos para asegurar que el estado de enlace inundado a través de un área es un proceso confiable. Cada LSA en un paquete de actualización de estados de enlace contiene un campo type. Hay cuatro tipos de LSA:
- *Enrutador links advertisements* (RLA): Describe los estados coleccionados de los enlaces de un enrutador a un área específica. Un enrutador manda un RLAS para cada área a la cual el pertenece. RLA son inundados en el área entera, y no más.
- *Network links advertisements* (NLA): Mandados por el enrutador designado. Ellos describen todos los enrutadores que son adjuntos a una red multi- acceso, y son distribuidos en el área que contiene la red multi- acceso.
- *Summary links advertisements* (SLA): Resume rutas a destinos fueras de area, pero dentro de un SA. Ellos son generados por los *área border enrutadores*, y son distribuidos en el área. Solamente rutas intra-área son anunciadas dentro del esqueleto. Ambas, rutas intra e Inter-área, son anunciadas en otras áreas.
- *AS external links advertisements*: Describe una ruta a un destino que es externo al SA. Anuncios de enlaces a SA externos son originados por un enrutador limite del SA. Este tipo de anuncio el único tipo que es siempre enviado en el SA; todos los otros son enviados solamente dentro de áreas especificas.

3) *Enrutador ID*: Identifica la fuente del paquete.
4) *Packet length*: Especifica la longitud del paquete en bytes, incluyendo el Encabezado OSPF.
5) *Area ID*: Identifica el área a la cual pertenece el paquete. Todos los paquetes OSPF son asociados con un área.
6) *Checksum*: Chequea el contenido completo del paquete de daña potenciales sufridos en transito.
7) *Authentication type*: Contiene el tipo de autentificación. "Simple password" es un ejemplo de un tipo de autentificación. Todos los intercambios del protocolo OSPF son autentificados. El tipo de autentificación es configurable en una base por área.
8) *Authentication*: Contiene la información de autentificación y su longitud es de 64 bits.

3.9.4 Características adicionales de OSPF

La incorporación de características adicionales a OSPF incluyen igual costo, enrutamiento multitrayectoria y enrutamiento de peticiones de tipo de servicio basado en capas superiores. El enrutamiento basado en tipo de servicio (TOS) soporta que los protocolos de aquellas capas superiores puedan especificar tipos de servicio. Por ejemplo, una aplicación podría especificar que cierto dato es urgente. Si OSPF tiene enlaces de alta prioridad y su disposición, este puede ser usado para transportar el datagrama urgente. OSPF soporta una o más métricas. Si solo una métrica es usada, es considerada arbitraria, y TOS no es soportada. Si mas de una métrica es usada, TOS es opcionalmente soportada a través del uso de una métrica separada (y, por lo tanto, una tabla de enrutamiento separada) para cada uno de sus ocho combinaciones creadas por los tres bits de TOS IP (los bits de delay, throughput y reliability) Por ejemplo si el bit del TOS IP especifica bajo delay, bajo throughput y alta reliability, OSPF calcula rutas para todas para todos los destinos basados en designación de TOS. Las máscaras de subredes IP son incluidas con cada destino anunciado, habilitando mascaras de subredes de longitud variable (VLSM). Con mascaras de subredes de longitud variable, un red IP puede ser particionada en varias subredes de varios tamaños. Esto provee administradores de red con flexibilidad extra de configuración de redes.

3.9.5 IS-IS (Intermediate System to Intermediate System)

IS-IS es un protocolo similar a OSPF: también emplea el estado del enlace, el algoritmo SPF. Sin embargo, IS-IS es un protocolo OSI usado para los paquetes CLNP (*Connectionless Network Protocol)* en un dominio de enrutamiento. CLNP es el protocolo OSI más comparable a IP. El IS-IS integrado extiende IS-IS para compararse a TCP/IP. Su meta es proporcionar un solo (y eficiente) protocolo de enrutamiento para TCP/IP y para OSI. Su diseño hace uso del protocolo de enrutamiento OSI IS-IS, aumentado con información IP especifica, y proporciona apoyo explícito para subredes IP, máscaras de red variable, y enrutamiento externo, además de recurso para la

autentificación. El IS-IS integrado se basa en el mismo algoritmo de enrutamiento que OSPF, el cual describimos con anterioridad. No emplea encapsulación mutua de los paquetes IP y CLNP: ambos tipos se envían tal como son, ni cambia el comportamiento del enrutador. Se comporta como un IGP en una red TCP/IP y en una red OSI. El único cambio es la adición de información adicional relacionada con IP. Este protocolo agrupa las redes en dominios de modo análogo a OSPF. Un dominio de enrutamiento es análogo a un AS, y se subdivide en áreas, exactamente como OSPF. Aquí hay una descripción de los aspectos más importantes del enrutamiento IS-IS. Cuando es posible, se hacen comparaciones con conceptos equivalentes de OSPF. Los enrutadores se dividen en enrutadores de nivel 1, que no saben nada de la topología fuera de sus áreas, y de nivel 2, que conocen la topología de nivel superior, pero no saben nada de la topología que existe dentro de las áreas, a menos que sean también enrutadores de nivel 1. Dichos enrutadores de nivel 1 pueden pertenecer a más de un área, pero a diferencia de OSPF esto no se hace con propósitos de enrutamiento sino para facilitar la gestión del dominio, y normalmente por poco tiempo. Un enrutador de nivel 1 reconoce a otro como un vecino si están en la misma área. Un enrutador de nivel 2 reconoce a todos los demás de nivel 2 como vecinos. Un enrutador de nivel 2 puede ser también un enrutador de nivel 1 en un área, pero no en más. Hay una troncal de nivel 2 que contiene todos los enrutadores de nivel dos. El esquema de dirección OSI identifica explícitamente el área objetivo de un paquete, permitiendo una selección sencilla de las rutas del modo siguiente:

- Los enrutadores de nivel 2 enrutan hacia el área sin importarles su estructura interna.
- Los enrutadores de nivel 1 enrutan hacia el destino si está en su área, o al enrutador de nivel 2 más cercano.

Capítulo 4

VPN'S BASADAS EN MPLS

Capitulo 4 VPN's BASADAS EN MPLS

4.1 Introducción

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, suponen cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90's y a principios del nuevo siglo que apenas comienza. Esta situación se mejora con una nueva arquitectura de red de reciente aparición, conocida como Multi-Protocol Label Switching (MPLS) la cual es la tecnología de red que trataremos en este capitulo. MPLS se considera fundamental en la construcción de los nuevos cimientos para la Internet de este siglo. Se aprovecha esta introducción para avanzar un aspecto fundamental del MPLS, que consiste en la clara separación entre las funciones de routing (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de forwarding (es decir el envío en sí de datos entre elementos de la red). La segunda parte de este capítulo centra en la descripción funcional del MPLS, en concreto, se presenta la utilidad del MPLS para el soporte de aplicaciones de: ingeniería de tráfico, de diferenciación de servicios en distintas clases (Co'S) y de establecimiento de redes privadas virtuales (VPN's) sobre una topología "inteligente", muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales.

MPLS como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. MPLS integra sin discontinuidades los niveles de capa 2 (enlace) y 3 (red), combinando eficazmente las funciones de control del ruteo con la simplicidad y rapidez de la conmutación de capa 2. Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de enrutamiento y el envío en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del enrutamiento con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido.

Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de

envío de paquetes, los objetivos establecidos para este estándar son:

- MPLS debe funcionar sobre cualquier tecnología de capa dos, no sólo ATM
- MPLS debe soportar el envío de paquetes tanto Unicast como Multicast
- MPLS debe permitir el crecimiento constante de la Internet
- MPLS debe ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP en caso de que se trate de un LSR. Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet). Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

4.2 Conceptos Generales de VPN's

A medida que las computadoras fueron incorporadas a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de dichas empresas. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fue inicialmente las líneas telefónicas, y después las líneas dedicadas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. El gran inconveniente del uso de las líneas dedicadas es su alto costo en el que se tienen en cuenta la distancia. Las VPN (Virtual Private Networks) son una alternativa a la conexión WAN, bajando los costos y brindando los mismos servicios.

4.2.1 Definición y estructura

Una VPN (Red Privada Virtual) es un mecanismo de comunicación que permite conectar una o más redes mediante una red pública, generalmente Internet, de forma que estas redes parezcan para cada uno de sus elementos sólo una red privada(Virtual) más, manteniendo su privacidad.

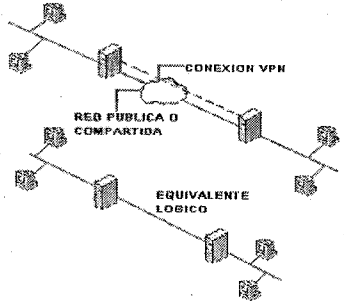


Figura 4.1 Estructura de una VPN

Una solución VPN se define según la extensión de las características ofrecidas. Una VPN debe proteger contra ataques a la información; asegurar la entrega confiable de datos en situaciones críticas y ser fácilmente administrable para la empresa. Una solución VPN tiene los siguientes componentes

- *Proveedor de Servicios.* que es una organización dueña de la infraestructura (el equipo y el medio de transmisión) que proporciona líneas dedicadas a sus clientes. El Proveedor de Servicios ofrece al cliente un servicio de Red Privada Virtual.
- *El cliente.* quien se conecta a la red del proveedor de servicio a través del Equipo en Sitio del Cliente (CPE, Customer Permises Equipment). El dispositivo CPE es también llamado CE (Customer Edge). El cliente es quien paga por los servicios de una VPN.
- *El dispositivo CE.* el cual se conecta a través del medio de transmisión (usualmente es una línea dedicada, pero también puede ser una conexión de línea conmutada) hacia el equipo del Proveedor de Servicios, el cual puede ser un conmutador X.25 o Frame Relay o ATM. También puede ser un enrutador IP. El CE es generalmente un dispositivo ensamblador y des ensamblador de paquetes (PAD, Packet Assembly and Disassembly). Este provee la conectividad del puente o el enrutador en la terminal.
- *El dispositivo PE.* que es la frontera del proveedor de servicio (Provider Edge). El PE interconecta a los dispositivos CE con la red del Proveedor de Servicios.
- *Dispositivos P.* Frecuentemente el proveedor de servicio tiene un equipo adicional en el corazón de su red (conocida también como P-Network o Red-P). Estos dispositivos son llamados Dispositivos-P (P-Devices), y como ejemplo están los Enrutadores-P (P-Enrutadores) o Conmutadores-P (P-Switches).
- *El sitio.* La parte contigua a la red del cliente es llamada sitio (site). Uno se puede conectar a la Red-P a través de una o varias líneas de transmisión, usando uno o varios dispositivos CE y PE, según los requerimientos de redundancia.

Las líneas dedicadas se proporcionan de forma local al cliente por el Proveedor de Servicios sobre el modelo VPN.
Cuando conectamos redes geográficamente distantes, lo normal es utilizar líneas dedicadas. Aunque el nombre puede llevar a cierta confusión, las líneas dedicadas pueden ser cualquier cosa, desde las tradicionales T (T1, T3 o análogas europeas, E), líneas OC (OC3, OC12, OC48, OC192) o enlaces inalámbricos (microondas, RF o satélite). Las líneas son dedicadas porque el ancho de banda que proporcionan es de su propietario. Las líneas dedicadas son buenas para algunas aplicaciones, una línea dedicada podría ser una buena elección porque ofrece un ancho de banda garantizado. Además podemos negociar líneas dedicadas según el rendimiento que necesitemos.
Otra ventaja de las líneas dedicadas es que siempre están (o deberían estar) disponibles. Como controlamos el equipo que mantiene la conexión, tenemos un control razonable sobre ella, la nube WAN está muy controlada y normalmente tiene enlaces redundantes con capacidad de recuperación automática ante fallos. La probabilidad de que experimentemos una caída como resultado de un fallo de una nube WAN es relativamente baja. Aunque una línea dedicada tiene ventajas en determinadas situaciones, puede ser muy costosa. Además con una VPN no se tiene que invertir en otras líneas dedicadas en caso de futuras migraciones o esfuerzos de expansión.

Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio.

Otra de las ventajas es la escalabilidad. La implementación y configuración de la VPN es sencilla y rápida, permitiendo un crecimiento escalable en cantidad de puntos. De esta manera evitamos el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet, se deriva simplemente en accesos distribuidos geográficamente.
En general, una VPN ofrece más ventajas que las redes basadas en líneas dedicadas:

- Costos más bajos que en las redes privadas: el costo total se reduce con el bajo costo del transporte de los datos, del ancho de banda, del equipo para el backbone y de operaciones.
- Arquitecturas más flexibles y escalables que las clásicas redes WAN, además de que habilita a las empresas para extender su conectividad rápidamente y a costo s efectivos y facilita la conexión o desconexión a oficinas remotas, locaciones internacionales, usuarios móviles o a redes de las empresas socias, según se requiera.
- Reducida administración de la carga en comparación con las redes privadas propias, pues las empresas pueden relegar la administración de su red a un Proveedor de Servicios y se enfocan más en los negocios que les competen.
- Topologías de red más simples, resultado de una reducida administración de la carga. Utilizar un backbone IP elimina los Circuitos Virtuales Permanentes (PVC's) asociados a los protocolos orientados a conexión, tales como ATM o Frame Relay. Además de que crea una topología de malla completa que disminuye el costo y la complejidad de la red.

También, una VPN bien diseñada puede ofrecer grandes beneficios a una empresa, como por ejemplo:

- Conectividad en una extensa área geográfica.
- Seguridad en la información.
- Reducidos tiempos en el transporte de datos y bajos costos para los usuarios remotos.
- Simplifica la topología de la red. Oportunidad de interconectarse globalmente.
- Reduce la tasa de tráfico

Una VPN típica debe tener una red LAN principal en los edificios de una compañía así como otras LAN's en oficinas remotas. También sirve a usuarios individuales que se conectan desde un lugar remoto. Básicamente, una VPN es una red privada que usa en una red pública (usualmente Internet) para conectarse a sitios remotos, pero en lugar de usar líneas dedicadas, la VPN emplea conexiones virtuales enrutadas a través del Internet desde la LAN principal, hasta el sitios remoto.

Los elementos esenciales de una VPN deben tener ciertas características:

- Escalabilidad en la plataforma.
- Seguridad.

- Confiabilidad.
- Administración.
- Políticas de seguridad.

4.2.2 Clasificación de las VPN's

Como existe una gran variedad de tecnologías y topologías para VPN, la única manera de manejar con éxito esta diversidad, es introduciendo una clasificación de VPN's. Esto se puede realizar de acuerdo a los siguientes criterios:

- *El problema del negocio de VPN's que se trate de solucionar.* La mayoría de los problemas surgen en la comunicación entre una misma compañía (también llamada comunicación intranet), en la comunicación entre compañías y en el acceso para usuarios móviles (mejor conocido como Red VPN Dial-up).
- *La capa del modelo OSI* en la cual el proveedor de servicio intercambia la información de topología con el cliente. La mayoría de las categorías son modelos overlay (extendidos), donde el Proveedor de Servicios atiende al cliente únicamente con un conjunto de enlaces punto a punto (o multipunto) entre los sites. También hay modelos peer-to-peer (vecino-a-vecino o igual-a-igual), donde el Proveedor de Servicios y el cliente intercambian información de enrutamiento de capa 3.
- *La tecnología de capa 2 o de capa 3* se usa para implementar el servicio VPN dentro de la red proveedora. Esta puede ser X.25, Frame Relay, SMDS, ATM o IP.
- *La topología de la red*, existe desde una topología simple con un hub hasta una red con una malla completa o topologías multiniveles jerárquicas en redes más grandes.

Las Redes Privadas Virtuales (VPN's) se clasifican en varias formas. La clasificación tecnológica más amplia es aquella basada en la forma en la que se intercambia información en la VPN.

En el modelo VPN peer-to-peer, la información de enrutamiento del cliente se intercambia entre los enrutadores del cliente y los enrutadores del Proveedor de Servicios. En el modelo VPN overlay, el Proveedor de Servicios proporciona únicamente VC's (líneas lógicas rentadas) y la información de enrutamiento es intercambiada directamente entre los enrutadores de los clientes en la frontera (enrutadores CE).

Los dos modelos pueden combinarse en una red más grande de Proveedor de Servicios: el modelo VPN peer-to-peer puede usar VPN overlay en sus partes de acceso (por ejemplo, enlace de los enrutadores del Proveedor de Servicios a través de ATM).

La clasificación más detallada de las VPN's, se enfoca en la tecnología de capa 3. Se usa para el transporte de paquetes sobre la VPN. El modelo VPN overlay se implementa con tecnologías WAN de conmutación de capa 2 (como X.25, Frame Relay, SMDS o ATM) o con tecnologías de encapsulado de capa 3 (como IP sobre IP,

IPsec). El modelo VPN peer-to-peer por lo general se usa con base en complejos trucos de enrutamiento o con listas de acceso IP.

Las VPN's basadas en MPLS (Multiprotocol Label Switching), supera la mayoría de las fallas de otras tecnologías VPN peer-to-peer. Esto permite que los Proveedores de Servicios combinen los beneficios del modelo peer-to-peer (más sencillo de enrutar) con la seguridad y el aislamiento inherente del modelo VPN overlay.

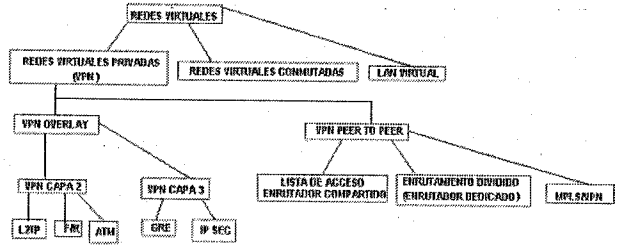


Figura 4.2 Clasificación de las VPN's

Los tres problemas típicos de una empresa que una red privada virtual (Virtual Private Network) trata de resolver son Comunicación interna en la organización (intranet), Comunicación con otras organizaciones y acceso de usuarios móviles, trabajadores, oficinas distantes y otras a través de un medio de conmutación barato. Por lo regular estas tres soluciones con VPN's usualmente explotan la mayoría de las topologías y tecnologías ofrecidas por los Proveedores de Servicios VPN's, pero difieren grandemente en el nivel de seguridad requerido en su implementación. El servicio VPN se usa para implementar la comunicación intranet. También debe ofrecer altos niveles de aislamiento y seguridad. Éstas son las razones principales por las cuales existen muchas organizaciones que usen Internet para comunicarse. Éste no puede ofrecer Calidad de Servicios punto a punto, aislamiento o seguridad, así como una infraestructura adecuada para la comunicación intranet. Las Redes Privadas Virtuales o VPN's fueron implementadas comúnmente con tecnologías tradicionales, como X.25, Frame Relay o ATM. Frecuentemente, las comunicaciones inter-organizacionales aparecen entre los sitios centrales de las organizaciones. Usualmente se usan dispositivos exclusivos de seguridad, tales como firewalls o equipos de cifrado similares como se muestra en la siguiente figura:

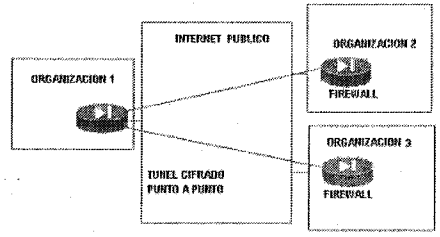


Figura 4.3 Dispositivos de seguridad dentro de las VPN's

Dentro de una red corporativa el acceso del usuario remoto, tiene lugar desde direcciones cambiantes o desconocidas Siempre se filtra con elementos de seguridad, obtenidos a lo largo del enlace punta a punta. Usan tecnologías de cifrado o una contraseña de una sola vez (one-time password). De esta manera, los requerimientos de seguridad para los servicios VPDN son tan rigurosos para las comunicaciones intranet, que la mayoría de los servicios están implementados actualmente sobre IP (Internet Protocol), sobre Internet o usando el backbone privado de un Proveedor de Servicios, tal como se muestra en la siguiente figura:

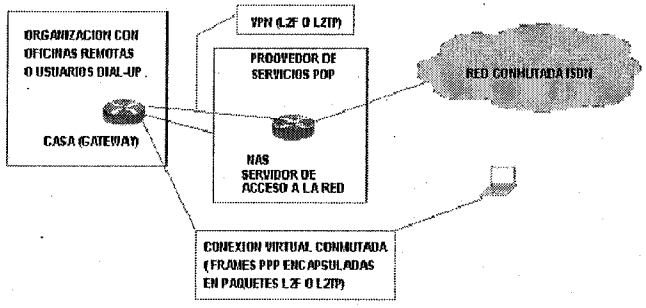


Figura 4.4 Red VPN montada sobre un Backbone privado de un proveedor de servicios

Los protocolos usados para implementar servicios de VPN's sobre IP incluyen L2F (Layer 2 Forward), PPTP (Point-to-Point Tunneling Protocol) o L2TP (Layer 2 Trasnport Protocol)

4.2.3 Modelos VPN Peer-to-Peer y Overlay

Los dos modelos de implementación que han expandido su uso son:

- El modelo *overlay*, en el cual el Proveedor de Servicios proporciona al cliente líneas rentadas.
- El modelo *peer-to-peer*, donde el Proveedor de Servicios y el cliente intercambian información de enrutamiento de capa 3. El proveedor enruta los datos entre los sitios de los clientes en la trayectoria óptima, sin la participación del cliente.

En este caso el modelo al cual le daremos énfasis será el modelo peer to peer debido a que es el modelo que se utilizara para implementar una VPN con MPLS.

4.2.3.1 VPN Overlay

El modelo VPN overlay es el más sencillo de comprender debido a que claramente proporciona la separación de las responsabilidades entre el cliente y el Proveedor de Servicios. El Proveedor de Servicios proporciona al cliente un conjunto de líneas contratadas. Dichas líneas son llamadas Circuitos Virtuales. Pueden estar disponibles permanentemente (PVC's) o establecidos por demanda (SVC's).

La siguiente figura muestra la topología de una VPN overlay y los circuitos virtuales usados en ella:

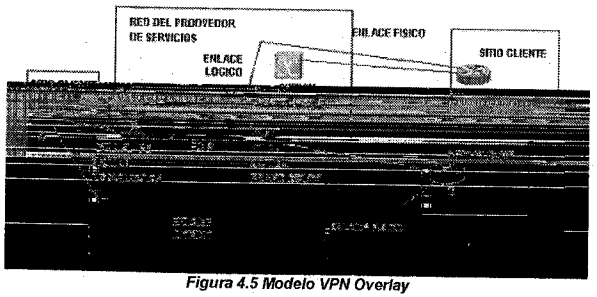


Figura 4.5 Modelo VPN Overlay

El cliente establece la comunicación de enrutador a enrutador entre los equipos CE del cliente. Estos son dispositivos sobre los cuales se instauran los circuitos virtuales por medio del Proveedor de Servicios. Los datos del protocolo de enrutamiento siempre se intercambian entre los dispositivos del cliente y el Proveedor de Servicios no tiene conocimiento de la estructura interna de la red del cliente. La siguiente figura muestra la topología de los enrutadores de la red VPN de la figura anterior:

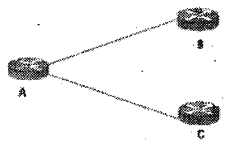


Figura 4.6 Topología de enrutadores de una VPN overlay

La Calidad de Servicio (QoS) garantiza que el modelo VPN overlay sea expresado comúnmente en términos del ancho de banda comprometido en un circuito virtual determinado y un máximo ancho de banda disponible en el circuito virtual. La garantía del ancho de banda consignado se proporciona usualmente a través de la estadística de los servicios de capa 2. Depende de la estrategia de sobreventa del Proveedor de Servicios. Esto significa que la tasa registrada no está realmente garantizada, aunque el proveedor pueda proporcionar una Tasa Mínima de Información o MIR (Minimum Information Rate), que es obtenida a través de la infraestructura de capa 2.
La garantía del ancho de banda es también una garantía del ancho de banda entre dos puntos en la red del cliente. Sin una matriz completa de tráfico para todas las clases de tráfico, es difícil para el cliente maniobrar las garantías en la mayoría de las redes overlay. También es difícil proporcionar las múltiples Clases de Servicio debido a que el Proveedor de Servicios no diferencia el tráfico en medio de la red. Trabajar así, creando múltiples conexiones (por ejemplo, en Frame Relay los PVC's) entre los sitios de los clientes, sólo incrementa el costo general de la red.
Las redes VPN's overlay se usan con un gran número de tecnologías de conmutación de WAN de capa 2. Incluyen a X.25, Frame Relay, ATM o SDMS. En los últimos años, las redes VPNs overlay se usan con túneles de IP sobre IP, todos en backbones privados de IP sobre el Internet público. Los dos métodos más comunes de establecimiento de túneles IP sobre IP son Generic Route Encapsulation (GRE) y el cifrado con IP Security (IPSec).

A pesar de que es relativamente fácil de entender y usar, el modelo VPN *overlay* tiene desventajas:

- Es apropiado para configuraciones no redundantes con poCo'S sitios centrales y sitios bastantes lejanos. Pero llega a ser extremadamente difícil de administrar en una configuración más compleja.

- La implementación propia de las capacidades del circuito virtual requiere un conocimiento detallado de los perfiles de tráfico de sitio a sitio, los cuales no siempre están disponibles.
- Cuando es implementado con tecnologías de capa 2, el modelo VPN *overlay* introduce otra capa innecesaria de complejidad en las redes *New World Service Provider* que, en su mayoría, se basan en IP, lo que incrementa los Co'Stos operacionales de tal red.

4.2.3.2 Modelo VPN Peer-to-Peer

Este modelo fue introducido hace pocos años para superar las desventajas del modelo VPN overlay. En el modelo peer-to-peer, el dispositivo límite o de frontera (PE) del proveedor es un enrutador (PE). Intercambia la información de las rutas con CE. El modelo peer-to-peer proporciona ciertas ventajas sobre el modelo overlay tradicional:

- Desde el punto de vista del cliente el enrutamiento llega a ser extremadamente simple. El equipo CE del cliente intercambia información de las rutas con sólo uno (o unos cuantos) dispositivos PE (mientras que en las redes VPN overlay, el número de enrutadores vecinos pueden crecer a un número grande).
- Entre los sitios del cliente el enrutamiento siempre es óptimo. El equipo PE del proveedor conoce la topología de la red del cliente. También puede establecer un enrutamiento óptimo entre sitios.
- El suministro del ancho de banda es más simple. El cliente tiene que especificar sólo el ancho de banda de entrada y de salida para cada sitio (Tasa de Acceso Comprometido, y Tasa de Entrega Comprometida, CDR) y no los perfiles de tráfico exactos de sitio a sitio.
- La agregación de un nuevo sitio es sencilla. El Proveedor de Servicio acondiciona sólo un sitio adicional y cambia la configuración en el enrutador PE adjunto. En el modelo VPN overlay, el Proveedor de Servicio debe proporcionar todo el conjunto de VC's manejado desde este sitio hacia otros sitios de clientes de la VPN.
- Hay dos opciones disponibles para el modelo de VPN peer-to-peer:
  1) Enrutador compartido, donde varios clientes VPN comparten el mismo enrutador PE.
  2) Enrutador dedicado, donde cada cliente VPN tiene un enrutador PE dedicado.

4.2.3.2.1 Modelo peer-to-peer con enrutador compartido

Cuando se tiene un enrutador compartido, varios clientes pueden conectarse al mismo dispositivo PE. Las listas de acceso se configuran en todas las interfaces PE-CE en los enrutadores PE.
Así aseguran la separación de los clientes de la VPN y previenen que un cliente de la VPN irrumpa en otra red VPN. Esto también evita que un cliente de una VPN no pueda atacar otra red VPN. La siguiente figura ilustra un ejemplo de la configuración de enrutador compartido.

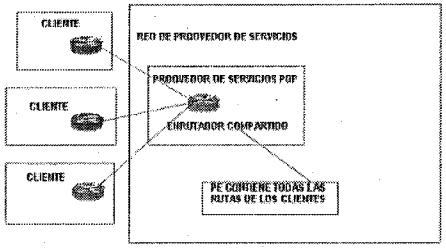


Figura 4.7 Ejemplo de configuración de enrutador compartido

4.2.3.2.2 Modelo peer to peer con enrutador dedicado

En el modelo *peer to peer* con enrutador dedicado, cada cliente VPN tiene su propio enrutador PE. Sin embargo, éste sólo tiene acceso a los equipos de la tabla de enrutamiento de PE.

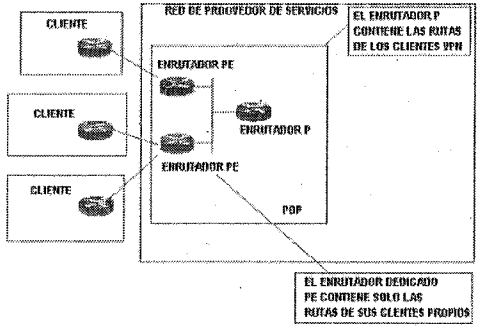


Figura 4.8 Modelo peer to peer con enrutador dedicado

En el modelo de enrutador dedicado aún se utiliza un protocolo para crear la tabla de rutas de la VPN en los PE. Las tablas de rutas en el PE contienen sólo los equipos anunciados por los clientes VPN conectados a él. El resultado es un aislamiento casi perfecto entre los clientes de la VPN (tiene que estar basado en una tabla de enrutamiento). Dentro de esta modalidad, el enrutador dedicado puede ser implementado como sigue:

- Cada protocolo de enrutamiento es ejecutado entre el enrutador PE y el enrutador CE.
- BGP es ejecutado entre el enrutador PE y el enrutador P.
- El enrutador-PE redistribuye rutas recibidas desde el enrutador-CE encapsuladas en BGP, marcadas con una identificación del cliente (ID, comunidad BGP) y propaga las rutas a los enrutadores-P. De esta manera, el enrutador P contiene todas las rutas de todos los clientes VPN.
- Los enrutadores P sólo propagan rutas en comunidades BGP apropiadas por los enrutadores PE. Así, los equipos PE sólo reciben las rutas que se originaron desde los CE dentro de la VPN.

4.2.3.2.3 Comparación de modelos peer to peer

El modelo *peer to peer* con enrutador compartido es muy difícil de mantener. Requiere el empleo de largas y complejas listas de acceso en casi cada interfaz del enrutador. El modelo de enrutador dedicado (más sencillo de configurar y de mantener), llega a ser muy caro para el Proveedor de Servicios cuando trata de servir a un gran número de clientes con sitios geográficamente dispersos.

Ambos modelos comparten varias desventajas que evitan la expansión de su uso:

- Todos los clientes comparten el mismo espacio de direcciones IP. Evita que se usen direcciones IP privadas. Para ser localizados por el Proveedor de Servicios los clientes deben usar direcciones IP diferentes ya sean públicas o privadas para ser localizados por el Proveedor de Servicios.
- Los clientes no pueden insertar la ruta de defalut en su VPN. Esta limitación evita que tengan acceso a Internet por medio de otro Proveedor de Servicios.
- Además de estas dos desventajas, el modelo de enrutador compartido sufre de complejidad cuando varios clientes usan protocolos de enrutamiento (RIP, RIPv2, BGP y IS-IS) en donde existen varias instancias. Algunos no son soportados por el software del enrutador.

4.3 Conceptos Generales de MPLS

4.3.1 Descripción funcional del MPLS

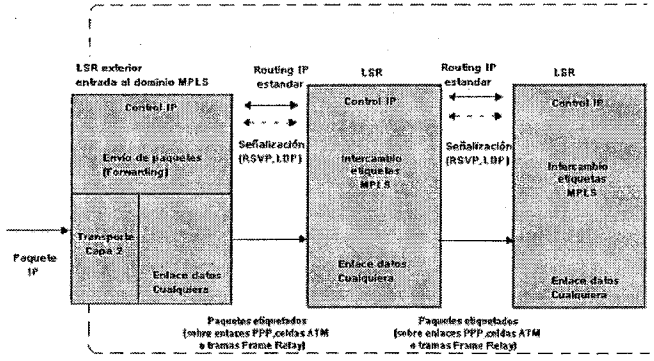
La operación del MPLS se basa en las componentes funcionales de envío y control, y que actúan ligadas íntimamente entre sí. Enseguida se explican cada una de dichas funciones

4.3.1.1 Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Los LSP son simples por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSP, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un conmutador de etiquetas (Label Swiching Router) a otro, a través del dominio MPLS. Un LSR no es sino un enrutador especializado en el envío de paquetes etiquetados por MPLS. Al igual que en las soluciones de señalización multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding).

Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSP's. Sin embargo, en MPLS o bien se utiliza el protocolo RSVP o bien el Label Distribution Protocol (LDP), del que se tratará más adelante. Pero, de acuerdo con los requisitos del IETF, la tecnología de capa 2 puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS.

El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.



BACKBONE (DOMINIO) MPLS

Figura 4.9 Señalización de MPLS

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, es LSR interiores del dominio MPLS. Un LSR es como un enrutador que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control. Cada entrada de la tabla contiene un par de etiquetas entrada / salida correspondientes a cada interfaz. En la figura 4.2 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

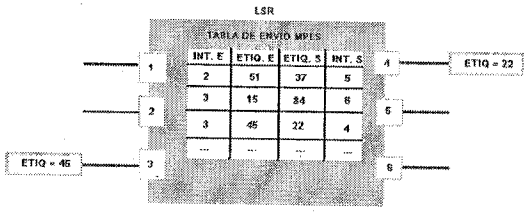


Figura 4.10 Funcionamiento de un LSR DEL Núcleo MPLS

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. El LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de enrutamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas), la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas, y finalmente lo envía por la interface de salida correspondiente. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto es el que lo saca de la red MPLS; paso siguiente, al consultar la tabla de conmutación de etiquetas le quita ésta y es entonces cuando envía el paquete por ruteo convencional, usando para ello la tabla de enrutamiento. Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de capa 2 de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay),

se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de capa 2 empleada no soporta un campo para etiquetas (por ejemplo, enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (capa 3).

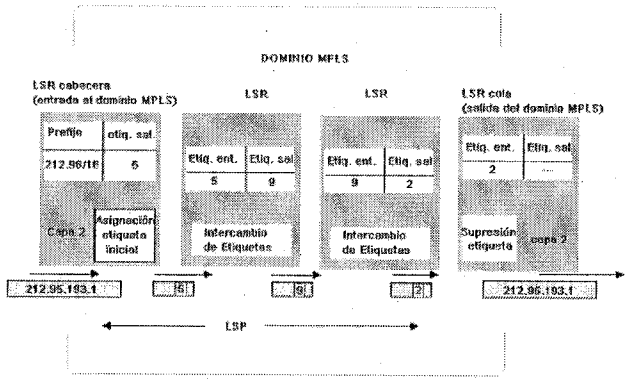


Figura 4.11 Dominio MPLS

En la figura se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado Co'S), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de capa 2, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

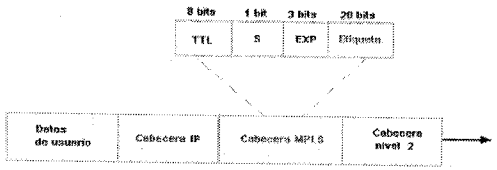


Figura 4.12 Campos de cabecera genérica de MPLS

4.3.1.2 Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSP's mediante el procedimiento de intercambio de etiquetas según las tablas de los LSR's. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSP's
- Cómo se distribuye la información sobre las etiquetas a los LSR's

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de enrutamiento. MPLS necesita esta información de ruteo para establecer los caminos virtuales LSP's. Lo más lógico es utilizar la propia información de enrutamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de enrutamiento (recuérdese que los LSR son enrutadores con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada / salida en cada tabla de los LSR's.

El segundo aspecto se refiere a la información de señalización. Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, siendo el caso del Label Distribution Protocol (LDP).

4.4 Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, es en el esquema global de funcionamiento, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de enrutadores IP.

El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de enrutadores a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología de tipo malla completa (directamente o por PVC's ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSP's (puede haber más de uno para cada par de enrutadores). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

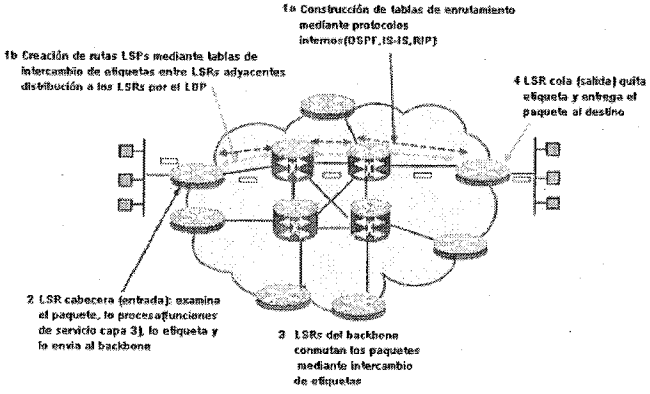


Figura 4. 13 Elementos que conforman la red MPLS

4.4.1 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico
- Diferenciación de niveles de servicio mediante clases (Co'S)
- Servicio de redes privadas virtuales (VPN)

Para nuestro caso particular, trataremos más a detalle el tercer punto, el cual se refiere al Servicio de Redes Virtuales (VPN).

4.4.1.1 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén sobre utilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 4.6 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino. El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los enrutadores correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer enrutamiento restringido (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

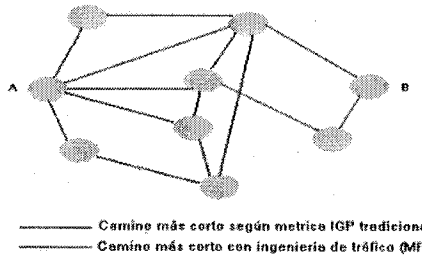


Figura 4.14 Camino más corto con ingeniería MPLS

1.0.0.0 Clases de servicio (Co'S)

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la Calidad de Servicio (Co'S) requerida en las mismas se basó únicamente en la integridad de los datos. En este sentido IP fue concebido, de forma óptima y segura, para tráfico sin requerimientos de tiempo real. Para esto el servicio que brinda IP es del tipo *Best-Effort* el cual se refiere a que el tráfico IP será manejado "tan bien como se pueda", sin ninguna responsabilidad por parte de la red.

Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma integra, sino que además requiere ser transferido en el tiempo adecuado, al ritmo adecuado, en correspondencia con la cadencia que es generado. En consecuencia, la Co'S en relación con el tráfico que tiene requerimientos de tiempo real necesita considerar otros parámetros de calidad, tales como la latencia (retardo), variación en el retardo (*jitter*) y el ancho de banda. Dados estos requerimientos de Co'S impuestos por el tráfico con características de tiempo real, como es audio y el vídeo, se necesitan mecanismos de señalización que propicien tener bajo control dichos parámetros de calidad, y dar garantía de Co'S.

1.0.0.0.0 Mecanismos de señalización para QoS

Hasta ahora existen dos mecanismos de señalización para Co'S: *Integrated Services y Differentiated Services*. A continuación se muestra lo esencial de cada uno.

1.1.1.1.1 Integrated Services (Int-Serv)

Basado en el protocolo RSVP (Resource Reservation Protocol), implica una reserva de recursos en la red para cada flujo de información de usuario, así como el mantenimiento en la red (en los enrutadores) de un estado para cada flujo. Esto conduce a un considerable tráfico de señalización y ocupación de recursos en cada

enrutador para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte realiza esta señalización a la congestión de la red. No es una solución escalable, ni es una solución adecuada para grandes entornos como Internet, pero si lo es para entornos más limitados y también para redes de acceso al backbone.

RSVP es un protocolo señalización de QoS, y posibilita:

- dar a las aplicaciones un modo uniforme para solicitar determinado nivel de Qo'S,
- encontrar una forma de garantizar cierto nivel de Qo'S, y
- proveer autentificación.

RSVP es un protocolo que se desarrolla entre los usuarios y la red, y entre los diferentes nodos (enrutadores) de la red que soportan este protocolo Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como mantener estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y la posterior cancelación, implican el intercambio de mensajes de señalización, lo que representa un tráfico considerable cuando de entornos como Internet se trata. RSVP ofrece dos tipos de servicios, a saber: Servicio de carga controlada y servicio garantizado.

- Servicio de carga controlada: aunque no está muy bien definido, se entiende en general que la pérdida de paquetes debe ser muy baja o nula.
- Servicio garantizado: se basa en solicitar determinado ancho de banda y cierta demora de tránsito máxima.

De los dos tipos de servicios que RSVP soporta, el más adecuado para aplicaciones con requerimientos de tiempo real es el servicio garantizado, aunque es más complejo de implementar que el servicio de carga controlada. RSVP define dos sentidos para la transferencia de sus mensajes de señalización, downstream y upstream. El flujo downstream se efectúa desde la fuente al receptor o receptores, y el flujo upstream en sentido contrario. PATH y RESV son dos mensajes básicos del protocolo RSVP, y son en definitiva los mensajes a través de los cuales se lleva a cabo la reserva de recursos en la red previa a la comunicación. Los mensajes PAHT's son generados por la fuente de mensajes de usuario necesitados de garantía de Co'S, e indica las características de éstos en cuanto a recursos que necesita. La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario, para lo cual se requiere previamente un «diálogo» entre el proceso RSVP y el proceso de ruteo, pues dicha ruta quien la determina es el protocolo de ruteo. Cada enrutador RSVP almacena la dirección del enrutador anterior. Así, con los mensajes PATH's se posibilita indicar al receptor, o receptores, no solo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los enrutadores que no soporten RSVP transfieren transparentemente los mensajes PATH's. Los mensajes RESV's son producidos por el receptor (o receptores) de los flujos de información de usuario, como «respuesta» a los mensajes PATH's, y solicitan a la red (a los enrutadores RSVP) las correspondientes reservas de recursos para soportar la

comunicación con cierta QoS, fluyendo hasta la fuente del stream de datos de usuario, es decir, en sentido upstream. Con la información de ruta que suministran previamente los mensajes PATH's, los mensajes RESV's dirigen las solicitudes de reservas a los enrutadores RSVP apropiados, esto es, por donde fluirán los streams de datos. Los mensajes RESV's especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un stream de datos específico. Vale decir además, que es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios streams de datos de usuario. Vale decir también que la reserva de recursos extremo a extremo que posibilita RSVP será válida si, y solo si, la congestión y demora que introduzcan los enrutadores no RSVP no son significativas.
Otros mensajes del protocolo RSVP son:

- PATHTEAR: son mensajes generados por la fuente de datos de usuario para eliminar los estados PATH's en todos los enrutadores RSVP. Siguen la misma ruta que los mensajes PATH's. También pueden ser originados por cualquier nodo cuando se agota el timeout del estado path.
- RESVTEAR: son generados por los receptores para borrar los estados de reserva en los enrutadores RSVP, por tanto viajan en el sentido upstream. Pueden ser también originados por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.
- PATHERR: viajan en sentido upstream hacia el emisor siguiendo la misma ruta que los mensajes PATH's, y notifican errores en el procesamiento de mensajes PATH's, pero no modifican el estado del nodo por donde ellos pasan en su viaje hacia la aplicación emisora.
- RESVERR: notifican errores en el procesamiento de mensajes RESV, o notifican la interrupción de una reserva. Se transfieren en la dirección *downstream* hacia el receptor o receptores apropiados.

En la siguiente figura, se muestra de forma muy simplificada el intercambio de mensajes RSVP, específicamente mensajes PATH's y RESV's entre un emisor y dos receptores (A y B), indicándose que la reserva representada por el mensaje RESV 2 prevalece sobre la reserva representada por el mensaje RESV1, de manera que esto sugiere que la reserva solicitada por el receptor A es mayor que la solicitada por el receptor B. Esto es, la reserva «mayor» prevalece sobre la reserva «menor», así el enrutador B sólo solicita al enrutador A la mayor de las dos solicitudes de reservas a él llegadas desde el enrutador C (originada por el receptor A) y desde el receptor B. Esto es una característica de RSVP.

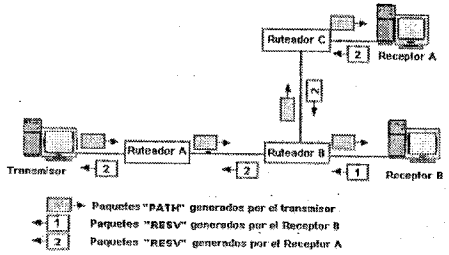


Figura 4.15 Protocolo RSVP resumido: intercambio básico de mensajes

Estas solicitudes de reserva conducen a que en cada enrutador RSVP se establezca un estado soft (Soft-State), es decir, una reserva en cada enrutador es un estado Soft con un determinado timeout, que debe ser refrescada periódicamente por los receptores, de lo contrario vence el timeout y se deshace la correspondiente reserva, con la consecuente generación de un mensaje RESVTEAR.

La liberación de recursos reservados mediante RSVP se puede materializar de diferentes maneras, así la solicitud para dar baja a determinada reserva puede ser originada:

- por el emisor,
- por el receptor,
- por un nodo de la red.

Por parte del emisor o de un receptor acontece cuando así lo decide la aplicación correspondiente, en cuyo caso esto se produce mediante la generación de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente. Por parte de un nodo se lleva a cabo cuando vence el timeout correspondiente del estado path o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

2.0.0.0.0 Differentiated Services (Diff-Serv)

Se basa en marcar los paquetes IP, y la red (los enrutadores) los tratarán en base a esa marca, esto es, se desarrolla un tratamiento diferenciado de los paquetes IP en los enrutadores. Define y utiliza diferentes tipos de enrutadores. Esta diferenciación no es la misma en los diferentes nodos, sino depende de si se trata de un nodo interior o un nodo frontera. En consecuencia, y a diferencia de la solución Servicios Integrados (basada en RSVP), la red con nodos Diff-Serv no establece ni mantiene estados de las conexiones por flujos de paquetes. Es una solución escalable, más apropiada para

grandes entornos como Internet. Puede ser fácilmente implementada en las redes IP existentes.
La versión seis de IP contempla este marcado de paquetes, mediante el campo DS (Differentiated Service), byte DS de la cabecera IP. El byte de Clase se puede utilizar como byte de servicios diferenciados, o byte de distinción, teniendo el mismo significado que en IPv4. También IPv4 permite dicho marcado de paquetes, a través del byte ToS (Type of Service), y en tal caso se utiliza éste como byte DS.

Se han definido dos tipos de Diff-Serv con garantía de Co'S:

Assured Forwarding Service (AFS): los paquetes se etiquetan con alta prioridad, aunque no se garantiza un ancho de banda. Se posibilita una Co'S superior al servicio tradicional best-effort de Internet. Brinda cuatro clases de servicios, cada una con tres niveles diferentes de dropping. Un nodo DS es, en principio, una combinación de cinco módulos funcionales, aunque no todo enrutador DS tiene que contener la totalidad de éstos:

- Clasificador de tráfico: clasifica los paquetes en base a uno o varios campos de su cabecera.
- Medidor de tráfico (Traffic Meter): mide las propiedades temporales de los paquetes.
- Marcador de paquetes (Packet Markers): establece un codepoint en el campo DS del paquete
- Conformador (Shapers): establece cierta demora para uno o más paquetes de un stream.
- Droppers: descarta algunos o todos los paquetes de un stream de tráfico.

Expedited Forwarding Service (EFS): equivale a una línea arrendada virtual, por lo que se garantiza cierto ancho de banda y reducida demora de cola. Emula un circuito.

Los tipos de routers en redes Diff-Serv se clasifican así:

- First Hop Router: es el router más próximo al host emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde a la etiqueta SLA (Service Level Agreement). Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.
- Ingrees Router: se sitúan en los puntos de entrada al backbone Diff-Serv. (Dominio DS), efectuando la clasificación de los paquetes en base al campo DS o en base a múltiples campos de la cabecera de éstos.
- Egress Router: se ubican en los puntos de salida de redes Diff-Serv. (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.
- Interior router: tienen la misión de sumar flujos, realizar la clasificación DS y reenvío de paquetes. Se sitúan dentro del backbone DS (dominio DS).

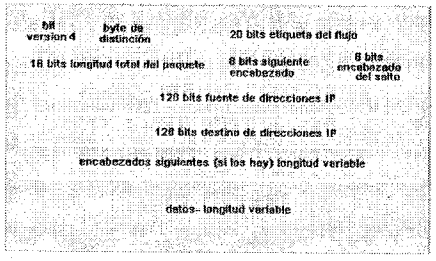


Figura 4.16 Formato del paquete IP v6

En la versión 4 de IP se emplea, como ya se dijo antes, el campo ToS (Type of Service) en la cabecera, que posibilita marcar cada paquete en base a cuatro tipos de servicios, a saber:

- mínimo Costo económico.
- máxima fiabilidad.
- máximo throughput.
- mínimo retardo.

Sin embargo, este byte prácticamente no ha sido utilizado, pues los enrutadores no procesaban esta información, además, con igual resultado se empleaban los bits de prioridad. No obstante, es una posibilidad de obtener diferentes grados de QoS en IPv4, y puede emplearse como byte DS en redes Diff-Serv. Tanto Int-Serv como Diff-Serv están en fase de experimentación, y ambas soluciones están basadas en modelos opuestos, en Diff-Serv la Co'S es controlada por el emisor y en Int-Serv la Co'S se controla por el receptor. Ahora bien, dadas las mejores características en cuanto a escalabilidad y grado de generación de tráfico de señalización que presenta la solución Diff-Serv, ésta se vislumbra como la mejor oferta para cubrir el sector backbone. Y de cara a las redes de acceso al backbone, parece ser lo más adecuado la solución Int-Serv. No obstante, todavía no se puede afirmar lo anterior categóricamente.

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, o el correo electrónico (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación, como son las de vídeo y voz interactivo. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio Co'S en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP
- entre cada par de LSR exteriores se pueden aprovisionar múltiples LSP's, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios.

4.5 Operación de una VPN basada en MPLS

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPN's es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que la información de los nodos de un usuario no es visible para el resto de los usuarios, dando la sensación de que posee una red con enlaces dedicados. Las IP VPN's son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales. Las VPN's tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCV's entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR).
Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSP's, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPN's, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos. El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPN's sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. A pesar de las ventajas de los túneles IP sobre los PVC's, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

- están basadas en conexiones punto a punto (PVC's o túneles)
- la configuración es manual

- la provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones
- plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales

La gestión de Co'S es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte Realmente, el problema que plantean estas IP VPN's es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremo a extremo (o circuitos virtuales) entre cada par de enrutadores de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPN's se implementan mediante los caminos LSP's creados por el mecanismo de intercambio de etiquetas MPLS. Los LSP's son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer Co'S y optimizar los recursos de la red con técnicas de ingeniería de tráfico. En la figura se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSP's) está en que éstos se crean dentro de la red, a base de LSP's, y no de extremo a extremo a través de la red.

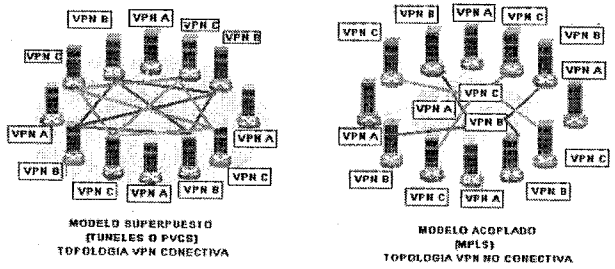


Figura 4.17 Diferencias entre una VPN basada en túneles a una basada en MPLS

Como resumen, las ventajas que MPLS ofrece para IP VPN's son:

- Proporcionan un modelo "acoplado" o "Inteligente", ya que la red MPLS "sabe" de la existencia de VPN's (lo que no ocurre con túneles ni PVC's)
- Evita la complejidad de los túneles y PVC's
- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router
- Tiene mayores opciones de crecimiento modular
- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino). Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet.

Capítulo 5

MULTICAST A NIVEL WAN

Capítulo 5 Multicast a nivel WAN

5.1 Conceptos Básicos de nivel WAN

5.1.1 Árboles de Camino corto (SPT)

Los enrutadores de Multicast crean árboles de distribución que controlan el camino que el Multicast IP toma a través de la red para entregar tráfico a todos los receptores. Los dos tipos básicos de árboles de distribución de Multicast son los árboles de camino corto y los árboles compartidos. La forma más simple de un árbol de distribución de Multicast es un árbol fuente de camino corto con su raíz en la misma fuente y ramas que forman un árbol a través de la red a los receptores. Debido a que este árbol usa el camino más corto a través de la red, también es llamado como árbol del camino más corto SPT (shortest path tree)

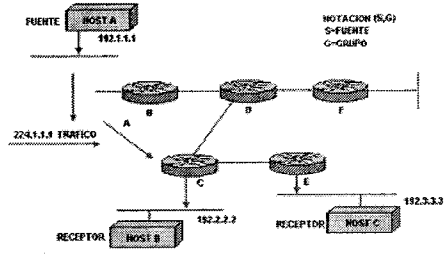


Figura 5.1 Host de un árbol de camino corto

El diagrama muestra un ejemplo de un SPT para el grupo 224.1.1.1 adaptado en la fuente (Host A) conectado con dos receptores B y C. La notación especial de (S, G), es decir fuente y grupo, enumera un SPT donde S son las direcciones IP de la fuente y G es la dirección de grupo Multicast. Usando esta notación, el SPT para el ejemplo en la figura sería (192.1.1.1, 224.1.1.1).
En el (S, G) la notación implica que existe un SPT para cada fuente individual que envía a cada grupo. Por ejemplo, si el receptor B también está enviando tráfico deberá agruparse en 224.1.1.1 El host A y C son receptores, entonces un SPT (S, G) existiría con una notación de (192.2.2.2, 224.1.1.1).

5.1.2 Árboles compartidos

Son árboles que tienen ubicada su raíz en un punto diferente a donde se encuentra la fuente, los árboles compartidos usan una sola raíz común puesta en algún punto

escogido en la red. El punto donde se encuentra la raíz se llama Punto de encuentro (RP)

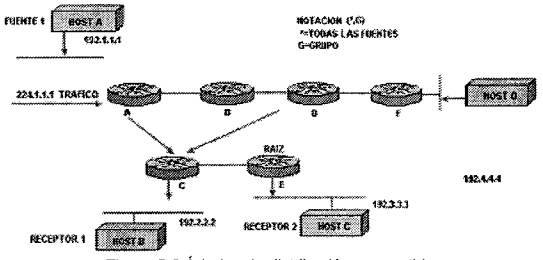


Figura 5.2 Árboles de distribución compartida

La figura muestra un árbol compartido para el grupo 224.2.2.2 con la raíz localizada en el enrutador D. Al usar un árbol compartido, las fuentes deben enviar su tráfico a la raíz y entonces el tráfico se remite bajo el árbol compartido para localizar a todos los receptores.
En este ejemplo, las fuentes Multicast envían tráfico (las fuentes son los Host A y D) y viaja hacia la raíz (enrutador D) y entonces baja el árbol compartido a los dos receptores B y C. Todas las fuentes Multicast se agrupan en un árbol compartido común, su notación es (*, G), lo que representa el árbol. En este caso, * son todas las fuentes, y G representa el grupo del Multicast. Por consiguiente, el árbol compartido mostrado en la figura se expresaría como (*, 224.2.2.2). Los Árboles del Camino más corto tienen la ventaja de crear el camino óptimo entre la fuente y los receptores. Esto garantizará el mínimo tiempo de retardo de la red por enviar tráfico a través de las fuentes Multicast. Esta optimización viene con un precio. Los enrutadores deben mantener información del camino para cada fuente. En una red que tiene miles de fuentes y miles de grupos esto es un problema recurso, que puede verse rápidamente en los enrutadores.

5.1.3 Protocolos de enrutamiento para Multicast

Para poder informar a otros enrutadores sobre fuentes y destinos de paquetes Multicast, se deben emplear protocolos de enrutamiento. Existen tres categorías básicas:

- Protocolos de Modo Denso (DVMRP y PIM-DM)
- Protocolos de Modo Sparse (PIM-SM y CBT)
- Protocolos de Estado de Enlace (MOSPF)

Los protocolos del tipo "Denso" (DM dense mode) utilizan el árbol más corto junto con un mecanismo de empuje. Este mecanismo de empuje asume que en cada interfaz del enrutador existe al menos un receptor del grupo Multicast. El tráfico es enviado (flood) a través de todas las interfaces. Para evitar el desperdicio de recursos, si un enrutador no desea recibir tráfico envía un mensaje de supresión (prune). Como resultado se tiene que el tráfico de paquetes Multicast es enviado únicamente a los enrutadores que tienen interés de la información de Multicast. Este comportamiento de "Flood" y "Prune" se repite aproximadamente cada 2 o 3 minutos dependiendo del protocolo, por esta razón protocolos del tipo denso son mayormente empleados en ambientes LAN y donde el número de receptores usualmente es alto comparado con el de las fuentes y donde el ancho de banda no es un factor restrictivo. Protocolos basados en modo denso son el Distance Vector Routing Protocol (DVMRP) y el Protocol Independent Multicast Dense Mode (PIM-DM).
Los protocolos del tipo "Sparse" (SM) hacen uso del modelo de árboles compartidos y ocasionalmente como el PIM Sparse Mode (PIM-SM) hace uso del "Short Path Tree"(SPT) para la distribución de tráfico Multicast. Al contrario de los DM, los SM hacen uso de un mecanismo de detección. Este mecanismo asume que no existen receptores interesados en el tráfico de Multicast, de esta forma ningún tráfico es enviado a menos que exista una solicitud explícita. Para que el árbol compartido sea construido, el enrutador receptor debe enviar a la raíz una solicitud de unión al árbol (Join message). Este mensaje viaja de enrutador a enrutador construyendo a su paso el camino hacia la raíz. Cuando un receptor desea dejar de recibir tráfico, debe enviar un mensaje de supresión (Prune) al igual que lo hacen los DM. Por su mecanismo detección, los protocolos SM son utilizados en ambientes WAN donde el ancho de banda es escaso o cuando se tienen más fuentes que destinos. El punto más crítico de estos protocolos es el "Rendezvous Point" (RP) ya que si este no está bien ubicado por el administrador de la red puede ocasionar que el camino fuente-destino no sea el óptimo o que por exceso de tráfico el RP se convierta en un cuello de botella. PIM-SM cuenta con un mecanismo que permite conmutar de árbol compartido a SPT para una fuente en particular.
Los protocolos de estado de enlace como Multicast Open Short Path First (MOSPF) hacen uso del "Short Path First" (SPF). Para construir estos árboles, los enrutadores envían información de estados de enlace que identifica la ubicación en la red de los grupos de miembros de Multicast. Con esta información los enrutadores forman un SPT de cada fuente hacia todos los receptores en el grupo.
A continuación se muestran algunas características de los protocolos de enrutamiento para Multicast.

- *Distance Vector Multicast Routing Protocol (DVMRP):* Primer protocolo de enrutamiento desarrollado para Multicast y que tuvo un uso masivo DVMRP.Vector distancia basado en RIP, tiene todas las desventajas de los DV. Updates Periódicos (cada 60 segundos) , 32 brincos máximo , es de clase Dense Mode y no es escalable .
- *Multicast Open Shor Path First (MOSPF):* Basado en OSPF, Debe construir árboles de expansión para construir árboles, Utiliza mucho CPU de enrutadores si la topología cambia constantemente, su escalabilidad es cuestionable, no ha sido ampliamente usado y además es complejo.

- *Protocol Independent Multicast Dense Mode (PIM DM):* Es de tipo Dense, hace un "flood" cada 3 minutos, no se recomienda para ambientes WAN, aunque es sencillo de configurar
- *Protocol Independent Multicast Sparce Mode (PIM SM):* Es del tipo Sparse, no genera tráfico a menos que se solicite, se recomienda para ambientes WAN y LAN, además es Independiente de protocolo de enrutamiento de Unicast.
- Multicast Border Gateway Protocol (MBGP): Permite usar los mismos comandos de que BGP, lo cual reduce sensiblemente el tiempo de trabajo, ademas permite que el tráfico de Multicast y Unicast puedan usar caminos (paths) diferentes. Algunas de sus desventajas es que las topologías no son congruentes, si las topologías son no congruentes, los caminos de Multicast y Unicast pueden tener políticas diferentes.

5.1.4 Arquitectura de IP Multicast Inter-dominio

Para la arquitectura de IP Multicast dentro del mismo dominio, se sugiere el uso de PIM Sparse Mode. Con PIM SM se eliminará el innecesario tráfico de Multicast por los enlaces WAN. Se recomienda además que los RP sean descubiertos de forma automáticos por los enrutadores de tal forma que el proceso sea más eficiente y a prueba de fallas. El protocolo que se recomienda es el PIMv2. Aunque este protocolo es un poco más complejo que el Auto-RP asegura la interoperabilidad con enrutadores de otras marcas. Esto además de evitar la configuración estática de los RP's, asegura una redundancia en caso de falla de los RP's. Finalmente se recomienda que las interfaces se configuren como de tipo sparse-dense, de tal forma que si todos los RP fallan, la red tenga oportunidad de conmutar a modo denso evitando que se pierda tráfico.

5.2 Protocolo de enrutamiento para Multicast (PIM)

Este protocolo de enrutamiento utiliza el modelo tradicional de Multicast IP de pertenencia iniciada por el receptor, admite tanto árboles compartidos como árboles de ruta de acceso más corta, no depende de ningún protocolo de enrutamiento de Unicast específico y utiliza El protocolo independiente de Multicast en modo esparcido (PIM-SM, *Protocol Independent Multicast-Sparse Mode*) envía paquetes de Multicast a grupos de Multicast y está diseñada para establecer de forma eficaz árboles de distribución a través de redes de área extensa (WAN). PIM-SM es "independiente de protocolo" porque puede utilizar la información de rutas que cualquier protocolo de enrutamiento introduzca en la Base de información de enrutamiento (RIB) de Multicast. Como ejemplos de estos protocolos de enrutamiento podemos encontrar protocolos como el Protocolo de información de enrutamiento (RIP, *Routing Information Protocol*) y el protocolo OSPF (*Open Shortest Path First*). No obstante, también se pueden utilizar protocolos de Multicast que llenan las tablas de enrutamiento, como el Protocolo de enrutamiento de Multicast de vectores de distancia (DVMRP, *Distance Vector Multicast Routing Protocol*). *Modo esparcido* significa que el protocolo está diseñado para situaciones donde los grupos de Multicast están dispersos en una región extensa.

Por el contrario, los protocolos de modo denso, como DVMRP y OSPF de Multicast (MOSPF, *Multicast OSPF*) están diseñados para situaciones en las que los grupos de Multicast cuentan con un número grande que los represente y hay suficiente ancho de banda. Con estos esquemas, es posible que la información acerca de la pertenencia de los paquetes de datos se envíe de forma innecesaria a interfaces que no conducen a fuentes de Multicast o a receptores interesados. Además, los enrutadores almacenan el estado relacionado con estos nodos no interesados, lo que resulta igualmente innecesario. Se acepta este exceso cuando la mayor parte de los host están interesados en los datos y hay suficiente ancho de banda para permitir el flujo de los mensajes de control. De cualquier otro modo resulta ineficaz. PIM-SM supone que ningún host desea datos si no los solicita explícitamente. Sin embargo, PIM tiene un protocolo equivalente para modo denso (PIM-DM) que puede interoperar con el modo esparcido.
PIM-SM ha sido diseñada para alcanzar los siguientes objetivos:

- Conservar el modelo de servicio tradicional de Multicast IP de pertenencia al grupo de Multicast iniciada por el receptor. Los receptores emiten señales a los enrutadores para unirse al grupo de Multicast que recibirá los datos.
- No alterar el modelo de host. PIM-SM es un protocolo de enrutador a enrutador, lo que significa que los hosts no tienen por qué actualizarse, pero deben distribuirse en la red enrutadores compatibles con PIM-SM.
- Permitir tanto árboles compartidos como de distribución de origen. Con los árboles compartidos, PIM-SM utiliza un enrutador central, denominado punto de reunión (RP, *Rendezvous Point*), como raíz del árbol compartido. Todos los hosts de origen envían el tráfico de Multicast al punto de reunión que, a su vez, reenvía los paquetes a través de un árbol común a todos los miembros del grupo. Los árboles de origen conectan directamente los orígenes con los receptores. Hay un árbol independiente para cada origen. Desde la perspectiva de las tablas de enrutamiento de Unicast, los árboles de origen se consideran árboles de ruta de acceso más corta. PIM-SM puede utilizar cualquier tipo de árbol o ambos simultáneamente.
- Utilizar mecanismos de estado flexible para adaptarse a las condiciones de red y a las dinámicas de grupos de Multicast cambiantes. Estado flexible significa que, a menos que se actualice, la configuración del estado del enrutador es a corto plazo y que caduca después de un cierto tiempo.

5.2.1 Protocolo PIM-SM

El protocolo PIM-SM puede dividirse en las siguientes partes:

- Mensajes de saludo
- Reenvío de paquetes de Multicast
- Unión al árbol compartido
- Registro con el punto de reunión
- Cambio del árbol de ruta de acceso más corta (SPT)
- Eliminación de interfaces
- Mensajes de aserción
- Determinación del punto de reunión.

Se analizará cada parte de forma sucesiva en un sistema estable, lo que significa que en él ya se ha seleccionado el punto de reunión (RP). La última sección mostrará cómo ocurre esto.

En primer lugar, se estudiará lo siguiente:

- Orientación y reenvío de ruta inversa (RPF)
- Árboles de ruta de acceso más corta
- Árboles compartidos

La comprensión de estos términos permitirá entender más fácilmente el protocolo PIM-SM.

5.2.1.1 Orientación y reenvío de ruta inversa

La orientación representa un esquema sencillo de enrutamiento que no depende de ningún tipo de información de enrutamiento. En este esquema, se transmite un paquete a todas las interfaces excepto a la interfaz remitente. Para limitar el número de veces que el paquete se reproduce, se utiliza una métrica, por ejemplo una cuenta de saltos. Cuando la métrica alcanza un umbral, el paquete se elimina. El problema que surge con este esquema es que se crea un número exponencial de copias de cada paquete. La orientación, por un lado, garantiza el envío a cada nodo de una copia de cada paquete, considerando que los paquetes no se pierden y, por otro lado, puede generar tanta congestión que es muy probable que los paquetes se pierdan. Reenvío de ruta inversa (RPF, *Reverse Path Forwarding*) es un concepto que representa una forma optimizada de orientación, en la que el enrutador acepta un paquete de un origen S a través de una interfaz I, sólo si I es la interfaz que el enrutador utilizaría para llegar a S. Determina si la interfaz es correcta mediante la consulta en las tablas de enrutamiento de Unicast. Esta técnica disminuye en gran medida la sobrecarga de trabajo relacionado con la orientación estándar. Considerando que un enrutador acepta un paquete desde un único vecino, orienta el paquete sólo una vez, lo que significa (si suponemos vínculos de punto a punto) que cada paquete se transmite por un vínculo una sola vez en cada dirección.

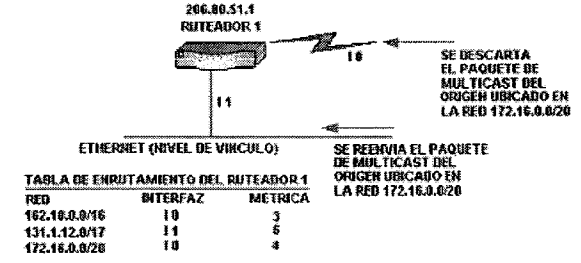


Figura 5.3 Ejemplo de reenvío de ruta inversa (RPF) Reverse Path Forwarding

En este ejemplo, el enrutador descarta el paquete procedente de un origen en la red 172.16.0.0/20 a través de la interfaz I0.
El paquete se descarta porque la tabla de enrutamiento no considera la interfaz como la ruta de acceso más corta a la red 172.16.0.0/20. Si el enrutador tuviera un paquete para reenviarlo a esa red, utilizaría I1. El paquete que llega a través de la interfaz I1 se reenvía porque la tabla de enrutamiento considera esta interfaz como la ruta de acceso más corta a la red. Observe que la tabla de enrutamiento de Unicast del enrutador determina la ruta de acceso más corta para los paquetes de Multicast.

5.2.2 Árboles de ruta de acceso más corta

Los árboles de ruta de acceso más corta (shortest paht tree) también se conocen como árboles basados en el origen, lo que significa que las rutas de reenvío se basan en la ruta de Unicast al origen más corto. Esto es lo que se quiere dar a entender cuando se dice que los árboles de origen se consideran los árboles de ruta de acceso más corta desde la perspectiva de las tablas de enrutamiento de Unicast. Si la métrica de enrutamiento se basa en cuentas de saltos, las ramas de los árboles de ruta de acceso más corta de Multicast representan los saltos mínimos. Si la métrica simboliza retraso, las ramas representan el retraso mínimo. Para cada origen de Multicast, hay un árbol de Multicast correspondiente que conecta directamente el origen con todos los receptores. Una vez construido el árbol para el origen y para el grupo asociado, todo el tráfico a los miembros del grupo circula por este árbol. Los árboles de ruta de acceso más corta tienen una entrada (S, G) con una lista de interfaces salientes, donde S es la dirección de origen y G el grupo de Multicast. Como ejemplos de otros protocolos que utilizan este tipo de árboles se pueden destacar DVMRP y MOSPF, que son protocolos de modo denso. La figura 2 muestra un ejemplo de un árbol de ruta de acceso más corta.

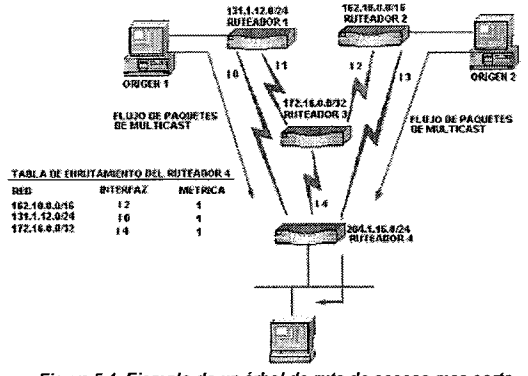


Figura 5.4 Ejemplo de un árbol de ruta de acceso mas corta

En el ejemplo, el árbol de ruta de acceso más corta para el origen 1 se encuentra, a través de la interfaz I0, en el enrutador 1, a pesar de que halla una ruta alternativa a través de la combinación de los enrutadores 1 y 3.
El árbol de ruta de acceso más corta para el origen 2 se genera a través de la interfaz I3, a pesar de que, una vez más, exista una ruta alternativa pero más larga. En este ejemplo la métrica representa cuentas de saltos.

5.2.3 Árboles compartidos

En PIM-SM, los árboles compartidos se conocen por árboles RP o árboles de punto de reunión (RPT), ya que confían en un enrutador central, el punto de reunión (RP), que recibe todo el tráfico desde los orígenes y lo reenvía a los receptores. Los miembros envían uniones explícitas al nodo central. De este modo, no se supone que todos los hosts sean receptores. Se obtiene como resultado un único árbol para cada grupo de Multicast, independientemente del número de orígenes.
Los únicos enrutadores que tienen información acerca del grupo son los que se encuentran en el árbol y los datos se envían sólo a los receptores interesados. Los árboles compartidos tienen una entrada (*, G), donde G es el grupo de Multicast. Con un punto de reunión, los receptores tienen un lugar al que se pueden unir aunque en ese momento no exista ningún origen. El árbol compartido es unidireccional, lo que significa que los datos fluyen sólo desde el punto de reunión hacia los receptores.
Para que un host diferente al punto de reunión realice envíos en el árbol, los datos se deben enviar por un túnel al punto de reunión antes de que se pueda realizar un envío Multicast a los usuarios. Esto significa que, si un receptor representa también un origen, no puede utilizar ese árbol para enviar paquetes al punto de reunión. Sólo lo puede utilizar para recibir paquetes desde él. Aunque ocurra así en la mayor parte de los casos, hay casos excepcionales, como cuando el origen se encuentra entre el punto de reunión y los receptores, y ya está en el árbol. En este caso, los datos fluyen directamente desde el origen hacia los receptores.
Los árboles de punto de reunión sufren mayores retrasos (los paquetes deben enviarse al punto de reunión antes de que se puedan distribuir) pero tienen que mantener menos información de estado de enrutador. A continuación se indican algunos ejemplos de aplicaciones en los que este tipo de árboles resulta adecuado:

- Redes con muchos orígenes de datos de baja velocidad
- Aplicaciones que pueden tolerar retrasos
- Aplicaciones que requieren políticas y control de acceso lógicos para muchos de los participantes de un grupo
- Redes en las que la mayor parte de los árboles de origen se solapan topológicamente con el árbol compartido

Las aplicaciones para conferencia pueden utilizar tanto los árboles de ruta de acceso más corta como los de punto de reunión (recuerde que PIM-SM admite el uso simultáneo de ambos). El árbol de punto de reunión se podría utilizar para paquetes de mantenimiento de conexiones abiertas, porque los datos se envían a baja velocidad. Los orígenes podrían utilizar los árboles de ruta de acceso más corta porque envían grandes cantidades de datos.

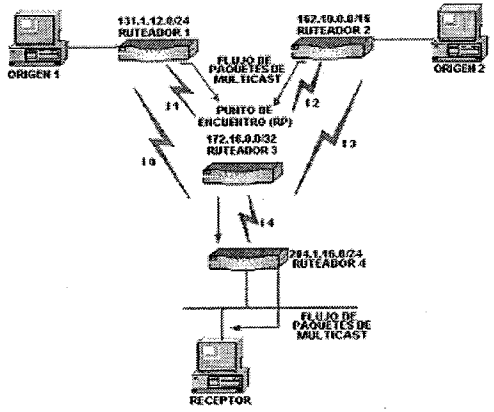


Figura 5.5 Ejemplo de un árbol compartido

En este ejemplo, aunque la configuración de la red sea la misma que en el ejemplo de la ruta de acceso más corta, el flujo del tráfico es diferente. Todo el tráfico de Multicast desde el origen(1) fluye por la interfaz I(1) en el enrutador 1 al enrutador 3, que es el punto de reunión, y desde el origen(2) fluye al punto de reunión por la interfaz I(2) en el enrutador 2. Estas rutas desde los orígenes al punto central son las más cortas.
A continuación, el punto de reunión distribuye los datos a los receptores que se han unido explícitamente al grupo de Multicast con un árbol único para todos los receptores. Puede haber varios puntos de reunión en una red, pero sólo debería haber uno para cada grupo de Multicast. A pesar de que cada ruta desde el punto de reunión al receptor sea la más corta, la ruta más corta desde el origen hasta los receptores no es la misma que la que va del receptor al punto de reunión.
Para el protocolo PIM-SM existe la posibilidad de utilizar tanto los árboles de acceso mas corto como los árboles compartidos.
En primer lugar, PIM-SM dispone de un método que permite al enrutador del último salto (el que está unido directamente a los receptores) abandonar el árbol compartido y unirse al árbol de ruta de acceso más corta si el volumen de tráfico lo garantiza. Este proceso se conoce como cambio a árbol de ruta de acceso más corta. En segundo lugar, cuando se utiliza un árbol de ruta más corta, los enrutadores no necesitan conservar tanta información de estado, lo que reduce la cantidad de memoria requerida.

5.2.4 Análisis del protocolo PIM-SM

5.2.4.1 Mensajes de saludo

Los enrutadores PIM envían de forma periódica mensajes de saludo para descubrir enrutadores PIM vecinos. El envío de paquetes Multicast de saludo se realiza mediante la dirección 224.0.0.13. Un campo Holdtime (tiempo de conservación) que especifica el periodo de validez de la información. Los enrutadores no envían ninguna confirmación de la recepción del mensaje de saludo. Asimismo, a diferencia de otros protocolos como DVMRP, cuando se recibe un mensaje de saludo, su interfaz no se agrega automáticamente a la lista de interfaces salientes para reenviar el tráfico de Multicast. PIM-SM utiliza un modelo de unión explícito en el que un receptor de dirección descendente debe unirse a un grupo antes de que el tráfico se reenvíe a la interfaz.

Reenvío de paquetes de Multicast

Los enrutadores de PIM-SIM reenvían tráfico de Multicast a todas las interfaces de los receptores que se han unido explícitamente a un grupo de Multicast. Los receptores realizan esta acción al enviar un informe de pertenencia al host de IGMP para cada grupo al que pertenecen. Estos mensajes se envían a la dirección del grupo. Tienen un periodo de vida (TTL) IP de 1 y están limitados a la subred local. El enrutador realiza una comprobación de orientación y reenvío de ruta inversa (RPF) antes de reenviar un paquete. El tipo de comprobación de RPF que un enrutador realiza depende de si el árbol es compartido o de ruta de acceso más corta.

Si es compartido, la comprobación de RPF utiliza la dirección IP del punto de reunión. Si es un árbol de ruta de acceso más corta, la comprobación de RPF utiliza la dirección del origen.

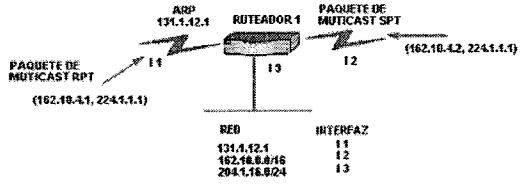


Figura 5.6 Comprobación de RPF en el árbol compartido y de ruta de acceso mas corta

El tráfico de Multicast del origen 162.10.4.1 utiliza el árbol compartido, lo que significa que el origen lo envía al punto de reunión y no al grupo de Multicast. El enrutador lo indicaría con una entrada (*, G) en lugar de con una entrada (S, G). Antes de enviar el tráfico, el enrutador 1 comprueba en la tabla de enrutamiento de Unicast si los

paquetes del punto de reunión llegan a la interfaz correcta. En este caso, sí lo hacen correctamente, ya que llegan a la interfaz I1 y se reenvían los paquetes. El tráfico de Multicast del origen 162.10.4.2 utiliza el árbol de ruta de acceso más corta. El enrutador lo indicaría con una entrada (S, G) para el origen. En este caso, el enrutador utiliza una dirección IP del origen para realizar la comprobación de RPF y mira la tabla de enrutamiento de Unicast para comprobar si el tráfico del origen llega a la interfaz correcta. El tráfico que llega a la interfaz correcta se envía a todas las interfaces salientes que conducen a los receptores de dirección descendente si se cumple cualquiera de las siguientes condiciones:

- Un enrutador de dirección descendente PIM-SM ha enviado una unión a este enrutador.
- Hay un receptor con conexión directa que ha unido explícitamente el grupo por medio del protocolo IGMP.
- Se ha configurado de forma manual la interfaz para unirse al grupo.
- Existe una lista de todas las interfaces salientes para cada entrada (*, G) o (S, G).

5.2.4.2 Unión al árbol compartido

Como se ha explicado anteriormente, cuando un host desea unirse a un grupo de Multicast, envía un mensaje IGMP al enrutador de dirección ascendente, lo que significa que el enrutador puede aceptar el tráfico de Multicast para el grupo. Para ello, el enrutador debe notificar al punto de reunión que desea unirse al árbol compartido, por lo que envía un mensaje de unión PIM (*, G) al PIM vecino de dirección ascendente, en la dirección del punto de reunión.
Los mensajes de unión se difunden salto a salto a la dirección 224.0.0.13, que representa el grupo (del ejemplo mostrado). Esto significa que, en una red de acceso múltiple, todos los vecinos PIM permiten la unión, pero que sólo el PIM vecino de dirección ascendente la realiza. Se utiliza el mismo mensaje tanto para uniones como para eliminaciones. Cuando un enrutador PIM recibe una unión (*, G) de un enrutador de dirección descendente, comprueba si existe el estado (*, G) para el grupo G en la tabla de enrutamiento de Multicast.
Si el estado ya existe, el mensaje de unión ha llegado al árbol compartido y la interfaz desde la que se recibió el mensaje se incluye en la lista de interfaces salientes. Si no existe ningún estado, se crea una entrada (*, G), se incluye la interfaz en la lista de interfaces salientes y se vuelve a enviar al mensaje de unión hacia el punto de reunión. Cuando se crea el estado (*, G) desde el enrutador de último salto al punto de reunión, el tráfico de Multicast para G puede llegar al host que se ha unido al grupo. Como se muestra en la siguiente figura:

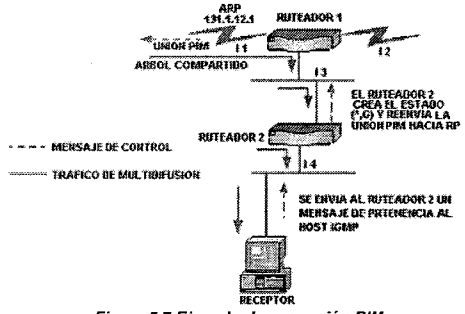


Figura 5.7 Ejemplo de una unión PIM

En este ejemplo, el receptor envía al enrutador 2 un mensaje de pertenencia al host IGMP y notifica su intención de unirse al grupo G de Multicast. Se trata del primer receptor conectado al enrutador 2 que participa en el grupo y, por tanto, el enrutador no tiene ningún estado (*, G). Crea una entrada y agrega I4 a la lista de interfaces salientes. A continuación, reenvía el mensaje de unión al vecino de dirección ascendente, osea al enrutador 1. Este enrutador tampoco tiene un estado (*, G), por lo que repite el proceso: vuelve a enviar el mensaje de unión al punto de reunión. El proceso continúa hasta que el punto de reunión recibe el mensaje de unión o hasta que un enrutador de dirección ascendente que tiene un estado (*, G) recibe el mensaje. En ambos casos se ha creado un árbol compartido que recorre el camino desde el punto de reunión al receptor. Observe que, hasta que el receptor envía el mensaje IGMP, no ocurre nada. El receptor inicia el proceso de unión.

El enrutador designado Cuando se conectan varios enrutadores a una red de acceso múltiple (por ejemplo, Ethernet) se debe elegir uno como enrutador designado (DR) para un cierto periodo. El enrutador designado es el responsable de enviar mensajes de unión y eliminación al punto de reunión. Para elegirlo, cada enrutador PIM de la red analiza los mensajes de saludo recibidos y compara su dirección IP con las de sus vecinos. El enrutador con la dirección más alta es el designado. Como se muestra en la siguiente figura.

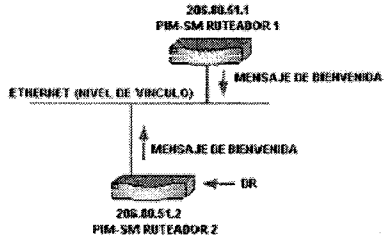


Figura 5.8 Selección del enrutador designado

En este ejemplo, el enrutador 2 se convierte en el enrutador designado porque tiene la dirección IP más alta. Si no se recibe ningún mensaje de saludo del enrutador designado después de un periodo configurable, se realiza otra selección de enrutador designado, lo que significa que el enrutador con la dirección IP más alta se convierte en el designado.

5.2.4.3 Registro con el punto de reunión

Los orígenes del tráfico de Multicast no se unen necesariamente al grupo al que envían datos. Un enrutador de primer salto (el enrutador designado) puede iniciar la recepción del tráfico desde un origen sin tener ningún estado (S, G) para el origen. Esto significa que no hay información acerca de cómo llevar tráfico de Multicast al punto de reunión a través de un árbol. Cuando el enrutador designado del origen recibe el primer paquete de Multicast, lo encapsula en un mensaje de registro Unicast y lo difunde al punto de reunión para ese grupo. El punto de reunión deshace la encapsulación en cada mensaje de registro y reenvía el paquete de datos extraído a los miembros de dirección descendente en el árbol compartido. Es posible que el punto de reunión envíe una unión (S, G) al enrutador designado para poder generar el árbol de ruta de acceso más corta en el origen. Esto ocurre, normalmente, cuando se alcanza un umbral de velocidad de datos.

Cuando se ha establecido la ruta de acceso desde el origen al punto de reunión, el enrutador designado comienza a enviar tráfico al punto de reunión en forma de paquetes de Multicast IP estándar y encapsulado dentro de mensajes de registro Unicast. Esto significa que el punto de reunión recibirá temporalmente algunos paquetes por duplicado. Cuando el punto de reunión detecta los paquetes de Multicast normales, envía un mensaje de detención de registro al enrutador designado del origen, lo que significa que debería dejar de enviar paquetes de registro Unicast.

La siguiente figura muestra el funcionamiento del proceso de registro (considerando que los enrutadores no tienen un estado preexistente).

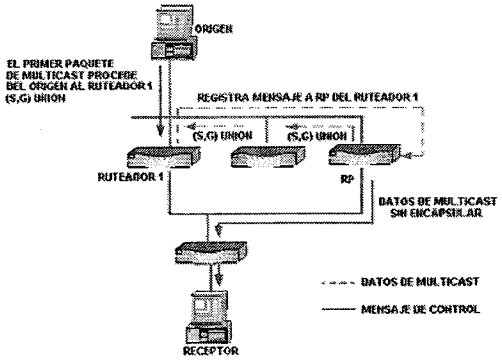


Figura 5.9 Ejemplo de paquetes de registro

La ilustración muestra un origen que comienza a transmitir datos de Multicast. El enrutador designado del origen (enrutador 1) crea un estado (S, G) y difunde el paquete al punto de reunión, encapsulado en un mensaje de registro. Cuando el punto de reunión recibe el paquete, extrae los datos de Multicast del mensaje de registro y, si hay receptores interesados, lo reenvía por el árbol compartido. Hasta que se establezca el árbol de ruta de acceso más corta, el enrutador 1 continuará el envío Unicast de mensajes de registro que contienen datos de Multicast al punto de reunión. Cuando se construye el árbol, el enrutador 1 comienza a reenviar el mismo tráfico de Multicast, enviado como paquetes de Multicast IP estándar, en dirección descendente en el árbol de ruta de acceso más corta. Esto significa que el punto de reunión recibirá temporalmente los datos del origen por medio de los mensajes de registro y a través del árbol de ruta de acceso más corta.
Cuando el punto de reunión comienza a recibir el tráfico del origen tanto en forma de mensajes de registro como en Multicast, envía un mensaje de detención de registro al enrutador designado. Esto notifica al enrutador designado que el tráfico se está recibiendo en forma de paquetes de Multicast IP estándar en el árbol de ruta de acceso más corta. Cuando el enrutador designado recibe este mensaje, deja de encapsular el tráfico en mensajes de registro Unicast.

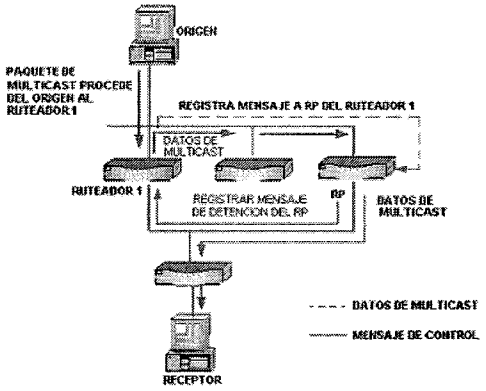


Figura 5.10 Ejemplo de un paquete de detención de registro

El otro caso en el que el punto de reunión envía mensajes de detención de registro se produce cuando ningún receptor pertenece al grupo de Multicast. Un origen puede iniciar la transmisión a un grupo que no tiene ningún miembro. El punto de reunión descarta estos paquetes y envía una detención de registro para que el enrutador designado deje de enviar mensajes de registro.

5.2.4.4 Eliminación de interfaces

Cuando un punto de reunión recibe un mensaje de eliminación, no vuelve a enviar tráfico desde el origen indicado en el mensaje. Estos mensajes se crean con un

enrutador hoja (el enrutador que está conectado directamente a los receptores), que se considerará el enrutador designado. Si el último miembro de un grupo de Multicast envía al enrutador designado un mensaje de renuncia de la versión 2 de IGMP (o, en la versión 1 de IGMP, simplemente agota el tiempo de espera), el estado IGMP del enrutador designado se elimina y se quita la interfaz de las listas de interfaces salientes (S, G) y (*, G) para el grupo G. Si se quitan todas las interfaces de esta lista del estado (*, G) (lo que significa que el enrutador no tiene receptores en ninguna interfaz que sean miembros de G), se envía un mensaje de eliminación al punto de reunión en dirección ascendente a través del árbol compartido. Si los enrutadores en dirección ascendente tampoco tienen listas de interfaces salientes, el mensaje se sigue reenviando al punto de reunión. Si un enrutador todavía tiene un estado (*, G) para los receptores en otra interfaz, también quitará esta interfaz, a menos que reciba un mensaje de suplantación de una unión de un vecino PIM. Se aplica el mismo proceso de eliminación de ramas si se está utilizando un árbol de ruta de acceso más corta en lugar de un árbol compartido.

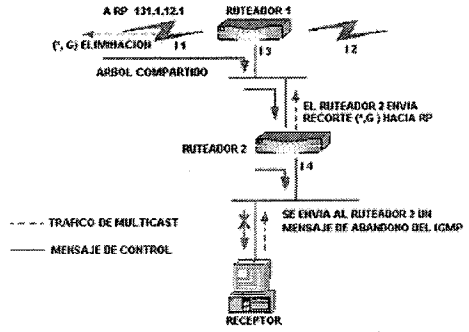


Figura 5.11 Ejemplo de proceso de eliminación

En este ejemplo, el enrutador 2 (enrutador hoja) recibe un mensaje de renuncia IGMP del receptor. Procesa el mensaje y, como no hay otros miembros del grupo, quita a I4 de (*, G) y de cualquier lista de interfaces salientes de (S, G). En este momento, la lista de interfaces salientes del enrutador es nula. Por tanto, envía un mensaje de eliminación (*, G) al árbol compartido, a través de I3, hacia el punto de reunión. El enrutador 1 recibe el mensaje de eliminación y provoca la eliminación de la interfaz de I3 de la lista de interfaces salientes de la entrada (*, G) en la tabla de enrutamiento de Multicast. Observe que transcurre cierto tiempo antes de que la eliminación sea efectiva. En redes de acceso múltiple, es importante esperar, porque es posible que se reciba un mensaje de suplantación de la unión de un vecino PIM. En este caso no se ha recibido ninguno y, por esta razón, se elimina la interfaz. Teniendo en cuenta que la lista de interfaces salientes de (*, G) ahora no tiene elementos, se reenvía un mensaje de eliminación (*, G) al árbol compartido hacia el punto de reunión. Este proceso se repite hasta que el punto de reunión recibe este mensaje o hasta que se alcanza un

enrutador cuya lista de interfaces salientes de (*, G) no llegue a estar vacía como resultado de la eliminación.

5.2.4.5 Mensajes de aserción

En redes de acceso múltiple, puede haber rutas paralelas al origen o al punto de reunión. A causa de este hecho, es posible que los miembros de los grupos reciban paquetes duplicados de varios enrutadores. Para evitar el problema, PIM-SM utiliza mensajes de aserción para determinar un retransmisor designado.

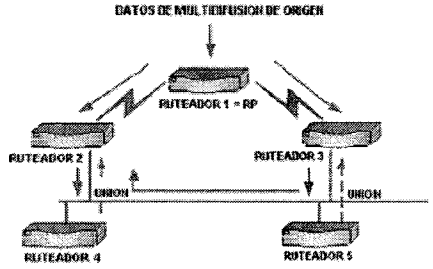


Figura 5.12 Ejemplo de una red que requiere aserción

En este ejemplo, el enrutador 1, el punto de reunión, reenvía tráfico de Multicast a sus vecinos, los enrutadores 2 y 3. Estos enrutadores, a su vez, reenvían el tráfico a la red de área local. Considere que el enrutador 3 transmite en primer lugar. El enrutador 2 recibe el paquete de Multicast en una interfaz que tiene este grupo en la lista de interfaces salientes. El enrutador 2 reenvía el paquete al enrutador 3, lo que significa que éste también ha recibido datos en una interfaz saliente. La recepción de un paquete entrante en una interfaz saliente alerta a los enrutadores del hecho de que otros vecinos PIM-SM en la red de área local también están reenviando tráfico al grupo. Esto significa que los miembros del grupo recibirán datos duplicados. Para evitar esta situación, los enrutadores emiten mensajes de aserción para seleccionar un único enrutador que reenvíe el tráfico. Los enrutadores de dirección descendente escuchan los mensajes de aserción para conocer el enrutador que se ha elegido y, por tanto, para saber dónde deben enviar los siguientes mensajes de unión. En el ejemplo, el enrutador 4 envía primero mensajes de unión al enrutador 2 mientras que el enrutador 5 envía primero mensajes de unión al enrutador 3. Después de la aserción, todos los mensajes de unión se enviarán al enrutador 2 ó 3, dependiendo de cuál de los dos se convierta en retransmisor designado. Si todos los enrutadores ejecutan el mismo protocolo de Unicast, el enrutador con la mejor métrica ganará la aserción. Por ejemplo, si todos los enrutadores utilizan RIP, se elegirá el enrutador con la cuenta de saltos más pequeña. Si las métricas son iguales, se elegirá el enrutador con la dirección IP más alta. Si los enrutadores ejecutan protocolos de Unicast diferentes, las métricas no se pueden comparar. Por ejemplo, RIP utiliza una cuenta de saltos como métrica mientras que la métrica de OSPF se basa en la velocidad de la interfaz. En este caso,

el valor de prioridad de la métrica determina el enrutador que reenviará el tráfico y el enrutador que eliminará la interfaz. Se pueden configurar las prioridades de la métrica para cada protocolo de Unicast que se ejecuta en la red. Cuando un enrutador recibe un mensaje de aserción para un grupo, se compara el valor de la prioridad de la métrica en el paquete con el suyo propio. Si son iguales, se pueden comparar las métricas para determinar el enrutador que reenviará el tráfico. Si las prioridades de la métrica son diferentes, se selecciona la que tenga la prioridad de métrica más baja.

5.2.4.6 Cambio a un árbol de ruta de acceso más corta

Se puede configurar un límite de tráfico (expresado en kilobytes) en el enrutador de último salto, de forma que, cuando se rebase el límite de un grupo, el enrutador pasa del árbol de punto de reunión, al árbol de ruta de acceso más corta. Cuando ocurre esto, el enrutador designado envía una unión (S, G) hacia el origen del paquete. Esto crea un árbol de ruta de acceso más corta desde el origen, S, hasta el enrutador. El cambio a árbol de ruta de acceso más corta implica la utilización de la ruta de acceso más corta para enviar el tráfico de Multicast. Según la ubicación del origen en relación al punto de reunión, el paso puede reducir de manera considerable la lentitud de la red. Como inconveniente se puede destacar que se debe mantener una mayor cantidad de información de estado en los enrutadores. Para determinar si se debería producir el cambio, se calcula el total de la velocidad de agregado del tráfico del grupo que fluye en dirección descendente hacia el árbol de punto de reunión en un intervalo periódico determinado. Normalmente, si se rebasa esta velocidad, el siguiente paquete recibido para el grupo ocasiona el cambio (los detalles reales de lo que ocurre y la frecuencia con que se calcula la velocidad de agregado dependen de la implementación. El protocolo no los especifica).

5.2.4.7 Determinación del punto de reunión

La versión 1 de PIM-SM contaba con dos métodos posibles de determinación del punto de reunión. El primero era un método estático. Se debía configurar cada enrutador hoja con la dirección de un punto de reunión para un grupo o un conjunto de grupos. La segunda opción era dinámica y utilizaba un método conocido como punto de reunión automático. La versión 2 de PIM-SM dispone de un único método que utiliza un enrutador de arranque (BSR) que origina mensajes de arranque (de Bootstrap). Estos mensajes se utilizan para elegir un enrutador de arranque, en caso necesario, y para diseminar la información del punto de reunión. El envío Multicast de los mensajes se realiza al grupo all-pim-routers en cada vínculo. Se configuran uno o varios enrutadores para que sean candidatos a enrutador de arranque. Si no está claro qué enrutador debe ser el de arranque, los candidatos dirigen anuncios al dominio (mediante Orientación y reenvío de ruta inversa, para que resulte más barato). Se elige el enrutador con la mayor prioridad. Si todas las prioridades son iguales, el candidato con la dirección IP más alta se convierte en enrutador de arranque. Un dominio en este contexto representa un conjunto contiguo de enrutadores que implementan la versión 2 de PIM-SM y que están configurados para funcionar dentro de unos límites comunes que definen los enrutadores de límite de Multicast PIM (PMBR). En resumen, los PMBR conectan cada dominio PIM al resto de Internet. Los enrutadores configurados para ser candidatos a punto de reunión difunden esta información al enrutador de

arranque. Es normal que los enrutadores configurados para ser candidatos a enrutador de arranque también se configuren para ser puntos de reunión. El anuncio del candidato a punto de reunión contiene la dirección del enrutador anunciante y el grupo de Multicast al que puede prestar servicios. El enrutador de arranque incluye un conjunto de candidatos a punto de reunión (el conjunto de punto de reunión), junto con las direcciones de grupo correspondientes, en los mensajes de arranque que crea periódicamente. Los mensajes de arranque se distribuyen salto a salto por el dominio.
Los enrutadores reciben y almacenan los mensajes de arranque que el enrutador de arranque origina. Cuando un enrutador designado recibe una indicación de pertenencia de IGMP, o un paquete de datos de un host conectado directamente, para un grupo para el que no tiene una entrada, el enrutador designado utiliza una función *hash* para asignar la dirección del grupo a uno de los candidatos a punto de reunión que pueden prestar sus servicios al grupo. A continuación, el enrutador designado envía un mensaje de unión o eliminación hacia (o difunde un mensaje de registro a) el punto de reunión.
Como se ha señalado al principio, al ser un protocolo de enrutador a enrutador, se deben actualizar todos los enrutadores de la red para que lo admitan. El segundo problema surge del hecho de que, teniendo en cuenta que el número de candidatos a punto de reunión aumenta linealmente con el tamaño del dominio, el protocolo no puede ampliarse de forma global. Al asignar G como punto de reunión se puede crear un problema de ampliación, ya que implica la orientación de los anuncios del enrutador de arranque. La ubicación del punto de reunión representa otro problema. Hay muchos proveedores de servicios Internet en el mundo y ninguno de ellos desea depender de un punto de reunión en el dominio de otro para atender la Multicast entre sus propios usuarios.

5.2.4.8 Mensajes de control de PIM-SM

Esta sección estudia los formatos para campos de dirección cifrados y mensajes de control de PIM-SM. Asimismo, muestra cómo se encapsulan los mensajes de control en paquetes IP y el encabezado estándar para los mensajes PIM. Para esto de analizarán los siguientes formatos:

- Encapsulación de mensajes de control PIM-SM
- Encabezado de paquetes de PIM-SM
- Campo de dirección de Unicast cifrada (*Encoded Unicast Address*)
- Campo de dirección de grupo cifrada (*Encoded Group Address*)
- Campo de dirección de origen cifrada (*Encoded Source Address*)
- Mensaje de aserción
- Mensaje de arranque
- Anuncio de candidato a punto de reunión
- Mensaje de saludo
- Mensaje de unión o eliminación
- Mensaje de registro
- Mensaje de detención de registro

5.2.4.8.1 Encapsulación de mensajes de control PIM

La siguiente figura muestra cómo se organizan los mensajes de control de PIM-SM en un paquete IP.

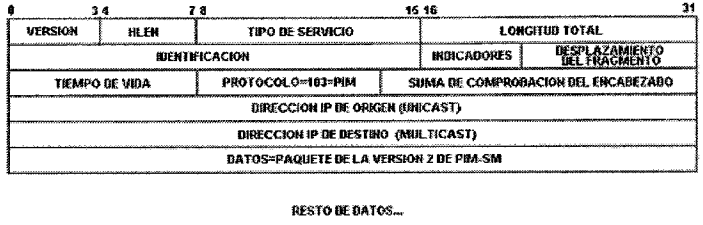


Figura 5.13 Mensaje de control PIM encapsulado

Los mensajes de la versión 2 de PIM-SM se encapsulan en paquetes IP con el número de protocolo 103.

5.2.4.8.2 Encabezado de paquetes PIM-SM

La siguiente figura muestra el encabezado para un paquete de la versión 2 de PIM-SM.

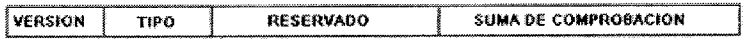


Figura 5.14 Encabezado de paquetes de la versión 2 de PIM encapsulado

Los campos del encabezado tienen los siguientes valores:

- *Ver* es el número de versión PIM. En la versión 2, el valor es 2.
- *Type* es el valor relacionado con el mensaje de control específico (consulte la tabla 1 a continuación).
- *Reserved* se transmite como 0. Tras la recepción se omite.
- *Checksum* es el complemento a uno de 16 bits de la suma en complemento a uno de todo el mensaje PIM (excluida la parte de datos del mensaje de registro).

Cada mensaje de control tiene un valor Type diferente, que se enumera en la tabla:

Tipo	*Descripción*
0	Saludo
1	Registro
2	Detención de registro
3	Unión o eliminación
4	Arranque
5	Aserción
8	Anuncio de candidato a punto de reunión

Tabla 5.1 Tipo de mensaje de la versión 2 de PIM

5.2.4.8.3 Dirección de Unicast cifrada (Encoded Unicast Address)

La siguiente figura muestra el formato del campo de dirección de Unicast cifrada.

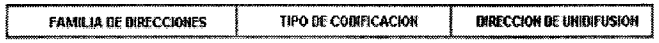


Figura 5.15 Formato del campo de dirección de Unicast cifrada

Los subcampos tienen los siguientes valores:

- *Address Family* representa la familia a la que pertenece la dirección de Unicast. Los números de Address Family y sus valores asociados se enumeran en la tabla 2 a continuación.
- *Encoding Type* representa el tipo de cifrado que se utiliza en una familia de direcciones específica. El valor 0 está reservado para este campo y representa el cifrado original de la familia de direcciones.
- *Unicast Address* representa la dirección de Unicast como lo especifican los campos Address Family y Encoding Type.
- La siguiente tabla muestra los números de la familia de direcciones para las versiones 4 y 6 de IP. A pesar de que se asignen otros números, no se suelen utilizar.

Número	Descripción
0	Reservado
1	Versión 4 de IP
2	Versión 6 de IP

Tabla 5.2 Número de direcciones para las versiones 4 y 6 de IP

5.2.4.8.4 Dirección de grupo cifrada (Encoded Group Address)

La siguiente figura muestra el formato del campo de dirección de grupo cifrada.

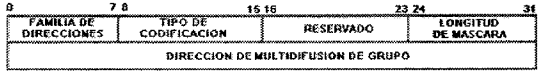


Figura 5.16 Formato del campo de dirección de grupo cifrada

Los subcampos tienen los siguientes valores:

- *Address Family* y *Encoding Type*: consulte más arriba las definiciones de la sección "Encoded Unicast Address".
- *Reserved* se transmite como 0. Se omite tras la recepción.
- *Mask Length* representa el número de bits contiguos y justificados a la izquierda que se utilizan como máscara para describir la dirección. La longitud de la máscara debe ser menor o igual que la longitud de la dirección expresada en bits para la familia de direcciones y el tipo de cifrado específicos. En la

versión 2 de PIM-SM, se recomienda que el valor de este campo sea 32 para el cifrado original de la versión 4 de IP.
- *Group Multicast Address* representa la dirección del grupo de Multicast.

5.2.4.8.5 Dirección de origen cifrada (Encoded Source Address)

La siguiente figura muestra el formato del campo de dirección de origen cifrada.

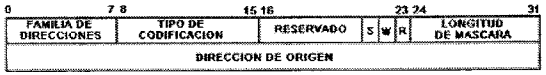


Figura 5.17 Formato del campo de dirección de origen cifrada

Los subcampos tienen los siguientes valores:

- *Address Family, Encoding Type* y *Reserved*: consulte más arriba las definiciones de las secciones "Encoded Unicast Address" y "Encoded Group Address".
- El campo *S* representa el bit de esparcido (Sparse). El valor para PIM-SM es 1. Se utiliza por razones de compatibilidad con la versión 1 de PIM.
- El bit *WC* representa el bit comodín. Si su valor es 1, la unión o eliminación se aplica a la entrada (*, G) o (*, *, punto de reunión). Si el valor es 0, la unión o la eliminación se aplica a la entrada (S, G), donde S representa la dirección de origen. Las uniones o eliminaciones que se envían al punto de reunión deben establecer el valor del bit en 1. Un paquete de datos coincidirá con una entrada (*, *, punto de reunión) si no hay más entradas específicas, como (S, G) o (*, G), y la dirección del grupo de destino del paquete se asigna al punto de reunión enumerado en la lista de la entrada (*, *, punto de reunión). Para obtener más información acerca de esta entrada en particular y acerca de su relación con la interoperabilidad entre PIM-SM y protocolos de modo denso, consulte el documento RFC 2362.
- El bit *R* representa el bit RPT (árbol de punto de reunión o compartido). Si su valor es 1, la información referente a (S, G) se envía al punto de reunión. Si es 0, la información se envía a S, donde S representa la dirección de origen.
- *Mask Length*: consulte la definición proporcionada más arriba en la sección "Encoded Group Address".

5.2.4.8.5 Mensaje de aserción

En la siguiente figura muestra el formato del mensaje de aserción.

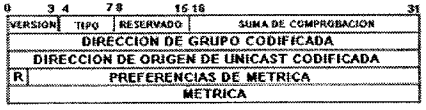


Figura 5.18 Formato del mensaje de aserción

Los campos tienen los siguientes valores:

- *Version, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Encoded Group Address* representa la dirección del grupo al que estaba dirigido el paquete y que ha desencadenado la aserción. El formato está definido en la sección "Encoded Group Address".
- *Encoded Unicast Source Address* representa la dirección de origen que se encuentra en el paquete de Multicast que ha desencadenado la aserción. El formato se define más arriba en la sección "Encoded Unicast Address".
- *R* representa el bit RPT. Tiene el valor 1. Si el paquete de Multicast que ha desencadenado la aserción se enruta en dirección descendente al árbol de punto de reunión, el bit RPT se iguala a uno. Si el paquete se enruta en dirección descendente al árbol de ruta de acceso más corta, el bit RPT se iguala a cero.
- *Metric Preference* representa el valor de prioridad asociado al protocolo de enrutamiento de Unicast que ha proporcionado la ruta a la dirección del host.
- *Metric* representa la métrica de la tabla de enrutamiento de Unicast. Se expresa en las unidades adecuadas para el protocolo de enrutamiento de Unicast.

5.2.4.8.6 Mensaje de arranque

Los mensajes de arranque se dividen en *fragmentos semánticos* si el mensaje original rebasa el tamaño máximo de paquete. La siguiente figura muestra el formato de un fragmento sencillo. Los campos tienen los siguientes valores:

- *Version, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Fragment Tag* representa un número generado al azar que se utiliza para distinguir entre fragmentos que pertenecen a diferentes mensajes de arranque. Los fragmentos que pertenecen al mismo mensaje de arranque llevan la misma etiqueta de fragmento.
- *Hash Mask Length* representa la longitud (en bits) de la máscara para que se utilice en la función *hash*. Se recomienda el valor 30 para la versión 4 de IP y el valor 126 para la versión 6 de IP.
- *BSR Priority* representa el valor de prioridad del enrutador de arranque incluido. Este campo se considera de un byte de orden alto al comparar direcciones de enrutadores de arranque.
- *Encoded Unicast BSR Address* representa la dirección del enrutador de arranque para el dominio. Tiene el mismo formato del campo Encoded Unicast Address.

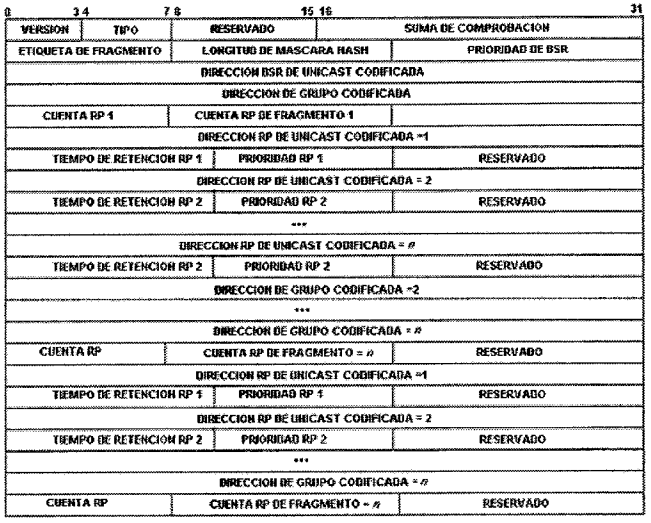


Figura 5.19 Formato del mensaje de arranque

- *Encoded Group Address* representa el prefijo de grupo (dirección y máscara) con el que se relacionan los candidatos a punto de reunión. El formato se analiza más arriba en la sección "Encoded Group Address".
- *RP Count 1Un* representa el número de direcciones de candidatos a punto de reunión incluidos en el mensaje de arranque completo para el prefijo de grupo correspondiente.
- *Fragment RP Count 1Um* representa el número de direcciones de candidatos a punto de reunión incluidos en el fragmento del mensaje de arranque para el prefijo de grupo correspondiente.
- *Encoded Unicast RP Address 1Um* representa la dirección de los candidatos a punto de reunión para el prefijo del grupo correspondiente. El formato se define más arriba en la sección "Encoded Unicast Address".
- *RP1Um Holdtime* representa el periodo de validez para el punto de reunión correspondiente. Este campo se copia desde el campo Holdtime del punto de reunión relacionado que se encuentra almacenado en el enrutador de arranque.
- *RP1Um Priority* representa la prioridad de punto de reunión y de Encoded Group Address correspondientes. Este campo se copia desde el campo Priority almacenado en el enrutador de arranque al recibir un anuncio de un candidato a punto de reunión. La prioridad más alta es 0 (cuanto menor sea el valor del campo Priority, mayor será la prioridad). Observe que la prioridad se representa para cada punto de reunión o dirección de grupo cifrada.

5.2.4.8.8 Mensaje de candidato a punto de reunión

La siguiente figura muestra el formato del mensaje de candidato a punto de reunión.

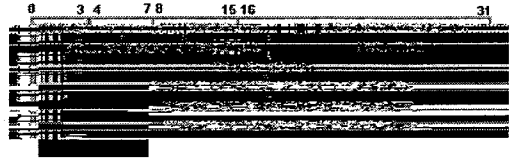


Figura 5.20 Formato del mensaje de candidato apunto de reunión

- Los campos tienen los siguientes valores:
- *Version, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Prefix Count* representa el número de direcciones de grupo cifradas incluidas en el mensaje. El valor 0 significa que se incluyen todos los grupos de Multicast.
- *Priority* representa la prioridad del candidato a punto de reunión para la dirección de grupo correspondiente. La prioridad más alta es 0, es decir, un valor menor significa una mayor prioridad. El enrutador de arranque almacena este valor junto con la dirección del punto de reunión y la dirección de grupo cifrada correspondiente.
- *Holdtime* representa el periodo durante el que el anuncio es válido.
- *Encoded Unicast RP Address* representa la dirección de la interfaz para anunciarse como candidato a punto de reunión.
- *Encoded Group Address 1Un* representa las direcciones de grupo para las que el candidato a punto de reunión se está anunciando.

5.2.4.8.9 Mensaje de saludo

La siguiente figura muestra el formato del mensaje de saludo.

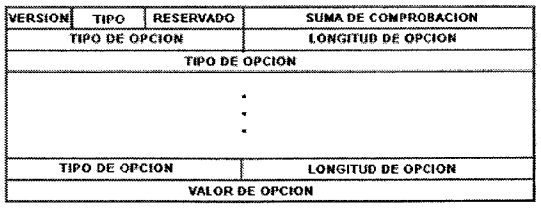


Figura 5.21 Formato del mensaje de saludo

Los campos tienen los siguientes valores:

- *Ver, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Option Type* representa el tipo de opción ofrecido en el campo Option Value.
- *Option Length* representa la longitud del campo Option Value en bytes.
- *Option Value* representa un campo de longitud variable que contiene el valor de la opción.

La tabla siguiente muestra los valores de los campos Option.

Option Type	Option Length	Option Value
1	2	Holdtime
2-16	Reservado	Reservado

Tabla 5.3 Valores de los campos Option

La tabla siguiente muestra los valores del parámetro del periodo de validez (Holdtime).

Valor	Descripción
0xFFFF	No hay tiempo de espera
0	Tiempo de espera igual a cero
Cualquier otro valor	Valor de tiempo de espera del vecino

Figura 5.4 Valores del parámetro Hold-Time

El valor de tiempo de espera 0xFFFF significa que el vecino nunca caduca. Este valor evita el envío periódico de mensajes de saludo. Resulta útil para conexiones con tarifa, por ejemplo, las proporcionadas por ISDN (RDSI). Los mensajes de saludo periódicos conservarían el vínculo activo, a pesar de que no hubiera tráfico de datos de usuario con lo que se facturaría de forma continua a los clientes.

5.2.4.8.10 Mensajes de unión o eliminación

La siguiente figura muestra el formato de los mensajes de unión o eliminación.

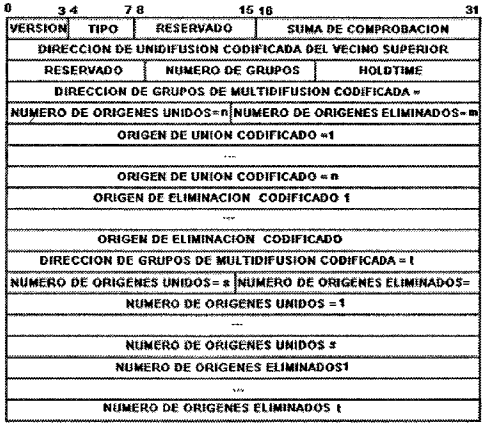


Figura 5.22 Formato de los mensajes de unión o eliminación

Los campos tienen los siguientes valores:

- *Version, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Encoded Unicast Upstream Neighbor Address* representa la dirección del vecino de dirección ascendente (a través de la interfaz RPF). El formato se define más arriba en la sección "Encoded Unicast Address".
- *Holdtime* representa el tiempo en segundos que el receptor debe mantener activo el estado de unión o eliminación. Si el valor de Holdtime es 0xFFFF, el receptor del mensaje nunca agota el tiempo de espera de la lista de interfaces salientes. Se puede utilizar este valor con líneas ISDN (RDSI) para evitar la conservación del vínculo con los mensajes periódicos de unión o eliminación. Si el valor de Holdtime es 0, el tiempo de espera de la información se agota inmediatamente.
- *Number of Groups* representa el número de conjuntos de grupos de Multicast del mensaje.
- *Encoded Multicast Group Address* representa la dirección del grupo de Multicast. El formato se define más arriba en la sección "Encoded Group Address".
- *Number of Joined Sources* representa el número de direcciones de orígenes de unión enumerados para un grupo específico.
- *Encoded Join Source Address 1...n* representa la enumeración de orígenes a los que el enrutador remitente reenviará paquetes de Multicast si se reciben en la interfaz correcta. El formato se describe más arriba en la sección "Encoded Source Address".
- *Number of Pruned Sources* representa el número de direcciones de orígenes de eliminación enumerados para un grupo.

- *Encoded Prune Source Address 1...n* representa la lista que contiene los orígenes que se van a eliminar.

5.2.4.8.11 Mensaje de registro

La siguiente figura muestra el formato de los mensajes de registro.

Figura 5.23 Formato de mensajes de registro

Los campos tienen los siguientes valores:

- *Ver, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *B* es el bit de límite (Border). Si el enrutador es uno designado para un origen al que está conectado directamente, el valor del bit B será 0. Si el enrutador es un PMBR para un origen en una nube conectada directamente, el valor del bit B será 1.
- *N* es el bit de registro nulo (Null-Register). Un enrutador designado que está analizando el punto de reunión antes de que caduque el temporizador local de registro y supresión establece su valor en 1. De otra manera, el valor es 0.
- *Multicast Data Packet* es el paquete original que envía el origen.

5.2.4.8.12 Mensaje de detención de registro

La siguiente figura muestra el formato de los mensajes de detención de registro.

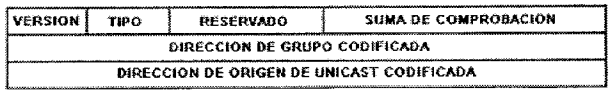


Figura 5.24 Formato de mensaje de detención de registros

Los campos tienen los siguientes valores:

- *Ver, Type, Reserved* y *Checksum*: consulte las definiciones proporcionadas más arriba en la sección "Encabezado de paquetes de PIM-SM".
- *Encoded Group Address*: consulte anteriormente la sección "Encoded Group Address".
- *Encoded Unicast Source Address*: representa la dirección de origen incluida en el paquete de Multicast encapsulada en el mensaje de registro. Encoded Unicast

Source Address utiliza el mismo formato que Encoded Source Address (consulte anteriormente este campo).

En la actualidad, PIM-SM es el protocolo de enrutamiento estándar de facto. Está diseñado para funcionar de forma eficaz en las redes de área extensa, donde los grupos de Multicast están dispersos. Conserva el modelo de servicio de Multicast IP tradicional de pertenencia iniciada por el receptor y admite árboles compartidos y de ruta de acceso más corta. PIM-SM no depende de un protocolo de enrutamiento de Unicast específico. Al ser un protocolo de enrutador a enrutador, se deben actualizar todos los enrutadores de la red para que admitan la versión 2 de PIM-SIM.

Capítulo 6

POSIBLES SOLUCIONES DE LA IMPLEMENTACION DE MULTICAST SOBRE MPLS-VPN

CAPITULO 6. Posibles Soluciones de la Implementación de Multicast sobre MPLS-VPN'S

6.1 Propósito de las posibles soluciones de implementación

El propósito de este capitulo es entender y conocer las posibles soluciones que necesitaremos para resolver el problema de cómo implementar una red de Multicast IP basada en las VPN's, además, describir las arquitecturas para este tipo de soluciones.

Hasta hoy, MPLS/VPN ha sido diseñado para soportar sólo transmisiones Unicast, sin embargo, hay que tomar en consideración que las empresas que utilizan redes privadas como las VPN's necesitan soportar algunas aplicaciones basadas en el principio de Multicast, y algunos ISP's requieren ofrecer a sus clientes servicios adicionales como por ejemplo: Video para clientes de VPN's. Es por esto que surge la necesidad de combinar el Multicast sobre VPN's que operan sobre la tecnología MPLS.

6.2 Descripción global del Multicast y sus ventajas ante Unicast

6.2.1 Generalidades de Multicast

Primero, comenzaremos por resumir algunas características importantes del Multicast, las cuales han sido descritas en capítulos anteriores. De la misma manera, describiremos la ventaja que nos proporciona la utilización del Multicast sobre el Unicast, esto para hacer una mejor definición del problema y tener mayor conocimiento de la solución que debemos aplicar.

Árboles

Una distribución en forma de árbol de Multicast surge cuando un paquete de datos es transmitido por una fuente, mientras que la red es la responsable de reproducir dicho paquete a cada punto de bifurcación en la red. Existen dos tipos de árboles:

- *ÁRBOLES DE CAMINO CORTO (SHORTEST PATH TREE)*
- *ÁRBOLES COMPARTIDOS (SHARED TREES)*

Shortest Path Tree (SPT)

Los árboles de camino corto se encuentran alojados en la raíz de la fuente de datos. Es el único tipo de árbol que se puede utilizar en redes de Dense Mode (DM), aunque también se utilizan en redes del modo Sparse Mode (SM).

Árboles Compartidos

Son árboles unidireccionales dentro de la red, los cuales se encuentran alojados un punto común. Los árboles compartidos se utilizan en el Protocol Independent Multicast

Sparse Mode (PIM SM) y la raíz común del árbol compartido se llama Rendezvous Point. Este es el punto donde los receptores adquieren información de las fuentes activas.

Protocolos de Enrutamiento de Multicast

Algunos protocolos de enrutamiento fueron diseñados para trabajar con IP, los cuales requirieron una tabla de enrutamiento aparte para el tráfico de Multicast IP. Estos protocolos de enrutamiento son:

Distance Vector Multicast Routing Protocol (DVMRP)

Fue el primer protocolo de enrutamiento para Multicast y es un ejemplo de los protocolos de enrutamiento de árbol- raíz. Este protocolo realiza el enrutamiento básicamente por inundación utilizando la técnica conocida como propagación en el camino inverso o RPF (Reverse Path Forwarding). Esto es, cuando llega un paquete de Multicast se verifica su dilección de origen y trata de seguirse el camino inverso de la ruta de la cual proviene.

Multicast Open Shortest Path First (MOSPF)

Este protocolo está diseñado para situaciones en las que los grupos de Multicast cuentan con un número grande que los represente y hay suficiente ancho de banda. Con estos esquemas, es posible que la información acerca de la pertenencia de los paquetes de datos se envíe de forma innecesaria a interfaces que no conducen a fuentes de Multicast o a receptores interesados. Además, los enrutadores almacenan el estado relacionado con estos nodos no interesados, lo que resulta igualmente innecesario. Se acepta este exceso cuando la mayor parte de los hosts están interesados en los datos y hay suficiente ancho de banda para permitir el flujo de los mensajes de control. De cualquier otro modo resulta ineficaz

Core Base Trees (CBT)

CBT's fue creado para utilizar árboles de distribución compartida para entregar datos de Multicast, pero nunca se utilizó prácticamente mas que para redes experimentales.

Protocol Independent Multicast (PIM)

Este protocolo de enrutamiento admite tanto árboles compartidos como árboles de ruta de acceso más corta, no depende de ningún protocolo de enrutamiento de Unicast específico y utiliza el protocolo independiente de Multicast en modo esparcido (PIM-SM, *Protocol Independent Multicast-Sparse Mode*) envía paquetes de Multicast a grupos de Multicast y está diseñado para establecer de forma eficaz árboles de distribución a través de redes de área extensa (WAN). PIM-SM es "independiente de protocolo" porque puede utilizar la información de rutas que cualquier protocolo de enrutamiento introduzca en la base de información de enrutamiento de Multicast. Como ejemplos de estos protocolos de enrutamiento podemos encontrar protocolos como el Protocolo de información de enrutamiento (RIP, *Routing Information Protocol*) y el protocolo OSPF (*Open Shortest Path First*). No obstante, también se pueden utilizar

protocolos de Multicast que llenan las tablas de enrutamiento, como el Protocolo de enrutamiento de Multicast de vectores de distancia (DVMRP, *Distance Vector Multicast Routing Protocol*). Modo esparcido significa que el protocolo está diseñado para situaciones donde los grupos de Multicast están dispersos en una región extensa. PIM-SM supone que ningún host desea datos si no los solicita explícitamente. Sin embargo, PIM tiene un protocolo equivalente para modo denso (PIM-DM) que puede interoperar con el modo esparcido.

PIM Dense Mode (DM)

PIM DM no es un protocolo que haya sido ampliamente utilizado, debido a que el protocolo PIM SM ha demostrado ser el protocolo mas eficiente y empleado para el Multicast.

PIM Sparce Mode (SM)

PIM en modo disperso se ha reforzado durante años evolucionando de su forma experimental a su forma estándar actual. Ahora, el modo disperso es el protocolo de Multicast mas utilizado, emplea un árbol compartido, el cual permite acceder al árbol fuente, esta es una metodología eficiente, debido a que este previene el inundamiento de datos (DM), aunado con el menor gasto de recursos, a su vez, el envío de datos se lleva a cabo por el camino más óptimo. La creciente demanda de la aplicación del Multicast IP ha hecho necesario crear dos maneras de distribución del mismo PIM BI DIR y SSM.

Bi-directional PIM (PIM Bi-Dir)

PIM BI DIR crea un árbol bidireccional remitiendo información multipunto-multipunto haciendo una comunicación más eficaz y reduciendo el ancho de banda, un ejemplo palpable de este tipo de aplicaciones son las aplicaciones financieras de una sucursal a otra.

Source Specific Multicast (SSM)

SSM es una solución en la cual los usuarios pueden especificar la fuente del grupo al que pertenecen, de la cual desean recibir información. SSM es muy útil para las aplicaciones como Internet y para las comunicaciones corporativas.

6.2.2 Multicast vs. Unicast

El Multicast IP, al igual que el Unicast, es una parte del protocolo TCP/IP. Como primer punto de comparación, podemos mencionar que mientras el Unicast IP utiliza las clases A, B, y C, el Multicast IP usa la clase de direcciones D, además, los paquetes de Multicast IP son reproducidos por enrutadores dentro de la red, esto cuando existe más de una subred que requiere una copia de los datos enviados por la fuente.

Por su parte, el Unicast sobre IP hace a la fuente responsable de crear una cadena individual para cada receptor. El Multicast sobre IP es una solución mas robusta y escalable para la comunicación dentro de un grupo, debido a la replica distribuida de

datos y porque solamente una copia del paquete de datos se necesita para que sea enviada a varios usuarios. Por ejemplo, supongamos a un presidente de una compañía el cual necesita enviar una presentación a todos sus empleados. Con IP Multicast, el ancho de banda que utilizaría en un envío es igual al ancho de banda que se utilizaría para enviarles la presentación a todos sus empleados, mientras que con Unicast IP esto sería imposible, debido a que cada receptor tendría una secuencia de datos única. Las áreas de aplicaciones que se aprovechan del Multicast del IP incluyen, pero no se limitan a, las comunicaciones corporativas, el aprendizaje a distancia, y la distribución de software.

6.3 Problemática de implementación de Multicast sobre MPLS/VPN

Pese a que la solución para crear VPN's Unicast usando MPLS ha resultado exitosa y altamente escalable, esta tecnología no fue diseñada para soportar comunicaciones Multicast, dado que las etiquetas de MPLS sólo se asocian a destinos específicos en la red. Derivado de lo anterior, y de la necesidad de implementar Multicast sobre este tipo de VPN's, se han buscado varias alternativas que van desde el uso de la encapsulación de IP sobre IP (túneles) hasta el desarrollo de nuevas tecnologías, las cuales serán discutidas mas adelante.

6.4 Posibles soluciones de Implementación para Multicast sobre MPLS/VPN´s

6.4.1 Túneles CE-CE

La primera aproximación usada es la encapsulación de tráfico Multicast sobre túnelès únicast entre los CE´s que conforman una VPN. Aunque en principio parece una alternativa muy sencilla, esta no es escalable ni eficiente debido a que los túneles CE-CE eliminan los beneficios del Multicast sobre la red dorsal MPLS; además de que se requiere una configuración de túneles del tipo malla completa entre los equipos CE. RPF presenta problemas de operación al tener trayectorias no congruentes entre Multicast y Unicast por el uso de túneles. Por lo tanto, una mejor solución es requerida.

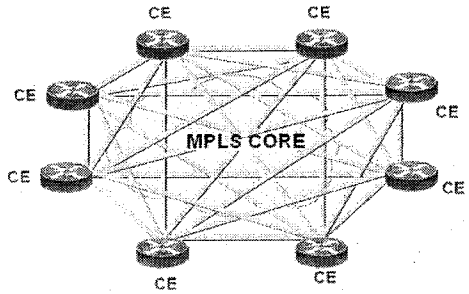
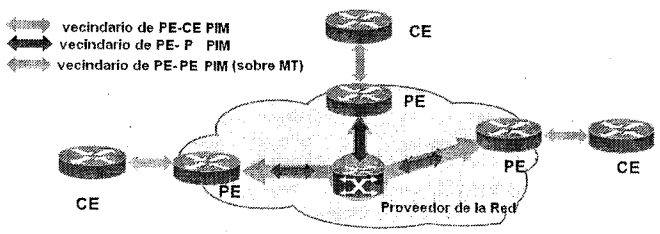


Figura 6.1 Estructura de los túneles CE-CE

6.4.2 Multicast Domains

Multicast Domains (MD) se refiere a un conjunto de VRF's que pueden enviar Multicast recíprocamente. Los Multicast VRF (a su vez nombrados MVRF) se refieren a un conjunto de VRF's que son capaces de soportar tablas de enrutamiento tanto de Unicast como de Multicast. El túnel de Multicast (MT) es utilizado para enviar paquetes de Multicast (C) a través de los enrutadores PE en un Dominio de Multicast que es común para estos enrutadores. Esto opera de la siguiente forma: un MVRF es asignado a un Dominio de Multicast, entonces por cada Dominio de Multicast es definido un grupo P de direcciones IP Multicast las cuales deberán de ser únicas e irrepetibles, los paquetes de información C son encapsulados en los enrutadores PE y son enviados en los túneles de Multicast MT como paquetes P a todos los enrutadores PE de su vecindario PE-PE. La dirección fuente del MT es la dirección BGP del PE directamente conectado al CE que introduce tráfico Multicast a la dorsal MPLS, y la dirección de destino es el grupo de direcciones P.



El tunel de Multicast se establece entre los enrutadores PE del Proveedor de la Red

Los enrutadores CE forman vecindarios PIM con instancias de VRF en enrutadores PE

Los enrutadores PE forman un vecindario PIM con otros enrutadores PE sobre el túnel de Multicast. A esto se le conoce como un vecindario específico de VRF

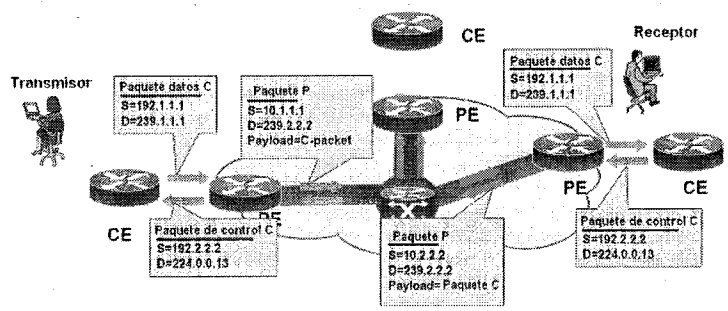
Los enrutadores PE forman vecindarios con los enrutadores P. Esto forma un vecindario Globalizado

Los paquetes de Multicast que provienen de los enrutadores CE serán enviados sobre túneles Multicast

Figura 6.2 Ejemplo de implementación de Multicast Domains

Las ventajas que se pueden obtener con esta solución es que la estabilidad en el centro de la red se mantiene, dicha estabilidad se logra para todos los estados de Multicast.

El estado óptimo en la base de la red para todos los elementos del Multicast dentro de una VPN se conservan. Otro punto a considerar es que el ISP (Proveedor de Servicios de Internet) tiene el control del envío de paquetes destino. Esto por un lado, por otro lado hay que mencionar que el tráfico que se forma por las réplicas de envío de paquetes es mayor y no se optimiza tanto, ya que los PE que no tienen receptores interesados aún recibirían todo el trafico Multicast por cada VPN.



El control del acceso de clientes y de el tráfico de datos son enviados sobre el túnel de Multicast

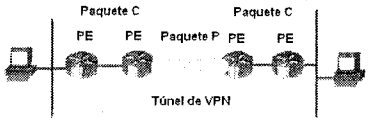
Los enrutadores P solamente ven paquetes P pero no pueden crear estado de tráfico dentro de la VPN

Los paquetes PE serán enviados a cada enrutador P que se encuentre dentro del dominio de Multicast

Figura 6.3 Ejemplo de Multicast Domains

Implementación de Multicast Domains

Esta solución requiere que el proveedor de ISP incluya el servicio de Multicast IP dentro de su red. En cada enrutador de frontera de red (PE), el proveedor crea una interfaz MTI (Multicast Túnel Interface) y un túnel VPN de Multicast en el envío (VRF) para cada cliente. El MTI encapsula los datos de Multicast de los clientes dentro de su propio paquete del Multicast para un grupo destino al cuál pertenecen todos los clientes para ese PE en particular.



Paquete P =234.10.10.10

Paquete C =225.1.1.1

Figura 6.4 Ejemplo de encapsulación MTI

6.4.3 VPN-IP PIM

Para este tipo de implementación surge la necesidad de modificar el mensaje de enrutamiento PIM con una ruta diferenciadora además de que se también se suma la técnica de RPF-hint. Otra característica adicional que requiere este tipo de implementación es la de la utilización de etiquetas para el envío de paquetes de Multicast. Un estado del Multicast en la dorsal se crea para cada estado del Multicast dentro de la VPN

Ruta diferenciadora (route distinquisher RD)

Las rutas hacia las fuentes dentro de una VPN son diferenciadas en el enrutador del PE por la ruta diferenciadora. El mensaje de PIM debe incluir el RD para permitir utilizar direcciones duplicadas.

(S,G) => (RD:S,G)

(*,G) => (RD:*,G)

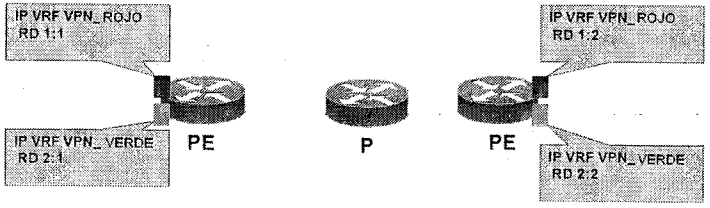


Figura 6.5 VPN-PIM Ruta diferenciadora

RPF-hint

Las rutas hacia las fuentes dentro de una VRF son conocidas vía el next-hop transportado en los mensajes MP-BGP. Este next-hop es accesible en todos los enrutadores P, y es insertado en el mensaje PIM para después llamar al proceso RPF-hint, el cual le indica a los enrutadores P que direcciones utilizar para la verificación RPF. En al siguiente figura se muestra como las dirección de next-hop correspondiente al PE1 es relacionada con la direciones IP de las fuentes R y G:

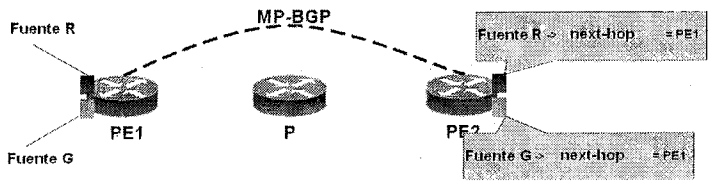


Figura 6.6 RPF indirecta

VPN-IP PIM requiere que los datos del Multicast de los clientes sean entregados a través de la red del proveedor de servicios.

Cada cliente VRF se registra en una tabla global. Esta solución requiere que la fuente del árbol del Multicast sea monitoreada y el VRF de ese árbol sea diferenciado usando un RD.

La fuente asociada con el RD "RD:S" hace la entrada de la ruta Multicast única para ese cliente. Mientras que el RD permite que el proveedor identifique únicamente los datos del Multicast, el paquete se debe encapsular con las etiquetas del Multicast de MPLS para remitir los datos en orden.

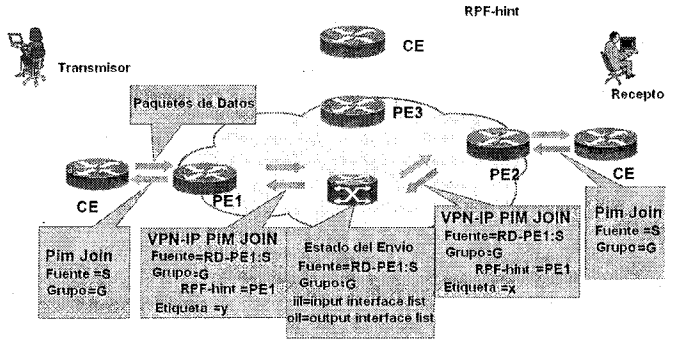
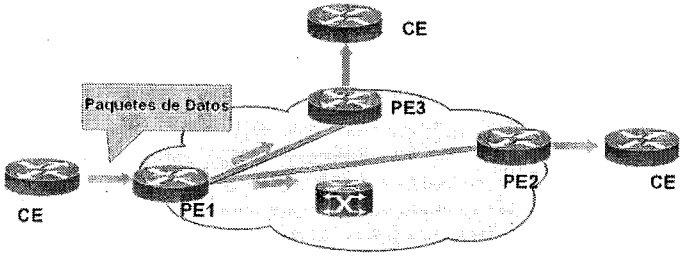


Figura 6.7 Ejemplo de VPN-PIM

Como resultados podemos indicar que el envío en la dorsal de la red es óptimo, aunque por otro lado se puede ver que en la dorsal de la red se encuentran todos los estados del Multicast presentes en cada VPN de la red. Por otra parte es necesario modificar PIM en todos los enrutadores P así como en los enrutadores PE. Lo anterior nos conduce a encontrar otra posible solución que nos simplifique la tarea de modificar los mensajes de PIM.

6.4.4 Multicast Domain (MD) Utlizando técnicas PIM NMBA (No Broadcast Multi-Access)

En esta solución los paquetes Multicast son tratados como paquetes Unicast. Una vez que un paquete Multicast llega a un PE, este es replicado para cada PE destino y conmutado después usando etiquetas unicast (una por cada PE destino). Esta solución es ventajosa en el sentido de que no se mantiene el estado de los grupos Multicast en la dorsal, sin embargo se tiene como desventaja un mayor tráfico en la misma y una replicación de paquetes en cada PE.



Enrutadores PE generan réplicas de los paquetes de datos

Etiquetas de Unicast son utilizadas (2)

Crea mucho tráfico en la red

UNICAST

MULTICAST

Figura 6.8 PIM NBMA

6.5 Diversas comparaciones de las aproximaciones para la implementación de Multicast sobre VPN'S

A continuación se muestran las comparaciones de ventajas y desventajas de las soluciones descritas anteriormente para la implementación de la red de Multicast sobre VPN con la técnica de MPLS.

6.5.1 Ventajas de los métodos

Multicast Domains

- La estabilidad de la dorsal de la red se proporciona controlando el número de estados de PIM.
- El Multicast puede ser utilizado con naturalidad en la dorsal de la red sin que se necesite la actualización de los enrutadores P

VPN-IP PIM

- El reenvío Multicast es utilizado en la dorsal de la red.
- No existen estados Multicast en la dorsal de la red si no existen estados Multicast en la VPN.
- Reenvío óptimo. El tráfico Multicast va únicamente a los enrutadores PE solicitantes.

VPN-IP PIM MD utilizando PIM NMBA

- No existen estados PIM en la dorsal de la red.

6.5.2 Desventajas de los métodos

Multicast Domains

- Se tiene un esquema subóptimo de reenvío de paquetes, dado que el tráfico generado por una fuente es reenviado a todos los enrutadores PE del dominio. Este problema se acentúa cuando se tienen fuentes con altas tasas de tráfico.

VPN-IP PIM

- La estabilidad de la red dorsal no puede asegurarse.
- No se puede utilizar el Multicast nativo, dado que se necesita el uso de nuevos mensajes PIM Multicast. Lo anterior implica una actualización de software de la dorsal de la red.

VPN-IP PIM MD utilizando PIM NMBA

- La réplica de los paquetes se hace en el enrutador PE, lo que puede resultar en tráfico innecesario en la dorsal de la red.

Dado que el método VPN-IP PIM no asegura la estabilidad de la red, éste es rápidamente descartado. Los dos métodos restantes, aseguran la estabilidad de la red, sin embargo ambos presentan deficiencias de reenvío de tráfico. Por un lado el método MD PIM NBMA presenta la desventaja de sobrecarga de tráfico en la dorsal de la red y por otro, Multicast Domains presenta la desventaja de reenvío subóptimo; la cual como desventaja tiene ventaja sobre la desventaja de MD PIM NBMA.

Así la mejor de las alternativas mostradas es el método de Multicast Domains. Finalmente, sería bueno que pudiéramos conseguir librarnos de la desventaja del método Multicast Domains y todavía mantener sus ventajas actuales.

Capítulo 7

ANALISIS PARTICULAR PARA LA IMPLEMENTACION DE MULTICAST SOBRE UNA VPN BASADA EN MPLS

Capitulo 7. Análisis particular para la implementación de Multicast sobre una VPN basada en MPLS

7.1 Diagrama general de solución a partir de las necesidades del cliente

En este capitulo se dará un ejemplo de la implementación de Multicast sobre una VPN basada en MPLS, tal como se planteo en los objetivos iniciales, se considerara una empresa dedicada a capacitación de personal en diversas regiones de la República Mexicana. Cabe mencionar que los estados de Guadalajara, Monterrey, y la Cd. de México de los cuales hacemos referencia en este proyecto, tienen a su cargo las Gerencias Regionales, (Bajío, Norte, y Región Centro) las cuales concentran el 90% de personal, además son puntos estratégicos de operación, refiriéndonos al alcance que pueden tener los estados.

Por ejemplo si un curso de capacitación se imparte desde la Cd. De México, con la nueva implementación que se llevara a cabo, los demás centros tendrán la oportunidad de tener alcance a nivel regional (ya sea en la región Norte o en la de Bajío) así, se elimina el problema de gastos excedentes (transporte, hospedaje) y tiempos de estadía utilizados en capacitaciones foráneas. El siguiente diagrama representa la infraestructura de red con la que cuenta actualmente la empresa, únicamente se realizaron configuraciones en los equipos de comunicaciones (switches y enrutadores) logrando la implementación de MVPN.

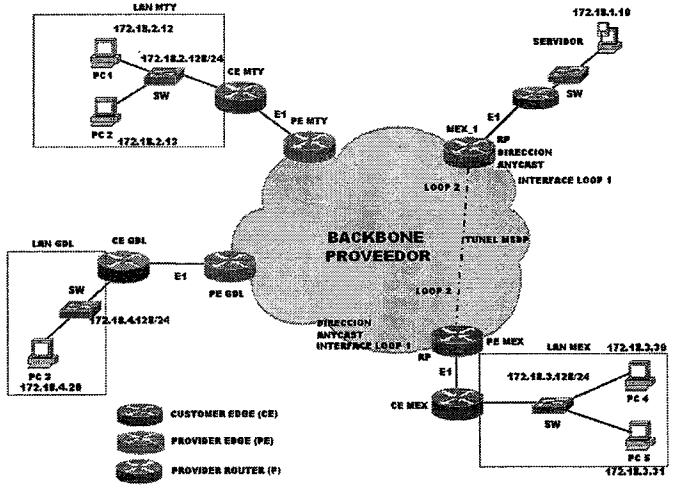


Figura 7.1 Diagrama General, Interconexión de Equipos.

La figura anterior muestra la arquitectura de red de la empresa (CE, Servidor y LAN en 3 puntos MEX, GDL, Y MTY); las direcciones IP utilizadas son meramente ilustrativas para la implementación. El Backbone pertenece al proveedor de servicios, así como los enrutadores de frontera PE_MTY, PE_GDL y PE_MEX,MEX_1 mientras que los enlaces en los puntos PE y CE corresponden a E1 (2048 kbps). Es importante mencionar que la empresa maneja las licencias de Win2000 y WinXP, en los equipos de las distintas localidades. También nos muestra la ubicación lógica de los puntos de reunión (RP) y la relación MSDP entre los mismos. Esta relación se realiza entre direcciones IP de interfaces Loopback en los PE's pertenecientes a la VPN y que no están ligadas al equipo en particular, con el fin de que los RP puedan cambiarse sin afectar la configuración.

Cabe hacer notar que los equipos que forman la red de datos son en su totalidad equipos de la marca Cisco, esto facilita el trabajo de configuración ya que al ser equipos homogéneos reduce el trabajo de configuración. En la tabla siguiente se muestran los equipos de comunicaciones que conforman la red de datos.

NOMBRE	MODELO	VERSION IOS
CE MTY	Cisco 3640	12.0
PE MTY	Cisco 7513	12.0(23)S6
CE GDL	Cisco 3640	12.0
PE GDL	Cisco 7513	12.0(23)S6
CE MEX	Cisco 3745	12.0
PE MEX	Cisco 7507	12.0(23)S6
MEX_1	Cisco 7507	12.0(23)S6
SWITCH(4)	Catalyst 1900	N/A
SWITCH	Cisco 5500	N/A

Tabla 7.1 Equipos que conforman la red de datos

7.2 Análisis de la situación y factibilidad de implementación de cada nodo

Después de haber analizado diferentes métodos de implementación de Multicast se determinó que Multicast Domains (MD) es el método mas factible, ya que nos permite aprovechar al máximo las características de IP Multicast y al mismo tiempo, obtener ventajas tanto de la VPN propiedad de la empresa como de la red del proveedor; de esta forma, se decidió aplicar el esquema llamado Multicast Domains Tunneling,

mediante el cual se encapsula el tráfico Multicast interno de la VPN en un conjunto de direcciones IP Multicast, a través del protocolo Source Specific Multicast (SSM).

7.3 Implementación de Multicast a nivel WAN entre Ps

Es importante hacer notar que para que funcione correctamente la solución planteada para Multicast VPN, es necesario que se tenga conectividad entre todos los sitios de la VPN que quieran comunicarse a través de Multicast, tal como se muestra en la figura 7.2. Para ello deben tenerse configurados previamente los equipos a través de MPLS VPN. Las configuraciones típicas de Multicast VPN se incluyen de manera informativa en el Anexo 1. Los cambios a efectuar sobre los equipos Ps (enrutadores MPLS del Backbone del proveedor) para soportar IP Multicast y sobre la VPN son mínimos. Los comandos se describen en el Anexo 1.

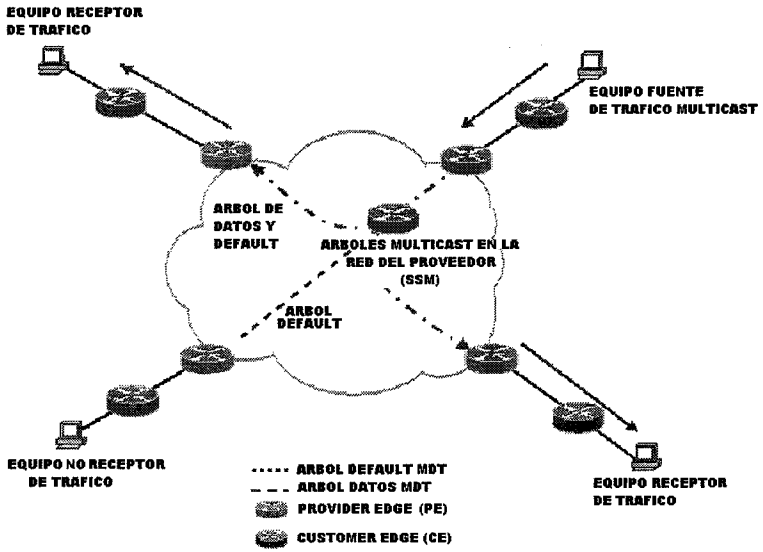


Figura 7.2 Árboles Multicast Generados en el Sistema Multicast Domains

7.4 Implementación de Multicast a nivel WAN entre PE's

El uso de SSM nos obliga a crear un árbol para cada fuente de tráfico Multicast (de ahí el nombre source specific), los cuales no necesariamente comparten entre sí una ruta específica dentro del proveedor. Se decide utilizar un árbol compartido (ST), con raíz en el punto de reunión (RP). Esta encapsulación permite asignar grupos específicos SSM por VPN, lo que es conveniente para llevar el orden necesario para el manejo eficiente del tráfico Multicast a través de la red del proveedor.

Para realizar la encapsulación se configura un árbol default formado por Túneles Multicast Dinámicos (MDT). Los túneles conforman una estructura lógica de red similar a la que se encuentra definida en la MPLS VPN. Estos túneles son asignados a la VRF perteneciente a la VPN en cada PE y son enrutados con base en Reverse Path Forwarding (RPF), que se basan en el protocolo de enrutamiento de la red del proveedor, como cualquier tráfico IP Multicast que curse fuera de una VPN.

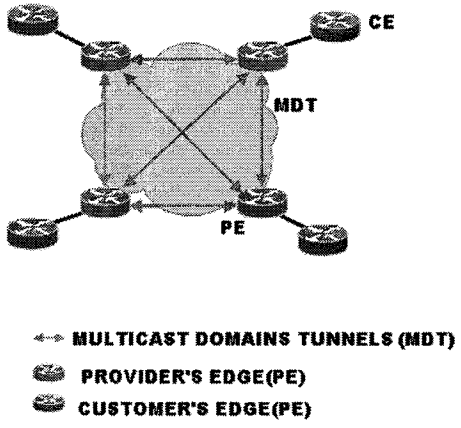


Figura 7.3 Túneles MDT entre equipos PE de la VPN

7.5 Implementación de Multicast a nivel LAN entre CE's

Debido a que en el ambiente LAN los paquetes Multicast son interpretados como paquetes Broadcast, se utilizó el esquema IGMP Snooping para evitar las storms provocadas por el proceso de flooding de los paquetes Multicast, que además suelen transportar aplicaciones con anchos de banda considerables, evitando que se queden puertos abiertos que no requieran el tráfico Multicast. En la VPN del cliente se cuenta actualmente con switches que soportan IGMP Snooping en Hardware, por lo que no se espera un incremento en el procesador a pesar de tener aplicaciones basadas en Multicast con altas tasas de transmisión de datos, audio y video (videoconferencias, presentaciones a distancia, por citar algunos ejemplos.)

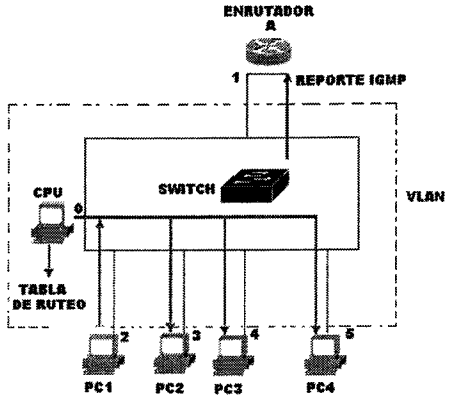


Figura 7.4 Multicast en el ambiente WAN

La figura anterior nos muestra como se realizan las peticiones al enrutador por medio del reporte IGMP.

1) La petición accesa a través del Switch
2) El switch identifica los mensajes de join y abre el puerto al tráfico de Multicast;
3) Si el switch identifica un mensaje de leave, cierra el puerto al trafico Multicast.

Esto nos evita replicas de trafico innecesario a puertos que no lo requieran y de esta forma evita interrupciones a los equipos que ya están conectados a los puertos.

7.6 Funcionamiento de la implementación en el esquema

Después de haber realizado las configuraciones en los equipos de comunicaciones y en general en la red de datos de la empresa, es necesario explicar cual será el uso que le dará el usuario final.

Para comprender de mejor forma se requiere ejemplificar como se realiza una videoconferencia dentro de la empresa. Para ello se requiere sin duda una aplicación que permita realizar conferencias y pláticas para brindar capacitación a distancia. Esto en principio de cuenta se logra accesando al sitio Web de la empresa, el servidor esta ejemplificado en la figura con un servidor Web. Es indispensable que los equipos cuenten con la aplicación instalada, en caso de que no se cuente con el programa, en el momento de obtener acceso al servicio (a través de una verificación de nombre de usuario y contraseña) se descargará automáticamente la aplicación, la cual se describe con más detalle en el Anexo 3. Para poder hacer uso cabal de la aplicación, se

requiere de cámaras de video, micrófono y bocinas (WEB CAM) en cada uno de los clientes. Luego de esto el método de distribución corresponderá a Multicast. El usuario de la aplicación que tome el papel del instructor debe realizar lo mismo señalado anteriormente, pero identificarse con su nombre de usuario y contraseña específicos para registrarse como tal. Una vez hecho lo anterior, el instructor tendrá el control en sus manos de la distribución del video.

Primeramente, el mismo instructor estará difundiendo la imagen y audio a todos los demás clientes, sin embargo, es capaz de permitir que otros usuarios envíen su video y sonido. El host que se encuentre difundiendo su video y audio se tendrá que registrar como fuente de tráfico Multicast al punto de reunión. Mientras tanto, los hosts que reciban la señal se registrarán entonces como destinos de tráfico Multicast con su default gateway. Tomando en cuenta la topología se identificó indistintamente a uno de los llamados "clientes" dentro del diagrama, como *Instructor*. Así, a veces se identificó como instructor a una PC de Mty, otras veces la de Gdl. y otras veces una de las de Méx., Esto con el fin de verificar que en cualquier punto de la red pudiera uno contar con las funcionalidades específicas del instructor.

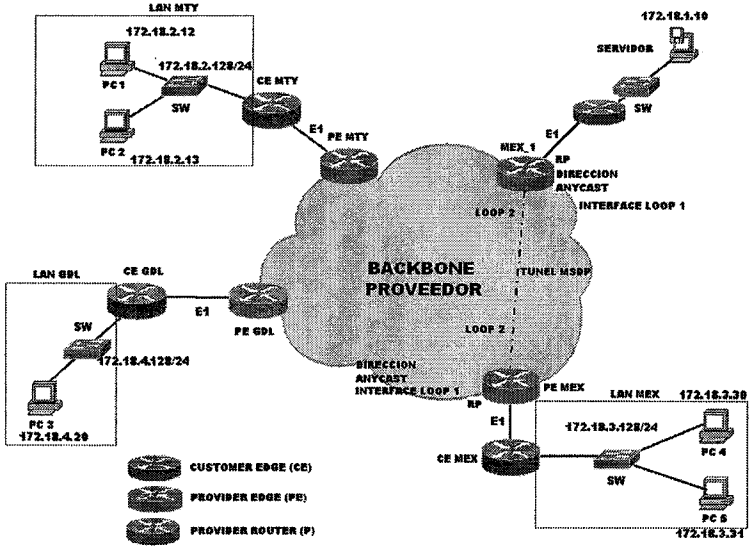


Figura 7.5 Diagrama de la red de datos

Mediante la implementación plasmada en este capítulo, se ha determinado que las configuraciones propuestas para soportar Multicast en la VPN del cliente son las adecuadas, de este modo podemos pasar a las conclusiones, donde tomaremos en cuenta algunos puntos de mejora, además de revisar el éxito de los objetivos propuestos inicialmente.

CONCLUSIONES

8 Conclusiones

En este trabajo se han estudiado diferentes tecnologías, tal es el caso de Multicast, VPN y MPLS. Después de haber analizado individualmente cada tecnología y de revisar diferentes escenarios, se lograron extraer las características más importantes de cada una para implementar la red que cubriera las necesidades de la empresa en cuestión, cumpliendo de esta manera con el objetivo principal de este proyecto el cual consistió en la optimización de gastos de una empresa dedicada a la capacitación a distancia sin necesidad de cambiar su infraestructura principal de la red de datos.

Después de haber analizado diferentes métodos de implementación de Multicast se determinó que Multicast Domains (MD) es el método mas viable y eficiente, ya que nos permitió aprovechar al máximo las características de IP Multicast en conjunto con la MPLS VPN de la empresa y del proveedor de servicios; estableciendo una base eficiente para soportar videoconferencias punto-multipunto desde un equipo emisor ubicado en cualquier punto de la red a varios equipos receptores.

Entre los beneficios que el cliente obtendrá de la implementación realizada se pueden enlistar las siguientes:

- La implementación de MVPN (Multicast MPLS VPN) en la red de la empresa que se encuentra en operación, se puede lograr con transparencia para el usuario final, esto quiere decir que físicamente los cambios no son perceptibles, ya que simplemente se realizan modificaciones necesarias a los equipos de comunicaciones. Cabe hacer la observación de que se necesita de una ventana de mantenimiento para la realización exitosa de la implementación.

- Se logro la disminución de costos de la empresa significativamente por conceptos de transportación y hospedajes, así como mejor aprovechamiento de los tiempos de los instructores, al no tener que desplazarse a diferentes partes de la Republica Mexicana.

  Haciendo referencia a la reducción de los gastos de la empresa, es necesario mencionar que la implementación a la red de datos implica costos, por lo que finalmente después de hacer un balance se determina que se logró cumplir con el objetivo planteado.

  Los puntos que se tomaron en cuenta para poder realizar este balance fueron:

  -Gastos relacionados directamente con la configuración de los equipos de comunicaciones, así como el tiempo que llevaría la implementación.
  -El aprovisionamiento del servicio por parte del proveedor.
  -La capacitación al personal de operación de la nueva tecnología dentro de la empresa.

  Los puntos anteriores se compararon contra los gastos que se originan anualmente por conceptos de:

-Hospedaje, alimentación y transporte de personal a diferentes partes de la República Mexicana.
-Viáticos y sueldos del personal que viaja al interior de la Republica,

Después de realizar este balance, se puede determinar que la reducción de los gastos de la empresa anualmente es significativa.

- No solamente para envío y recepción de de videoconferencias se obtuvieron logros significativos, también se logró la optimización del ancho de banda de la red de datos del cliente –lo que implica menores costos por concepto de crecimiento en la red-, manejo otras aplicaciones de red como lo son el acceso a Internet, el Chat, mensajero, por citar unos ejemplos de los beneficios que se obtienen con la implementación de las nuevas tecnologías.

De la implementación realizada se observó que existen puntos de mejora. Un ejemplo de ello, es que la red del proveedor cuenta con esquemas de redundancia en el punto de reunión (RP), mediante la técnica llamada Anycast. Esta técnica nos permite tener balanceo de carga y un esquema de redundancia rápido basado únicamente en la velocidad de convergencia del protocolo de ruteo interno de la red del proveedor. Al igual que en la red del proveedor, en la Red Privada Virtual se cuenta con un esquema de Anycast para brindar redundancia y balanceo de carga. Sin embargo, para el caso de los RP en la VPN, la convergencia en la caída de un RP es mucho más lenta ya que depende de las actualizaciones de BGP, que es el protocolo de ruteo que mantiene las tablas de la VPN internas. Se recomendaría que para este caso, las actualizaciones para Anycast se transportaran por un IGP (OSPF, IS-IS) para acelerar el tiempo de convergencia en el proveedor.

Finalmente de la instalación de Multicast VPN basado en MPLS se puede concluir lo siguiente:

- Es una opción muy viable de fácil instalación y configuración, que ofrece muchas ventajas para una empresa en desarrollo.

- Es una tecnología que permite aprovechar adecuadamente los recursos de la red (ancho de banda) y de procesamiento de CPU logrando una utilización eficiente de recursos.

- Es escalable, dado que la solución puede soportar sin problemas el crecimiento de aplicaciones que demanden el servicio de Multicast sin requerir cambio alguno. Lo único que habrá que cuidar es que el proceso de capacidad de red asegure el crecimiento oportuno de los enlaces para evitar condiciones de saturación.

- Ofrece reducción de gastos y optimización de los tiempos del personal de las empresas que la utilicen.

ANEXOS

A1. Configuraciones típicas para MPLS VPN.

Equipo	Configuración
Provider	ip cef <distributed> tag-switching tdp router-id Loopback666 interface tipo x/y tag-switching ip
Provider Ps	ip multicast-routing distributed int tipo tarjeta/puerto ip pim sparse-mode;. ip mroute-cache distributed;
Provider's Edge	ip cef distributed ip vrf ( ) rd 172.18.0.0:1 route-target export 172.18.0.0:1 route-target import 172.18.0.0:1 ! tag-switching tdp router-id Loopback111 ! interface Serial x/y ip vrf forwarding I( ) ! router bgp 666 no synchronization bgp log-neighbor-changes neighbor ( ) _RR peer-group neighbor ( )_RR remote-as 666 neighbor ( )_RR update-source Loopback666 neighbor 10.111.7.91 peer-group( ) _RR default-information originate no auto-summary ! address-family vpnv4

Provider's Edge	neighbor 172.18.x.x activate neighbor 172.18.x.x send-community both default-information originate no auto-summary exit-address-family ! address-family ipv4 vrf ( ) redistribute connected redistribute static no auto-summary no synchronization exit-address-family ! ip route vrf ( ) 172.18.x.x 255.255.255.0 Serialx/y

Route Reflector	ip cef router bgp 666 no synchronization bgp log-neighbor-changes neighbor ( ) _PE peer-group neighbor ( ) _PE remote-as 666 neighbor ( ) _PE update-source Loopback666 neighbor ( ) _PE route-reflector-client neighbor 172.18.x.1peer-group ( ) _PE neighbor 172.18.x.1description R1_DOC neighbor 172.18.x.2 peer-group ( )_PE neighbor 172.18.x.2 description R2_NDI neighbor 172.18.x.3 peer-group ( ) _PE neighbor 172.18.x.3 description R3_NDI neighbor 172.18.x.4 peer-group ( ) _PE neighbor 172.18.x.4 description ( ) _DOC no auto-summary ! address-family vpnv4 neighbor 172.18.x.1activate neighbor 172.18.x.1 route-reflector-client neighbor 172.18.x.1send-community extended neighbor 172.18.x.2 activate neighbor 172.18.x.2 route-reflector-client neighbor 172.18.x.2 send-community extended neighbor 172.18.x.3 activate neighbor 172.18.x.3 route-reflector-client neighbor 172.18.x.3 send-community extended neighbor 172.18.x.4 activate neighbor 172.18.x.4 route-reflector-client neighbor 172.18.x.4 send-community extended no auto-summary

Route Reflector	exit-address-family !

A2. Configuraciones de los Equipos de Comunicaciones

Para los equipos Ps (routers MPLS del backbone del proveedor):	ip multicast-routing distributed ! Lo siguiente se hace en todas las interfaces activas del equipo int *tipo tarjeta/puerto* ip pim sparse-mode ip mroute-cache distributed

Configuración de los puntos de reunión RP:	RP #sh run : : ! Define la dirección IP de Anycast Interface Loopback100 ip address 172.18.X.X 255.255.255.255 no ip directed-broadcast ip pim sparse-mode ! !Define que los datos viajen por árboles SPT y no por el árbol default compartido en la VPN ip pim spt-threshold 0 !Define al equipo como un punto de reunión mediante una dirección Anycast ip pim bsr-candidate Loopback100 1 ip pim rp-candidate Loopback100 group-list GRUPOS_MULTICAST !Define la relación de peer MSDP con el otro punto de reunión para permitir el balanceo de carga ip msdp peer 172.18.X.X connect-source Loopback1 ip msdp originator-id Loopback1 PE_GDL#sh run

Configuración de los puntos de reunión RP:	: : !Define la dirección IP de Anycast interface Loopback100 ip address 172.18.4.X 255.255.255.255 no ip directed-broadcast ip pim sparse-mode ! ! Define que los datos viajen por árboles *SPT* y no por el árbol *default* compartido en la VPN ip pim spt-threshold 0 ! Define al equipo como un punto de reunión mediante una dirección *Anycast* ip pim bsr-candidate Loopback100 1 ip pim rp-candidate Loopback100 group-list GRUPOS_MULTICAST ! Define la relación de peer MSDP con el otro punto de reunión para permitir el balanceo de carga ip msdp peer 172.18.X.X connect-source Loopback666 ip msdp originator-id Loopback666 ! !La siguiente lista de acceso define los grupos Multicast permitidos dentro de la red del proveedor ip access-list standard GRUPOS_MULTICAST permit 232.0.1.1 permit 232.0.2.0 0.0.0.255 ! : : end

Configuración de los equipos PE's:	! Dentro de la vrf se definen las direcciones a utilizar por los árboles *default* y de datos ip vrf mdt default 232.0.1.1 mdt data 232.0.2.0 0.0.0.255 threshold 1 ! ! Se activa multicast de forma global y dentro de la vrf ip multicast-routing distributed ip multicast-routing vrf ( )distributed ! Se habilita multicast en las interfaces hacia los routers P y los CE interface Serial*x/y/z* ip pim sparse-mode ip mroute-cache distributed ip pim ssm default

Configuracion de los puntos de reunión en los equipos PE_MEX y MEX_1:	PE_MEX #sh run Building configuration... : ! ! Se activa la interface que fungirá como dirección IP Anycast dentro de la VPN Interface Loopback ip vrf forwarding ip address 172.18.3.X 255.255.255.255 no ip directed-broadcast ip pim sparse-mode !

	! Se define la interface mediante la cual se intercambiarán los RPs la información sobre fuentes Multicast Interface Loopback999 ip vrf forwarding ip address 172.18.3.x 255.255.255.255 No ip directed-broadcast ip pim sparse-mode ! ! Se habilita como RP dentro de la VPN de ip pim vrf () bsr-candidate Loopback777 1 ip pim vrf () rp-candidate Loopback777 group-list GRUPOS_MULTICAST ! ! Se crea la relación con el otro RP para intercambiar fuentes Multicast ip msdp vrf () peer 172.18.3.X connect-source Loopback999 ip msdp vrf () originator-id Loopback999 ! End

Activación de la interfase que funge como direccion IP Anicast dentro de la VPN:	dc_MEX_1 #sh run Building configuration... : : ! ! Se activa la interface que fungirá como dirección IP Anycast dentro de la VPN () Interface Loopback777 ip vrf forwarding ip address 172.18.X.X 255.255.255.255 no ip directed-broadcast ip pim sparse-mode ! ! Se define la interface mediante la cual se intercambiarán los RP's la información sobre fuentes Multicast Interface Loopback999 ip vrf forwarding ip address 172.18.X.X 255.255.255.255 no ip directed-broadcast ip pim sparse-mode ! !Se habilita como RP dentro de la VPN () ip pim vrf () bsr-candidate Loopback777 1 ip pim vrf () rp-candidate Loopback777 group-list GRUPOS_MULTICAST ! ! Se crea la relación con el otro RP para intercambiar fuentes Multicast ip msdp vrf () peer 172.18.X.X connect-source Loopback999 ip msdp vrf () originator-id Loopback999 ! : : end

A3. Aplicación Para Videoconferencias.

El progreso en los medios de comunicación en los últimos años ha introducido nuevos procedimientos de trabajo en la empresa enfocados al ahorro de costos y un aumento de la efectividad. Sistemas multimedia como videoconferencia, permiten ofrecer nuevos e innovadores servicios a los clientes finales y compartir información dentro de la empresa. El resultado directo es una modernización que aumenta los ingresos por servicios y una disminución de los costos de operación (por ejemplo, en viajes). La videoconferencia ofrece una solución accesible a esta necesidad de comunicación con sistemas:

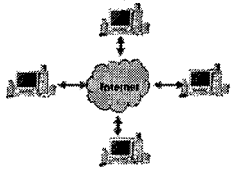
Tipos de equipos para videoconferencias:

- Equipo individual de escritorio.
- Equipos de salas.

• Punto a punto.

Videoconferencia punto a punto.

• Multipunto.



Videoconferencia Multipunto.

Características de la aplicación para videoconferencia:

- Debe interactuar por medio de audio y video entre diferentes usuarios al mismo tiempo.
- Debe ser multiplataforma.
- Debe ser una herramienta de fácil manejo para el usuario.

La finalidad es contar con un sistema de comunicación multimedia que permita la interacción visual, auditiva y verbal en tiempo real, que proporcione a las empresas, instituciones y universidades importantes beneficios en términos de ahorro, aumento de productividad e intercambio de ideas y conocimientos.

Si a ello agregamos el hecho que dicha solución sea implementada sobre una red IP y a través del Web, estamos frente a un servicio de videoconferencia IP, una alternativa accesible a todo tipo de empresas e instituciones.

Diagrama de casos de uso del sistema de videoconferencia

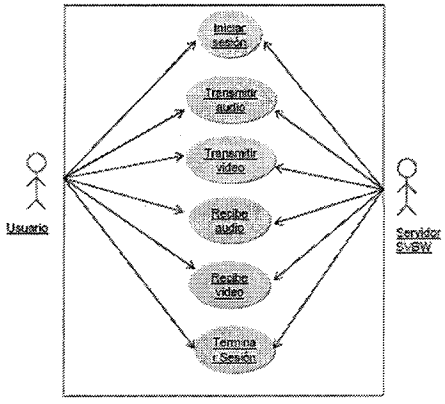
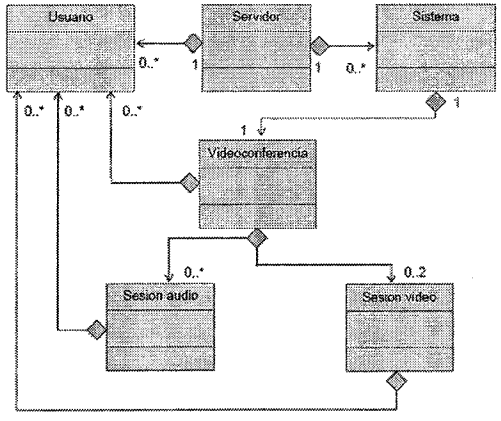


Diagrama de clases del sistema de videoconferencia.



Un diagrama de secuencia muestra una interacción ordenada según la secuencia temporal de eventos.

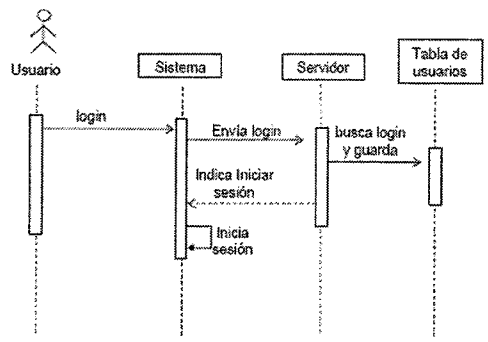
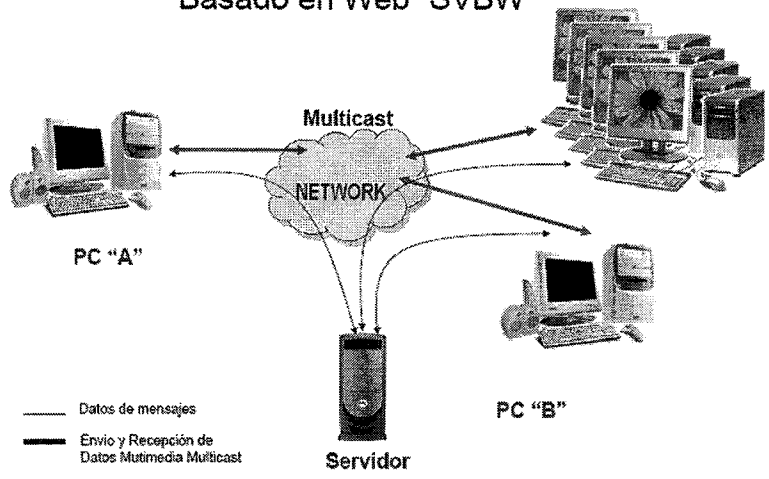


Diagrama de secuencia para iniciar una sesión

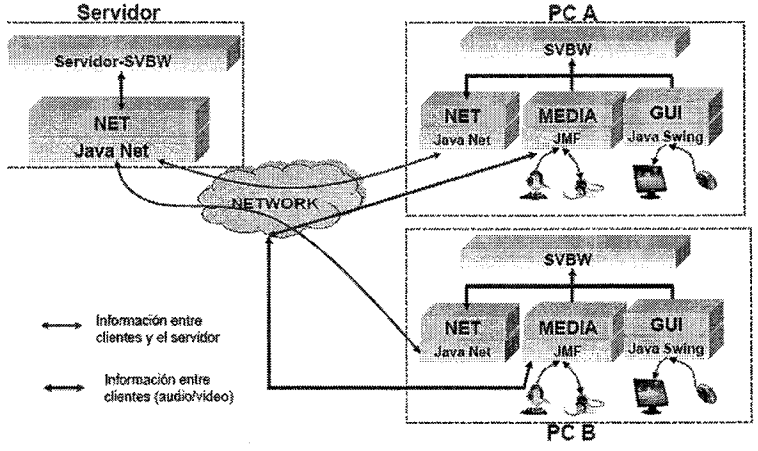
Requisitos necesarios para la interfaz del sistema Web Videoconferencia:

- Acceso a través del Web, por medio de navegadores.
- Visualiza video de dos o más usuarios al mismo tiempo.
- Manipula el envío e interrupción de video.
- Manipula el envío e interrupción de audio.
- Controla el volumen de la recepción de audio de los usuarios.

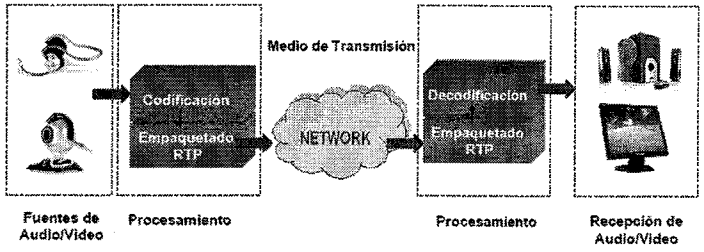
Esquema general Sistema De Videoconferencia Basado en Web "SVBW"



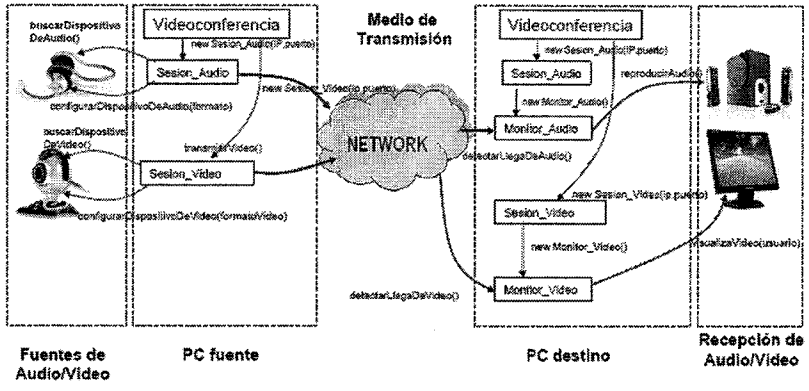
Esquema general de la implementación del Sistema de videoconferencia basado en Web (SVBW)



Esquema de transmisión y recepción de datos multimedia de un Sistema de videoconferencia.

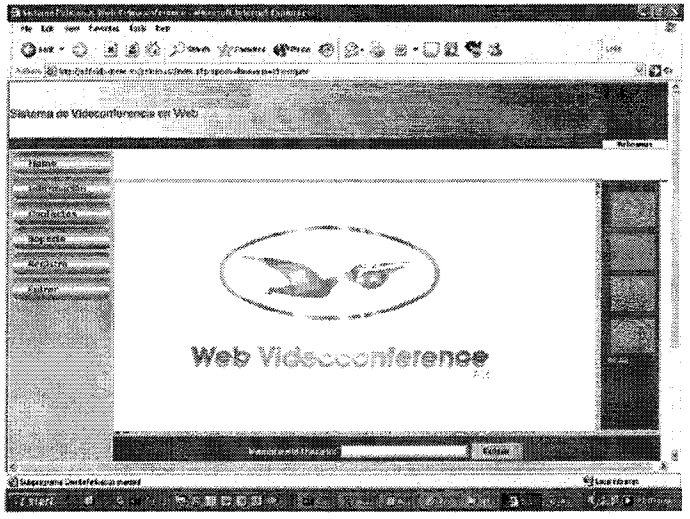


Esquema de transmisión y recepción de datos multimedia del Sistema de videoconferencia basado en Web (SVBW)

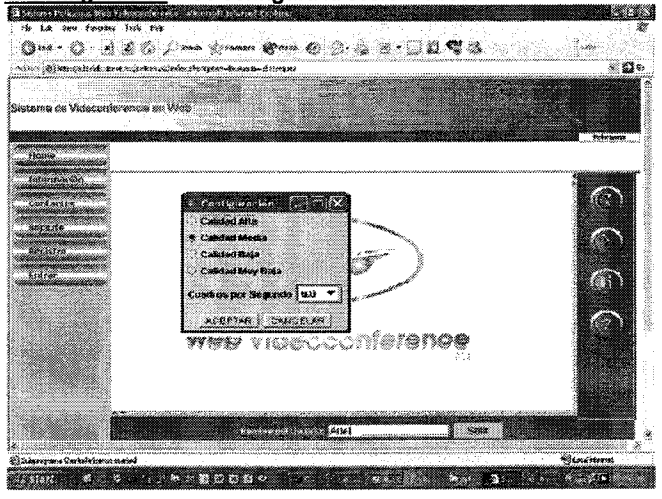


Guía de acceso a la videoconferencia para el usuario final.

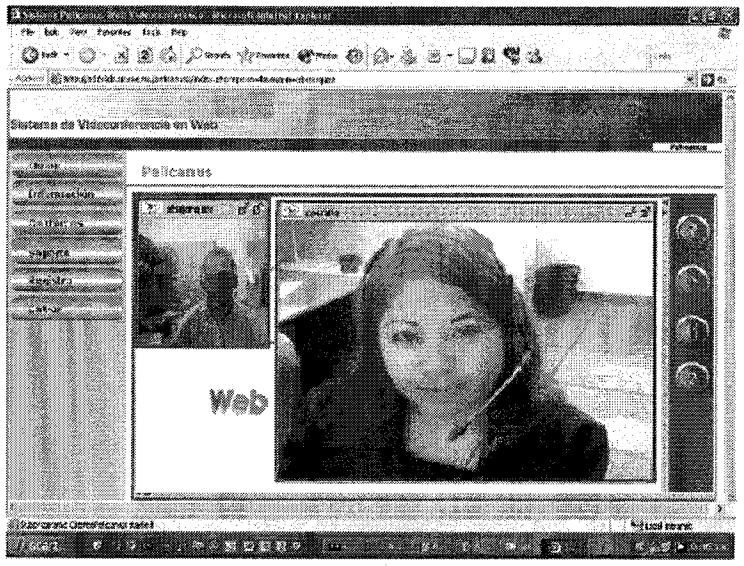
1. Validación ***Se solicita nombre de usuario y contraseña***



2. Configuración ***Se configura la sesión desde la PC remota***



3. Acceso ***Se valida usuario y contraseña permitiendo el acceso a la videoconferencia.***



- Es visible que los sistemas de videoconferencia son una tecnología importante de la actualidad.
- Es importante saber seleccionar los codec's tanto para audio como para video.
- El rendimiento de la aplicación depende del hardware (velocidad de CPU, memoria RAM y tarjeta de video) así como del tráfico de la red de datos.

A4. Glosario

As: Autonomous System; Sistema Autónomo

ANSI: Instituto Nacional Americano de Normalización

APPN: Internetwork avanzada de par a par

ARP: Protocolo de Resolución de Direcciones.

ASCII: Código americano normalizado para el intercambio de la información

Backbone: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

BGP: Border Gateway Protocol Protocolo de enrutador fronterizo

Binario: Sistema numérico compuesto por ceros y unos

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno.

Broadcast: Paquete de datos enviado a todos los nodos de una red.

Buffer: Memoria intermedia que se utiliza como memoria de datos temporal durante una sesión de trabajo.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits)

CHAP: Protocolo de autenticación de intercambio de señales

CBT: Cored Based Tree; Árbol basado en un núcleo

CIDR: Enrutamiento sin clase entre dominios

CIR: Velocidad de información suscrita Velocidad en bits por segundo.

CGMP: Cisco Group Management Protocol; Protocolo de Gestión de Grupos Cisco

CSMA/CD: Carrier Sense multiple Access/Collision Detection; Acceso Múltiple con Detección de Portadora y Detección de Colisiones

DARPA: Defense Advance Research Proyects Agency; Agencia de Proyectos de Investigación Avanzada para la Defensa

DCE: Data Communications Equipment; Equipo de transmisión de datos

DECNET: Digital Equipment Corporation Networking; Grupo de Productos de Comunicaciones

DHCP: Dynamic Host Configuration Protocol; Protocolo de configuración dinámica del Host.

DNS: Domain Name Service; Sistema de Denominación de Dominio.

DSL: Digital Subscriber Line; Línea Digital del Suscriptor

DTE: Data Terminal Equipment; Equipo Terminal de Datos

E1: Líneas dedicadas para el uso privado con velocidad de 2,048 Mbps.

Ethernet: El método de conexión más común en las redes de área local. Las estaciones del segmento comparten el ancho de banda total, que es 10 (Mbps), 100 Mbps o 1000 Mbps

FDDI: Fiber Distributed Data Interface; Interfaz de datos distribuida por fibra

Flooding: Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

Gateway: Se refiere a un dispositivo de enrutamiento, realiza conversión de capa de aplicación de la información de una pila de protocolo a otro

HDLC: Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación

HDLC: High Level Data Link control; Control de Enlace de Datos de Alto Nivel

Hexadecimal: base 16; representación numérica que usa los dígitos del 0 al 9, con su significado habitual, y las letras de la A a la F, para representar dígitos hexadecimales con valores del 10 al 15.

Host: Computadora en una red

HTML: Lenguaje de Etiquetas por Hipertexto. Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización.

HTTP: Protocolo de Transferencia de Hipertexto, utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

IANA: Internet Assigned numbers Authority; Agencia de Asignación de Números Internet

ICMP: Protocolo de mensajes de control en Internet ; informa errores y brinda información relativa al procesamiento de paquetes IP

IEEE: Institute of Electrical and Electrónics Engineers; Instituto de Ingeniería Eléctrica y Electrónica

IGRP: Interior Gateway Routing Protocol; Protocolo de enrutamiento de gateway interior Protocolo desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en redes heterogéneas de gran envergadura.

Internet: Abreviatura de internetwork de redes.

IP: Internet Protocol; Protocolo de Internet

IS-IS: Sistema Intermedio a Sistema Intermedio.

ISO: Organización Internacional para la Normalización

KBPS: Kilobits por segundo; Medida de velocidad de transferencia.

LAN: Local Area Network; Red de Area Local

LCP: Protocolo de Control de Enlace; proporciona un método para establecer, configurar, mantener y terminar una conexión punto a punto.

LSA: Publicación del estado de enlace; a veces se denomina paquete de estado de enlace (LSP).

LSP: Label Switched Path; Camino entre dos enrutadores usando etiquetas MPLS.

LSR: Label Switching Router; Enrutador con capacidad para MPLS

MAC: Media Access Control; Control de Acceso al Medio

MAU: Médium Access Unit; Unidad de Conexión al Medio

MBONE: Multicast Backbone; columna vertebral de la red Multicast en Internet

MPLS: Multiprotocol Label Switching; Switcheo de etiquetas Multiprotocolo

MOSPF: Multicast Open Shortest Path first; Protocolo de intra-Dominio de Enrutamiento Multicast

Multicast: Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino.

NAT: Network Address Translation; Traducción de Direcciones de Red

NIC: Network Interface Card; Tarjeta de Interfaz de Red

OSI: Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de redes de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

OSPF: Open Shortest Path First; Algoritmo abierto de primero la trayectoria mas corta basado en el estado enlaces.

PIM: Protocol Independent Multicast; Protocolo Independiente Multicast

PIM-DM: Protocol independent Multicast Dense-Mode

PIM-SM: Protocol Independent Multicast Sparse-Mode

PPP: Point to Point Protocol; Protocolo Punto a Punto

PVC: Permanent Virtual Circuit; Circuito Virtual Permanente

RDSI: Red digital de servicios integrados

RIP: Routing Information Protocol; Protocolo de información de enrutamiento

RP: Rendezvous Point; Punto de Reunión

RPF: Reverse Path Forwarding; Ruta de Reenvío de Regreso de Multicast

RTP: Real Time Protocol; Protocolo de Transporte en Tiempo Real.

SNMP: Protocolo Simple de Administración de Redes

SVC: Circuito Virtual Conmutado

Switch: Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

SPT: Shorthest Path Tree; Árbol de la Ruta Mas Corta

TCP/IP: Protocolo de Control de Transmisión /Protocolo Internet

TTL: Time to Live; Tiempo de Existencia

Unicast: Mensaje que se envía a un solo destino de red.

VLAN: LAN Virtual; Grupo de dispositivos de una LAN que están configurados (usando el software de administración) de tal modo que se pueden comunicar como si estuvieran conectados al mismo cable, cuando, en realidad, están ubicados en una serie de segmentos de LAN distintos.

VPN: Red Privada Virtual, o Virtual Private Network, permite establecer una conexión segura a través de una red pública, o Internet.

WAN: Wide Área Network; Red de Comunicación Extendida.

Bibliografía

"LDP Specification", Internet Draft, ANDERSSON L.
Et al, Junio 1999

"Introduction, Basics and Traffic engineering", Gabriele Schrenk.
EANTC AG, November 2001.

"MPLS and VPN Arquitectures", Jim guichard, Ivan Pepelnjak.
CISCO PRESS, 2001

"Multiprotocol Label Switching Architecture", ROSEN E.C., VISWANATHAN A., CALLON R., Agosto 1999

Referencias Electrónicas

"Multicast for MPLS/BGP VPN's"
http://www.cisco.com/mvpn.pdf

http://www.juniper.net/techcenter/techpapers/mpls/mpls.html, marzo 1999

SEMERIA C., "Traffic Engineering for the New Public Network", Juniper Networks Inc., Enero 1999, http://www.juniper.net/techcenter/techpapers// TE_NPN.html

SEMERIA C.,Stewart III J.W., "Optimizing Routing Software for Reliable Internet Growth", JuniperNetworksInc. , julio1999,
http://www.juniper.net/techcenter/techpapers/optimizing-routing-sw.fm.html
http://www.ietf.org/html.charters/mpls-charter.html

REDFORD R., "Enabling Business IP Services with Multiprotocol Label SWitching", Cisco Systems, Inc.
http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.html

"Intranet and Extranet Virtual Private Networking", Cisco Systems, Inc., Technical Service Description,
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/ievpn_rg.html

"Delivering New World Virtual Private Networks with MPLS", Cisco Systems, Inc.,
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.html