UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSGRADO

ANALISIS DE PROTOCOLOS Y POLITICAS DE ENRUTAMIENTO PARA EL PROVEEDOR DE SERVICIOS DE INTERNET

PRESENTA

Ing. Aldemar Gerardo Suárez Morales

TESIS

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERIA CON ESPECIALIDAD EN TELECOMUNICACIONES

SAN NICOLAS DE LOS GARZA N.L. DICIEMBRE DE 2007

UNIVERSIDAD AUTONOMA DE NUEVO LEON

FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

DIVISION DE ESTUDIOS DE POSGRADO

ANALISIS DE PROTOCOLOS Y POLITICAS DE ENRUTAMIENTO PARA EL PROVEEDOR DE SERVICIOS DE INTERNET

PRESENTA

Ing. Aldemar Gerardo Suárez Morales

TESIS

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS DE LA INGENIERIA CON ESPECIALIDAD EN TELECOMUNICACIONES

SAN NICOLAS DE LOS GARZA N.L. DICIEMBRE DE 2007

Universidad Autónoma de Nuevo León
Facultad de Ingeniería Mecánica y Eléctrica
División de Estudios de Posgrado

Los miembros del Comité de Tesis recomendamos que la Tesis **"Análisis de Protocolos y Políticas de Enrutamiento para el Proveedor de Servicios de Internet"** realizada por el alumno: **Aldemar Gerardo Suárez Morales** con número de matrícula: **1130069** sea aceptada para su defensa como opción al grado de Maestro en Ciencias de la Ingeniería con especialidad en Telecomunicaciones

El Comité de Tesis

_____
M.C. Leopoldo R. Villarreal Jiménez.
Asesor

_____
M.C. Catarino Alor Aguilar
Revisor

_____
M.C. José D. Rivera Martínez.
Revisor

Vo. Bo.

_____
Dr. Guadalupe Alan Castillo Rodríguez
Subdirector de Posgrado
División de Estudios de Posgrado

Ciudad Universitaria a 7 de Diciembre del 2007

DEDICATORIA

Este proyecto esta dedicado a todos quienes a lo largo de mi vida tanto académica como profesional han estado conmigo apoyándome en las metas que me he propuesto.

AGRADECIMIENTOS

Quiero agradecer a todas las personas que estuvieron y fueron parte de la realización de este proyecto, catedráticos, amigos y compañeros de trabajo, esto también es de ustedes… Gracias.

PROLOGO

En los últimos años el Internet ha crecido de manera impresionante, se han desarrollado muchas tecnologías y los servicios son cada vez mas demandantes, Internet en la actualidad juega un papel muy importante en la vida cotidiana y económica de las personas, y muchas empresas dependen de estar conectados a Internet para realizar sus operaciones.

La necesidad de estar conectado a Internet es cada vez mas grande, por ello el escoger quien va a brindar el Servicio de Internet es esencial, ya que es la seguridad que va a tener el usuario final de que sus actividades no se verán interrumpidas y se realizaran en tiempo y forma de una manera eficiente.

Para que un proveedor de Internet puede brindar un servicio de calidad debe de evaluar muchos puntos, uno de ellos y posiblemente sea el más importante es como va a enviar y recibir la información de sus clientes hacia Internet, es decir que protocolo de enrutamiento va a utilizar en su red, por lo anterior es necesario para el Proveedor de Servicios de Internet obtener la suficiente información, en este caso de los protocolos de enrutamiento que existen, incluyendo sus características, ventajas y limitaciones para poder tomar la mejor decisión de cómo va a enrutar el tráfico a Internet.

INDICE

PROLOGO **1**
CAPITULO 1 ..... ¡Error! Marcador no definido.
INTRODUCCION ..... ¡Error! Marcador no definido.
1.1 Descripción del problema. ..... **¡Error! Marcador no definido.**
1.2 Objetivo de la Tesis. ..... **¡Error! Marcador no definido.**
1.3 Propuesta. ..... **¡Error! Marcador no definido.**
1.4 Límites del estudio. ..... **¡Error! Marcador no definido.**
1.5 Justificación del estudio. ..... **¡Error! Marcador no definido.**
1.6 Metodología. ..... **¡Error! Marcador no definido.**
CAPITULO 2 ..... ¡Error! Marcador no definido.
CARACTERISTICAS Y SERVICIOS DE UN *ISP* ..... ¡Error! Marcador no definido.
2.1 Servicios de los ISPs. ..... **¡Error! Marcador no definido.**
2.2. Precio del Servicio de los *ISPs.* ..... **¡Error! Marcador no definido.**
2.3 Acuerdos a nivel de Servicio. ..... **¡Error! Marcador no definido.**
2.4 Criterios de selección del *backbone* del *ISP*. ..... **¡Error! Marcador no definido.**
2.5 Conexiones físicas. ..... **¡Error! Marcador no definido.**
2.6 Cuellos de botella potenciales de los *ISPs* y tasa de suscripción. ..... **¡Error! Marcador no definido.**
2.7 Nivel de redundancia del acceso a Internet de un *ISP*. ..... **¡Error! Marcador no definido.**
2.8 Distancia a los destinos. ..... **¡Error! Marcador no definido.**
2.9 Acuerdos de intercambio de tráfico. ..... **¡Error! Marcador no definido.**
2.10 Punto de demarcación. ..... **¡Error! Marcador no definido.**
2.11 Colocación del router. ..... **¡Error! Marcador no definido.**
CAPITULO 3 ..... ¡Error! Marcador no definido.
DIRECCIONAMIENTO IP EN INTERNET ..... ¡Error! Marcador no definido.
3.1 Arquitectura de direcciones en Internet. ..... **¡Error! Marcador no definido.**
3.2 Direccionamiento IP básico ..... **¡Error! Marcador no definido.**
3.2.1 Direccionamiento de Clase A ..... **¡Error! Marcador no definido.**
3.2.2 Direccionamiento de Clase B ..... **¡Error! Marcador no definido.**
3.2.3 Direccionamiento de Clase C ..... **¡Error! Marcador no definido.**
3.2.4 Direccionamiento de Clase D ..... **¡Error! Marcador no definido.**
3.2.5 Direccionamiento de Clase E ..... **¡Error! Marcador no definido.**
3.2.6. Direcciones IP Privadas. ..... **¡Error! Marcador no definido.**
3.3 Extensiones para IP ..... **¡Error! Marcador no definido.**
3.3.1 Máscaras de subred (*Subnetting*) ..... **¡Error! Marcador no definido.**
3.3.2 VLSM ..... **¡Error! Marcador no definido.**
3.3.3 Enrutamiento entre dominios sin Clase CIDR ..... **¡Error! Marcador no definido.**
3.3.4 NAT ..... **¡Error! Marcador no definido.**
CAPITULO 4 ..... ¡Error! Marcador no definido.
PRINCIPIOS DE ENRUTAMIENTO ..... ¡Error! Marcador no definido.
4.1 Definición del enrutamiento ..... **¡Error! Marcador no definido.**
4.2 Requisitos del enrutamiento ..... **¡Error! Marcador no definido.**
4.3 Funciones de un *router* ..... **¡Error! Marcador no definido.**
4.3.1 Interconectividad física ..... **¡Error! Marcador no definido.**
4.3.2 Interconectividad lógica ..... **¡Error! Marcador no definido.**
4.3.3 Cálculo y mantenimiento de rutas ..... **¡Error! Marcador no definido.**
4.3.4 Seguridad ..... **¡Error! Marcador no definido.**

4.4 Funciones del *router* en las WAN..... **¡Error! Marcador no definido.**
4.5 Escenarios de *Internetworking*..... **¡Error! Marcador no definido.**
4.5.1 Enrutamiento dentro de una red ..... **¡Error! Marcador no definido.**
4.5.2 Enrutamiento entre redes adyacentes ..... **¡Error! Marcador no definido.**
4.5.3 Enrutamiento entre redes no adyacentes ..... **¡Error! Marcador no definido.**
4.6 Criterios de rendimiento de una WAN ..... **¡Error! Marcador no definido.**
4.7 Información sobre enrutamiento ..... **¡Error! Marcador no definido.**
4.7.1 Distancia administrativa. ..... **¡Error! Marcador no definido.**
4.7.2 Métrica de enrutamiento. ..... **¡Error! Marcador no definido.**
4.8 Tipos de Enrutamiento. ..... **¡Error! Marcador no definido.**
4.8.1 Dos Tipos de protocolos de enrutamiento dinámico. ... **¡Error! Marcador no definido.**
4.8.2 Enrutamiento Estático. ..... **¡Error! Marcador no definido.**
4.8.3 Enrutamiento por vector distancia..... **¡Error! Marcador no definido.**
4.8.4 Enrutamiento por estado del enlace..... **¡Error! Marcador no definido.**
4.8.5 Enrutamiento Híbrido..... **¡Error! Marcador no definido.**
4.9 Convergencia ..... **¡Error! Marcador no definido.**
4.10 Cálculo de rutas..... **¡Error! Marcador no definido.**
4.11 Almacenamiento de múltiples rutas..... **¡Error! Marcador no definido.**
4.12 Inicio de las actualizaciones..... **¡Error! Marcador no definido.**
4.13 Métricas de enrutamiento..... **¡Error! Marcador no definido.**
CAPITULO 5 .....¡Error! Marcador no definido.
PROTOCOLOS DE ENRUTAMIENTO .....¡Error! Marcador no definido.
5.1.1 Actualización de Rutas de RIP ..... **¡Error! Marcador no definido.**
5.1.2 Métrica de Enrutamiento de RIP ..... **¡Error! Marcador no definido.**
5.1.3 Funcionalidades de Estabilidad de RIP ..... **¡Error! Marcador no definido.**
5.1.4 Temporizadores de RIP ..... **¡Error! Marcador no definido.**
5.2 RIP versión 2..... **¡Error! Marcador no definido.**
5.3 Protocolo de Información de *Gateway* Interior IGRP..... **¡Error! Marcador no definido.**
5.3.1 Métricas IGRP..... **¡Error! Marcador no definido.**
5.3.2 Uso de las métricas IGRP..... **¡Error! Marcador no definido.**
5.3.3 Mecanismos de IGRP..... **¡Error! Marcador no definido.**
5.3.4 Enrutamiento Multirruta..... **¡Error! Marcador no definido.**
5.3.5 Dominio de Proceso ..... **¡Error! Marcador no definido.**
5.4 Protocolo de Enrutamiento de *Gateway* Mejorado EIGRP.... **¡Error! Marcador no definido.**
5.4.1 Nuevas características de EIGRP ..... **¡Error! Marcador no definido.**
5.4.2 Estructuras de datos de EIGRP..... **¡Error! Marcador no definido.**
5.4.3 Tablas EIGRP..... **¡Error! Marcador no definido.**
5.4.4 Tipos de paquete EIGRP ..... **¡Error! Marcador no definido.**
5.5 Protocolo OSPF ..... **¡Error! Marcador no definido.**
5.5.1 Areas OSPF ..... **¡Error! Marcador no definido.**
5.5.2 Tipos de *routers* OSPF ..... **¡Error! Marcador no definido.**
5.5.3 Metrica OSPF..... **¡Error! Marcador no definido.**
5.5.4 Tipos de enrutamiento OSPF..... **¡Error! Marcador no definido.**
5.5.5 Enrutamiento entre redes..... **¡Error! Marcador no definido.**
5.5.6 Actualizaciones de enrutamiento..... **¡Error! Marcador no definido.**
5.5.7 Tipos de Paquete OSPF ..... **¡Error! Marcador no definido.**
5.5.8 Relaciones de vecindad OSPF..... **¡Error! Marcador no definido.**
5.5.9 Tipos de Red OSPF ..... **¡Error! Marcador no definido.**
5.5.10 Sumarización OSPF..... **¡Error! Marcador no definido.**
5.6 *Intermediate System-to-Intermediate System (IS-IS)* ..... **¡Error! Marcador no definido.**
5.6.1 Características de IS-IS: ..... **¡Error! Marcador no definido.**

5.6.2 Tipos de *Routers* IS-IS ..... **¡Error! Marcador no definido.**
5.6.3 Ennnrutamiento IS-IS Integrado o DUAL..... **¡Error! Marcador no definido.**
5.6.4 Estructura de Direcciones NSAP..... **¡Error! Marcador no definido.**
5.7 Protocolo de *Gateway* Fronterizo BGP..... **¡Error! Marcador no definido.**
5.7.1 Como trabaja BGP..... **¡Error! Marcador no definido.**
5.7.2 Características de BGP ..... **¡Error! Marcador no definido.**
5.7.3 Bases de Datos de BGP ..... **¡Error! Marcador no definido.**
5.7.4 Mensajes BGP ..... **¡Error! Marcador no definido.**
5.7.5 Selección de ruta BGP..... **¡Error! Marcador no definido.**
5.7.6 Atributos BGP ..... **¡Error! Marcador no definido.**
5.7.7 Criterios para selección de ruta en BGP..... **¡Error! Marcador no definido.**
5.7.8 Autenticación BGP..... **¡Error! Marcador no definido.**
5.7.9 Multihomming..... **¡Error! Marcador no definido.**
CAPITULO 6 .....¡Error! Marcador no definido.
POLITICAS DE ENRUTAMIENTO.....¡Error! Marcador no definido.
6.1 Usando Múltiples Protocolos de enrutamiento ..... **¡Error! Marcador no definido.**
6.2 Configurar Redistribución de rutas..... **¡Error! Marcador no definido.**
6.3 Interfaces Pasivas (*passive-interface*)..... **¡Error! Marcador no definido.**
6.4 Rutas predeterminadas o rutas estáticas..... **¡Error! Marcador no definido.**
6.5 Listas de distribución (*Distribute lists*)..... **¡Error! Marcador no definido.**
6.6 Mapas de Ruta (*route-maps*)..... **¡Error! Marcador no definido.**
6.7 Cambiar la distancia administrativa..... **¡Error! Marcador no definido.**
CAPITULO 7 .....¡Error! Marcador no definido.
CONCLUSIONES.....¡Error! Marcador no definido.
BIBLIOGRAFIA.....¡Error! Marcador no definido.
LISTADO DE FIGURAS .....¡Error! Marcador no definido.
LISTADO DE TABLAS .....¡Error! Marcador no definido.
GLOSARIO.....¡Error! Marcador no definido.
RESUMEN AUTOBIOGRAFICO.....¡Error! Marcador no definido.

CAPITULO 1

INTRODUCCION

1.1 Descripción del problema.

Actualmente en el mundo de las Telecomunicaciones, Internet se ha convertido en una de los Servicios más importantes debido a las múltiples actividades que se pueden realizar en la red, razón por la que en una empresa ya se ha convertido en un servicio indispensable el tener acceso a la información así también como para el usuario Doméstico, por lo tanto para obtener los mejores beneficios que el Internet puede ofrecer, es necesario escoger quien brindará ese servicio o la conectividad a nivel IP. Es ahí donde el Proveedor de Servicios de Internet ó por sus siglas en Inglés *ISP (Internet Service Provider*) que es como se le conoce comúnmente en el mundo de las telecomunicaciones es quien juega el papel más importante, porque dependiendo de que tan eficiente y seguro sea el Proveedor, es la garantía de que la empresa ó cliente que adquirió sus servicios podrá aprovecharlos al máximo y sabrá explotarlos de acuerdo a sus necesidades.

Uno de los aspectos más importantes que definen el éxito y óptimo funcionamiento de un *ISP* en el mercado es la forma en la que va a enrutar el tráfico en su red, es decir la manera en que fluirá la información ya sea proveniente del cliente hasta su destino final o viceversa, es decir que Protocolos y Políticas de enrutamiento manejará en su red.

Existen diversos protocolos de enrutamiento IP, los cuales se pueden clasificar en Internos o Externos, estos protocolos son los que un *ISP* deberá saber elegir, para aplicarlos en su red y así poder ofrecer un mejor Servicio, tanto hacia sus mismos *Carriers* ó Proveedores como al cliente final.

1.2 Objetivo de la Tesis.

El objetivo de esta tesis es analizar las diferentes opciones que puede tener un Proveedor de Servicios de Internet en cuanto a como va a manejar el enrutamiento de los datos IP en su red, para sus clientes y para sus otros proveedores, en base a los Protocolos de enrutamiento existentes y una serie de Políticas de enrutamiento que se pueden aplicar para obtener el mejor desempeño, de acuerdo a las características del *ISP*.

1.3 Propuesta.

Se plantea manejar un escenario de puesta en marcha de un *ISP* el cual le brindará al cliente final el Servicio de Internet ó a un *ISP* Local el cual se considera así por el hecho de revender el servicio que le proporcionan, hasta el *ISP* que servirá de Interconexión como Proveedor Internacional. Se recopilará información acerca de los Protocolos de enrutamiento internos y externos con el fin de analizarlos definir cual de ellos es el adecuado para cada empresa y proponer la implementación de ciertas políticas de enrutamiento para asegurar un óptimo funcionamiento y poder considerarse como un *ISP* confiable y eficiente en el mercado de las Telecomunicaciones.

1.4 Límites del estudio.

El caso propuesto se refiera a un *ISP* el cual pueda llenar las expectativas del mercado o la demanda de los usuarios, particularmente enfocados a los mercados que ya existen en nuestro país de Internet, y que a su vez sirve de proveedor a una Empresa que revende el Servicio, el cual puede ser un Operador de cable Local, llámese un Intercable, Telecable, Televicable, etc, que ya cuenta con una infraestructura de red en lo que respecta al servicio de cable, y puede ofrecer un Servicio de Internet a sus clientes por el mismo medio, y para esto necesita enrutar la información proveniente de sus clientes hacia Internet, el punto a resaltar es que si el Operador de Cable no cuenta con un proveedor Internacional hacia Internet, necesitará depender de un Proveedor más robusto que cuente con la suficiente infraestructura para soportar su Servicio y servirle de enlace hacia el proveedor internacional, es decir nuestro caso propuesto, un *ISP* que servirá como Interconexión con un Proveedor Internacional, y con los demás proveedores, de los cuales podemos mencionar a los tres principales y dominantes en el mercado Mexicano que son *Telmex, Axtel-Avantel y Alestra*, los cuales acaparan la mayoría del tráfico IP que circula en el país, ellos a su vez manejan sus propios *ISPs* internacionales: *Sprint*, *UUNET*, *Global Crossing* y *AT&T* como sus principales.

Debido a la cantidad de recursos de enrutamiento existentes (Enrutamiento Estático, RIP, IGRP, EIGRP, OSPF, IS-IS, IBGP, EBGP) solo se tomaran conceptos teóricos básicos de su funcionamiento, y conceptos de direccionamiento IP, Modelo OSI, LAN, WAN, Dispositivos de Interconexión, que sean de apoyo para comprender correctamente el tema y que serán aplicados a los casos prácticos propuestos de los escenarios mencionados, y servirán de antecedentes para obtener la mejor solución al requerimiento del *ISP.*

1.5 Justificación del estudio.

Como se ha mencionado el mercado de las Telecomunicaciones ha crecido demasiado en los últimos 10 años, por lo tanto existe una gran competencia a nivel global, y para poder llegar a convertirse en un digno participante en el mundo de los *ISPs*, aparte de contar con una buena solución tecnológica en lo que se refiere a Infraestructura de Red (*Backbone*) y los medios de transmisión que utilizará, como parte fundamental de un *ISP*, se encuentra el enrutamiento que dará a los datos desde su origen hasta su destino final, ya que de no existir este factor aplicado de manera correcta, el desempeño en general del servicio se verá impactado.

Esta es la razón por la cual se propone como proyecto de tema de tesis, un análisis a estos protocolos de enrutamiento que ayudaran al *ISP* a escoger cual de ellos se acomoda más a sus necesidades así como políticas de enrutamiento que le pueden ayudar a optimizar recursos y mejorar considerablemente el desempeño de su red y de los servicios que ofrece.

1.6 Metodología.

Para poder elegir el protocolo de enrutamiento IP correcto a utilizar en la red de un *ISP*, se necesita dejar en claro y entender conceptos básicos de temas relacionados entre sí que se trataran a lo largo del proyecto. De los cueles se resaltan:

- Introducción a la organización y funcionamiento de Internet, definir que papel juegan los *ISP* como proveedores de conectividad a los usuarios.

- Introducción y Fundamentos de Protocolos de Enrutamiento IP: Protocolos de Enrutamiento Internos y Externos en los que se incluirían tales como RIP, IGRP, EIGRP, OSPF, IS-IS, IBGP, EBGP, entender los conceptos como direccionamiento IP, LAN, WAN, Sistemas Autónomos.

- Conocer las características o giro de los *ISP* que se desean plantear (que Servicios ofrece a sus clientes tanto internos como externos). En esta parte se incluye desde la Topología de la Red que usarán, pasando desde su infraestructura, hasta sus recursos y capacidades tecnologías.

- Una vez reunida la documentación para soportar el proyecto se evaluarán las opciones de cada protocolo tomando en cuenta las ventajas y beneficios que pueda brindar el protocolo de enrutamiento, según los requerimientos del *ISP* en el caso de Investigación propuesto y en base a estos cuestionamientos teóricos, se tendrá como fin de escoger cual seria la solución mas viable para los propósitos fijados y diseñar de manera teórica como sería la implementación y configuración del protocolo de enrutamiento en la red y a su vez desarrollar las políticas de enrutamiento que reforzaran la optima distribución del trafico en la red como lo puede ser que exista redundancia en la red y un balance en la carga de trafico de los enlaces.

CAPITULO 2

CARACTERISTICAS Y SERVICIOS DE UN *ISP*

Es importante conocer los servicios básicos de un proveedor y las características que afectan a la calidad de las conexiones en Internet, cualquiera que pueda ofrecer conectividad a Internet se puede considerar un proveedor de servicios; el término “Proveedor de Servicios” incluye todo, desde un proveedor con un *backbone* y una infraestructura robusta, hasta un proveedor con un único *router* y un servidor de acceso modesto.

El precio no debería ser el principal factor sobre el cual basar la decisión para elegir un *ISP*. Factores realmente importantes a considerarse son tales como los servicios que ofrece el proveedor, el diseño del *backbone*, la tolerancia a los fallos, la redundancia, la estabilidad, los cuellos de botella, los acuerdos de equipamiento proveedor/cliente, y más.

Los comportamientos del enrutamiento en Internet se ven afectados por el comportamiento de los protocolos de enrutamiento y el tráfico de datos sobre una infraestructura física ya establecida. El buen diseño de la infraestructura y su mantenimiento son factores primordiales para un enrutamiento eficiente en Internet.

2.1 Servicios de los *ISPs*.

Los *ISPs* ofrecen diferentes servicios, dependiendo de su tamaño y de la infraestructura de sus redes. Principalmente, los proveedores pueden clasificarse por su método de acceso a físico a Internet, las aplicaciones que proporcionan a los clientes, y los servicios de seguridad que ofrecen.

A continuación se mencionan los modelos de servicio que son más comunes actualmente en el mercado de los *ISPs*. Dichos servicios varían desde el acceso telefónico mediante línea telefónica en los hogares hasta las posibilidades de hospedaje en un centro de datos donde se coloca el equipo y se conecta localmente.

- **Acceso a Internet dedicado**

El acceso dedicado a Internet se ofrece habitualmente a velocidades desde 56 kbps o 64 kbps hasta líneas T1/E1 (1.5 Mbps y 2 Mbps, respectivamente) en el extremo inferior, y T3/E3 (45 Mbps y 34 Mbps, respectivamente) y STM1 (155 Mbps) en el extremo superior. Pero ya los proveedores esta ofreciendo capacidades de STM4 y superiores como servicios de acceso de alta velocidad, incluso Servicios Ethernet a velocidades de 10/100/1000 Mb/s. Las conexiones de acceso dedicado se utilizan cuando el ancho de banda que se va a usar es previsible y la frecuencia de acceso a la red es lo suficientemente alta para justificar una línea de estas características las 24 hrs. del día. El mayor inconveniente del acceso dedicado es el costo, que normalmente es más alto.

Normalmente, el acceso dedicado a Internet implica la terminación del circuito físico en el dispositivo CPE (equipo terminal del abonado), así como una terminación de circuito directa en un *router* IP en el lado del proveedor del

servicio. Los protocolos de la capa de enlace, como PPP o el DIC de Cisco (un derivado de PPP), son utilizados para señalizar y transferir tramas a través de la conexión. La figura 2.1 ilustra una configuración típica de acceso dedicado a Internet.

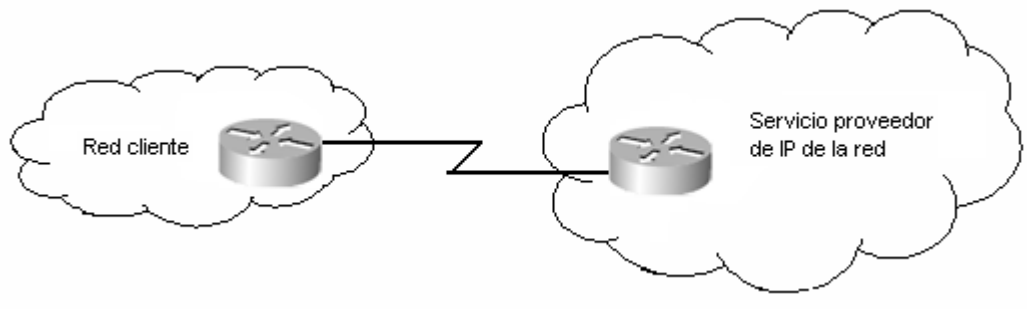

Figura 2.1. Configuración de acceso dedicado a Internet.

- **Acceso a Internet mediante *Frame Relay* y ATM**

Las conexiones *Frame Relay* y ATM (Modo de transferencia asíncrona) están entre las formas más económicas que las empresas pueden elegir para conectarse a Internet. Comprar conexiones de acceso dedicado con suficiente capacidad puede ser excesivamente caro para muchas compañías, en cuyo caso se debe considerar conectarse a Internet a través de servicios como *Frame Relay* o ATM existentes. Con dichos métodos de acceso alternativos, las empresas pueden comprar suficiente ancho de banda para satisfacer sus necesidades mientras proporcionan una ruta práctica de expansión según crecen los requerimientos de ancho de banda.

Dado que los proveedores de servicios pueden, según las estadísticas, multiplexar los datos de múltiples suscriptores sobre un único enlace y luego volver a transportar los datos a una red IP, normalmente los precios asociados a los servicios de acceso a Internet *Frame Relay* y ATM con mucho más bajos que el precio del acceso dedicado.

Los servicios de acceso *Frame Relay* y ATM son particularmente atractivos para empresas que disponen de redes *Frame Relay* y ATM, ya que los proveedores de servicio a menudo proporcionan *gateways* de acceso desde esas redes hasta sus redes IP, por lo que no se requiere una infraestructura adicional por parte del cliente para acomodarse a la nueva conexión.

Aunque *Frame Relay*, ATM y el acceso dedicado a Internet utilizan las mismas tecnologías de capa física subyacente, es importante comprender que los servicios ATM y *Frame Relay*, en comparación con el acceso dedicado, ejecutan una multiplexión estadística antes de proporcionar acceso a la red IP. Esta multiplexión estadística es lo que permite a los proveedores de servicio ejecutar una capa adicional de agregación de servicio, reduciendo así el costo del servicio.

Es importante entender la cantidad de agregación ejecutada por la red de *Frame Relay* o ATM, además de la capacidad y el diseño flexible del *gateway* a Internet. Por ejemplo, un *gateway* a Internet subscrito podría provocar una degradación significativa del rendimiento en su circuito de acceso a Internet.

- **Servicios de acceso telefónico**

Los servicios de acceso telefónico incluyen el tradicional acceso a través de un módem, con velocidad hasta 56 kbps. También incluyen ISDN-RDS (Red digital de servicios integrados), BRI (Interfaz de acceso básico) de hasta 128 kbps y PRI (interfaz de acceso primario) con velocidades de hasta 1.5 Mbps. Los servicios de acceso telefónico varían desde el servicio de usuarios individuales hasta empresas que subcontratan con los proveedores la obtención de todas sus necesidades de conexión remotas. Los servicios RDSI, BRI y PRI han experimentado un tremendo crecimiento durante los últimos

años, principalmente debido a su naturaleza bajo demanda (se utiliza sólo cuando se necesita) y su capacidad para transportar señales digitales empleadas por aplicaciones multimedia, como las de videoconferencia.

- **Línea de abonado digital**

Los servicios de Línea de abonado digital (DSL) proporcionan acceso a Internet de alta velocidad y bajo costo. Encajan adecuadamente entre el acceso telefónico y los servicios de acceso dedicado en términos de precio y velocidad. Los tipos de servicio DSL, varían en función de las tecnologías DSL que se utilice. Normalmente se utiliza el término xDSL para referirse a los servicios genéricos DSL, donde x puede representar cualquier número de las diferentes técnicas de codificación utilizadas a través de la línea física en la Capa 1.

Un beneficio de la tecnología DSL es que se puede utilizar los cables de par trenzado de cobre de la antigua red de telefonía básica (RTB), convirtiéndola en una tecnología de acceso popular para el hogar y pequeño negocio. Normalmente los servicios DSL disponibles varían significativamente entre proveedores y regiones, con velocidades entre 64 kbps y 52 Mbps (VDSL). La calidad de los cables tendidos y la distancia desde la oficina central (CO) servidora pueden tener que ver significativamente con el rendimiento y la tasa de transferencia características de una conexión DSL.

- **Módems por cable**

Al igual que DSL, los módems por cable son una tecnología de acceso de rápido crecimiento. Los módems por cable elevan el ancho de banda potencial de las líneas de televisión por cable para proporcionar servicios de acceso.

Dado que los servicios de MODEM por cable fueron diseñados para utilizar la infraestructura existente de fibra y cable coaxial de televisión, infraestructura que estaba optimizada para transportar difusiones en un solo sentido, el ancho de banda disponible es normalmente muy asimétrico por naturaleza. Por ejemplo, los servicios típicos proporcionan capacidades cercanas a los 2 Mbps en flujo descendente (hacia la ubicación del suscriptor) y 64 kbps de flujo ascendente (hacia la red del proveedor del servicio).

Además, a diferencia de DSL, que es una tecnología punto a punto, el ancho de banda del flujo descendente es compartido por múltiples usuarios del servicio, creándose de este modo problemas de seguridad para los fabricantes, proveedores de servicio y consumidores. A pesar de estos desafíos, los servicios del módem se han distribuido durante varios años, y el numero de abonados y la disponibilidad del servicio esta creciendo rápidamente.

- **Servicios de Alojamiento Dedicado**

Los grandes proveedores enfocados al alojamiento dedicado se conocen comúnmente como proveedores de contenido. Normalmente, dichos proveedores desarrollan centros de datos de alta tolerancia a fallos que alojan en armarios o *racks* en los cuales tanto empresas como clientes del alojamiento web pueden alquilar espacio y colocar servidores u otro equipamiento informático. Después, los proveedores venden acceso a Internet a los dispositivos colocados localmente, a través de las tecnologías como Fast Ethernet (100 Mbps) y GigabitEthernet (1Gbps).

Los proveedores de alojamiento utilizan a menudo *switches* Ethernet de alta gama para agregar tráfico precedente de miles de servidores colocados. Los consumidores deberían interesarse por el índice de sobresuscripción del flujo ascendente y los mecanismos de fallos utilizados por el proveedor.

También, dadas las implicaciones de seguridad de las redes conmutadas grandes, los consumidores deberían ser conscientes de si y cómo (normalmente con LAN virtuales) el proveedor separa los dominios de difusión. En una red conmutada compartida, común en el modelo de alojamiento de contenido, la compresión de esos temas es extremadamente importante para prevenir potenciales ataques de denegación del servicio, acceso no autorizado y visibilidad de los datos y otros problemas de seguridad y administración.

- **Otros Servicios de los *ISPs***

Otros servicios de capa superior incluyen e-mail y servicios de noticias, VPN (Redes privadas virtuales) y multidifusión IP. Como estos y otros nuevos servicios continúan evolucionando, los clientes necesitan calcular sus costos y beneficios en las opciones disponibles. La principal preocupación debe ser como se suministran y administran los servicios, así como del conocimiento base del personal asociado dedicado al soporte y la ingeniería.

Muchos *ISPs* también ofrecen consultoría y otros servicios de valor agregado, tales como la seguridad. Los servicios de seguridad más simples incluyen filtros de paquetes en el dispositivo de acceso. Otros servicios mas evolucionados incluyen encriptación de datos y detección de virus.

2.2. Precio del Servicio de los *ISPs.*

Los precios pueden variar significativamente en función de la dependencia del método de acceso de un proveedor dado, también varían significativamente basándose en la inversión en infraestructura, operaciones y en los recursos de la ingeniería. Además de evaluar la disponibilidad de los servicios, los clientes deberían considerar el precio y las características técnicas de un servicio ofrecido antes de seleccionar un proveedor. Aunque las

características técnicas en particular puedan parecer intimidatorias, influyen en la fiabilidad y facilidad de acceso al proveedor que finalmente se seleccione. Los temas técnicos a los que se dirige esta sección incluyen características de *backbone*, demarcación del circuito y alojamiento dedicado.

Los precios también varían incluso para los mismos servicios dentro de la misma región geográfica. La fuerza relativa del proveedor y la inversión en un área particular a menudo determinan el precio de un servicio determinado. Por ejemplo, un proveedor que ya tiene establecido un servicio de *Frame Relay* probablemente dará un precio mucho mejor que un proveedor que acaba de empezar a distribuir el mismo tipo de servicio. Por otro lado, el nuevo proveedor puede ser más competitivo porque no tiene una inversión en una infraestructura propietaria necesaria para acomodar el servicio, lo que le permite beneficiarse de la solidez de la nueva plataforma y de las capacidades del servicio proporcionado.

Por este y otros muchos factores, obtener el mismo precio de diferentes proveedores no significa necesariamente que se esté obteniendo los mismos servicios. Otro ejemplo, con un acceso dedicado, algunos proveedores incluyen el CPE, tal como un *router* y una CSU/DSU (Unidad de servicio de canal/Unidad de servicio de datos), como parte del producto. Otros cobran una tasa adicional por el CPE, existen varios factores, se puede ahorrar una cantidad significativa si se aporta el propio CPE o talvez pueda resultar más interesante pagar a un proveedor para proporcionar y/o administrar el CPE.

2.3 Acuerdos a nivel de Servicio.

Muchos proveedores de servicio actuales están creando también SLA/SL (Acuerdos a nivel servicio/Garantías a nivel de servicios) muy competitivos que definen una base para garantizar el rendimiento y la disponibilidad cuando se

utilizan sus servicios. Asegurarse que los detalles de estos acuerdos, así como las penalizaciones en caso de no cumplirlos estén claramente definidos. También preguntar al proveedor como se controlan actualmente las garantías y si se generan automáticamente informes de excepciones ya sean provenientes del mismo proveedor o del cliente.

Normalmente esas garantías tratan de los porcentajes aceptables de pérdidas de paquetes y del retraso en el que se incurre en la red, así como la disponibilidad de acceso al circuito y mantenimiento y/o líneas de tiempo de notificación obsoletas. Los compromisos a los que se llega un proveedor de servicios en los SLA pueden constituir un verdadero diferenciador del servicio.

2.4 Criterios de selección del *backbone* del *ISP*.

Un *backbone* de red de un *ISP* abarca muchas características técnicas importantes, incluyendo las siguientes:

- Topología física de la red.
- Cuellos de botella en la red y razones de suscripción.
- Nivel de la red y redundancia de los elementos individuales de la misma.
- Interconexiones con otras redes, incluyendo distancias a destinos y acuerdos de intercambio de tráfico.

Al momento de elegir un *ISP* es importante evaluar estas características; son mucho más importantes que el precio cuando se intenta predecir la calidad del servicio. Los arquitectos deberían considerar los beneficios potenciales y las dificultades asociadas con dichas características cuando instalen o amplíen sus redes.

2.5 Conexiones físicas.

Los clientes deberían investigar la topología física de la red del proveedor, y el proveedor debería ser capaz de proporcionar un mapa actualizado de la red con todas las conexiones indicadas. Con respecto a las conexiones, una topología física saludable es una que pueda proporcionar un ancho de banda consistente y adecuada para toda la trayectoria del tráfico, incluso en el caso de que una o varias conexiones no estén disponibles. La existencia de enlaces de *backbone* de alta velocidad tales como OC12 y OC48 no garantiza por sí mismo el acceso de alta velocidad para los clientes. Su tráfico puede entrar en la red del proveedor desde una conexión con *backbone* de baja velocidad, o una conexión de alta velocidad pero con un *backbone* altamente sobrecargado. Estos factores afectarán a la calidad de la conexión.

2.6 Cuellos de botella potenciales de los *ISPs* y tasa de suscripción.

La red del proveedor sólo es tan fuerte como su enlace más débil. Hay dos cuellos de botella potenciales en in *ISP*: sobresuscripción de enlaces troncales de *backbone* y circuitos pequeños que llevan a un cliente POP o de flujo descendente. Los *ISPs* que intentan ahorrar dinero sobrecargando sus *routers* o conexiones acabarán perdiendo credibilidad a largo plazo.

La sobresuscripción ocurre cuando la utilización acumulada de múltiples enlaces excede el ancho de banda del conducto utilizado para transportar el tráfico a su destino. Como se muestra en la figura 2.2 una regla común es usar un índice del 5:1; no debería haber más de cinco enlaces T1 por cada conexión T1 al *backbone*. Las tasas de suscripción varían basándose en el producto que se ofrece. Normalmente, los proveedores de alojamiento dedicado utilizan a menudo tasas de 8:1 o incluso 10:1. Dichos valores

normalmente están basados en experiencias anteriores, pero si no están cuidadosamente seleccionados y administrados, rápidamente pueden dar lugar a una congestión.

Otro ejemplo de cuello de botella potencial son los sitios de alta velocidad intentando acceder a la información de sitios de baja velocidad. Un servidor *web* ubicado en un sitio conectado a Internet mediante un enlace de 56 kbps puede ser accedido a una velocidad máxima de solo 56 kbps, sin reparar en la velocidad de los enlaces utilizados por las personas que acceden al sitio.

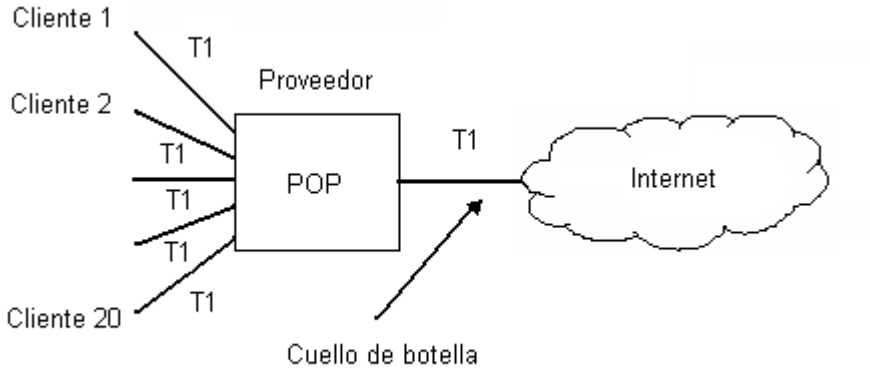

Figura 2.2. Limites de rendimiento del enlace más débil de un ISP.

2.7 Nivel de redundancia del acceso a Internet de un *ISP*.

Ya sea por condiciones climatológicas, problemas de la portadora o por otras causas, la conexión de un *ISP* a un *NAP* (Punto de acceso a la red), a otro proveedor o a otro POP no estará disponible en algún punto, lo que dará como resultado la imposibilidad potencial de alcanzar un conjunto de destinos. Una red redundante permite que el tráfico utilice una ruta alternativa para alcanzar dichos destinos mientras se soluciona el problema. Una red de un *ISP*

bien diseñada tiene los POP conectados a múltiples *NAP*, a las redes de otros proveedores y a muchos otros POP.

Es importante comprender que el *peering* (enlace de vecindad para compartir información) y la redundancia de interconexión con otras redes normalmente son proporcionados sobre una base global. Si la conexión a un proveedor deja de estar disponible a través del punto de intercambio de tráfico primario, se seleccionará el siguiente punto de intercambio más cercano. La idea no es aprovisionarse de capacidad redundante de la misma ubicación a otra red, sino asegurarse de que existe suficiente capacidad de interconexión y *backbone* sobrantes para evitar las fallas de uno o más lugares de la red. Con este enfoque, suministrando más interconexión y circuitos *NAP* en lugares geográficamente más óptimos puede compensar los costos de las conexiones redundantes, beneficiando a la red tanto durante el funcionamiento normal como en escenarios de falla suministrando esta redundancia sobre una base global frente a una base POP-por-POP.

Cuando se habla de redundancia, también se debería considerar un plan de reposición del proveedor. La mayoría de los proveedores mantienen en el sitio un suministro de componentes de *hardware* críticos y administran el equipamiento sobrante como un repuesto. El número de componentes sobrantes normalmente depende de la naturaleza crítica del componente, así como del tiempo medio entre fallos teórico del componente. Algunos proveedores prefieren subcontratar los servicios de repuestos, normalmente a compañías que mantienen almacenes geográficamente dispersos, y compartir el inventario entre varios clientes. Aunque esta actuación incrementa potencialmente el MTTR (tiempo promedio de reparación) cuando surgen problemas.

2.8 Distancia a los destinos.

Un típico concepto erróneo es que los clientes deberían preocuparse solo por el numero de saltos IP (el número de *routers* IP) requerido para alcanzar un destino de la red determinado a través de su ISP. En el pasado, era cierto de alguna manera que a mayor número de saltos IP mayor era la probabilidad de que algunos paquetes llegasen con retraso, se desvíen o fueran ilegibles. Actualmente sin embargo, muchos *backbones* de las redes de los ISPs están basados en tecnologías MPLS (*Switching* de etiqueta multiprotocolo), ATM o *Frame Relay*, que dan como resultado muchos saltos de dispositivos de Capa 2, pero son transparentes a las herramientas de detección de rutas IP tales como el trazado de ruta.

Un número menor de saltos IP a un destino a través de una red dada bien puede indicar una ruta mejor al destino que a través de una red con más saltos. Sin embargo, es importante comprender sobre qué tecnologías intermedias están basados antes de hacer tales suposiciones. Por ejemplo, podría ser más deseable tomar varios enlaces de alta velocidad en lugar de viajar a través de uno de baja velocidad.

Como ya se sabe, Internet es un gran conglomerado de *backbones* de red superpuestos conectados a través de puntos de intercambio e interconexiones directas. Es una idea razonablemente buena evaluar el número de saltos de red o de AS (el número de dominios de enrutamiento que se cruzan) para un conjunto dado de destinos. La distancia a los destinos dependerá del número de redes de destino que adquieran conectividad desde el proveedor y de la calidad de conexión del proveedor con las otras redes. Los proveedores más pequeños podrían conectarse sólo a un *NAP*, o podrían no conectarse a ninguno. A menudo, los grandes proveedores se conectan a otras redes a través de *NAP* e interconexiones directas.

2.9 Acuerdos de intercambio de tráfico.

Es un requisito absoluto que los *ISPs* sean parte de acuerdos de intercambio de tráfico, que normalmente son negociados bilateralmente sobre una base de igual a igual. Dada la arquitectura actual de Internet y la poca regulación que existe sobre quién y cómo debería interconectarse (si directamente o a qué *NAP*), es total responsabilidad del *ISP* cómo aproximarse al modelo de intercambio de tráfico.

Durante años, los *ISPs* han dado vueltas a ideas en lo que se refiere a acuerdos asociados con redes interconectadas, pero los argumentos sobre quién paga a quién y cómo deben medirse los costos han producido pocos consensos. Los grandes ISP están comenzando a mover más y más tráfico hacia un modelo de interconexión directa más distribuido, utilizando *NAP* sólo para conectarse a proveedores más pequeños. Los grandes *ISP*s son cada vez más estrictos en lo que se refiere a quiénes se conectan por igual a los *NAP*. Esa información a menudo está protegida por un NDA mutuo (Acuerdo de no revelación) firmado por ambas partes.

Aunque a los proveedores potenciales probablemente no les guste la idea de revelar especificaciones de acuerdos de intercambio de tráfico con otras redes, normalmente están deseando proporcionar números de capacidad disponibles y otra información útil en lo que se refiere a interconexiones y políticas de *peering*. El modo de conexión de un proveedor con otras redes podría ser la pieza más importante de información en lo referente a las características de rendimiento potencial de la conexión que adquiera.

2.10 Punto de demarcación.

Finalmente, además del precio, el *backbone* y los temas de interconexión, los clientes deberán considerar los temas relacionados a los puntos de demarcación cuando se seleccione un *ISP*. Un punto de demarcación es el punto que diferencia las responsabilidades y la red del proveedor de las responsabilidades y la red del cliente. Esto es particularmente cierto en un entorno de alojamiento dedicado de un proveedor de servicios. Es importante comprender la diferencia entre las responsabilidades del proveedor y las del cliente. Los puntos de demarcación definen hasta los cables y los conectores para asegurar la ausencia de desacuerdos en caso de problemas de equipamiento o de red, en la figura 2.3 se muestra un punto de demarcación típico entre la red de un *ISP* y la de un cliente.

Diferentes proveedores definen los puntos de demarcación de forma diferente, normalmente dependiendo de quien paga el equipamiento y la línea de acceso, dónde está situado el equipo y quién lo administra.

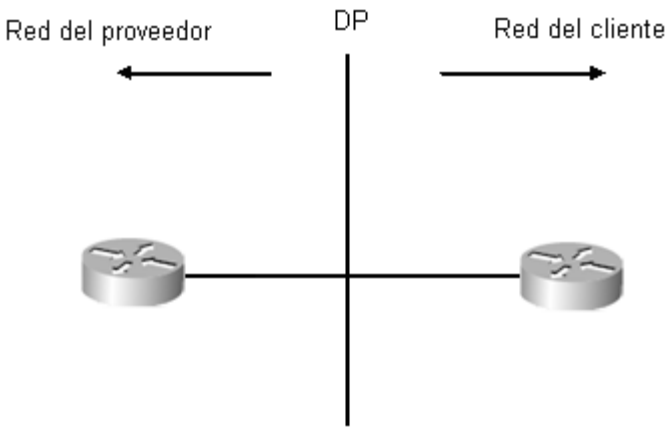

Figura 2.3. Punto de demarcación.

El proveedor siempre está disponible para solucionar problemas, normalmente por una tarifa adicional. Existen algunos paquetes de los *ISP*.

Uno de los paquetes ofertados es cuando el *ISP* es responsable de la línea de acceso y la CSU/DSU hasta el conector serie de la CSU en la ubicación del cliente. Se pueden imponer restricciones sobre el *router* local del cliente y reunir algunas pautas sobre la memoria y la revisión del software. Otro de ellos puede ser cuando le proporciona el acceso y la CSU/DSU; el cliente proporciona el *router*. El último que se mencionara es cuando el cliente proporciona el CPE y la línea de acceso. La responsabilidad del proveedor termina en el armario del cableado del POP, donde el *ISP* se Interconecta con la oficina central de la portadora.

2.11 Colocación del router.

La colocación es el acto de situar el equipo de una parte en el espacio de la otra. Un ejemplo de colocación es poner el *router* del cliente en el centro sitio de alojamiento del proveedor. Los motivos del cliente para dicho esquema de colocación serían que el *ISP* proporcione mayores velocidades de acceso o control local del equipamiento, o talvez ofrecer al cliente mejor control de la utilización del ancho de banda.

La situación opuesta a la descrita anteriormente es que el *ISP* coloque su propio *router* POP en el sitio del cliente. Normalmente, en este caso, el *ISP* adquiriría la línea de acceso y el *router* y cobraría al cliente una tarifa por el servicio completo.

Las características técnicas de la red de un *ISP* tienen repercusiones significativas en el servicio del cliente, incluyendo la calidad de la arquitectura del enrutamiento que es en lo que se centra este estudio. Dado que el cliente

no podría tener control directo sobre alguna de dichas características, es crítico que al menos, el cliente las evalúe y se asegure que le entregan la conectividad y la calidad requeridas.

Si se es cliente de un *ISP* cuyo punto de demarcación y acuerdos de colocación estipulan que está ejecutando y manteniendo el equipamiento en su propiedad (incluso si no lo posee en su totalidad) probablemente tomará un papel significativo en el desarrollo de las políticas de enrutamiento y arquitectura de la red. Incluso si no se está ejecutando y manteniendo el equipamiento, hay decisiones que se necesitan tomar y comprender con respecto a la arquitectura de enrutamiento.

CAPITULO 3

DIRECCIONAMIENTO IP EN INTERNET

3.1 Arquitectura de direcciones en Internet.

La arquitectura de direcciones de Internet está implementada en IP. El esquema original de IP se remonta a los primeros días de la computación en red. Es esa época, la propia Internet era más que una red semipública que interconectaba unas pocas decenas de universidades, organizaciones de investigación y organismos gubernamentales. Cada una de estas entidades conectadas a Internet tenía infraestructuras de computación en red limitadas. Generalmente, estas infraestructuras consistían en poco más que una computadora *mainframe* o algunas microcomputadoras basadas en UNIX. Las PCs no habían confluido en un formato utilizable, las redes de área local (*LAN*) estaban apenas desarrollándose. Por lo tanto una *internetwork* no requería una arquitectura robusta.

La Internet original tenía una jerarquía de dos niveles relativamente simple, pero compacta. El nivel superior era Internet, y el nivel inferior era el conjunto de redes individuales que estaban conectadas vía Internet. Se ilustra lo anterior en la figura 3.1. La arquitectura de Internet, simple pero poderosa y extensible, servía bien a la comunidad de usuarios.

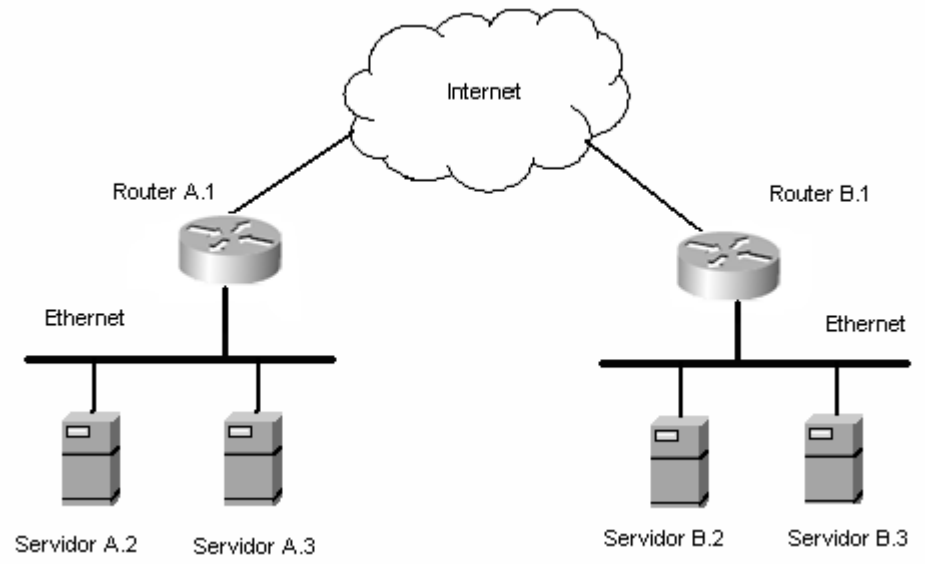

Figura 3.1. Internet usaba una jerarquía de dos niveles.

Publicación de direcciones de red

Cada uno de los *hosts* en Internet necesitaba tener una identificación única. En la jerarquía de dos niveles de Internet, esto requería una dirección de dos partes:

- Dirección de red
- Dirección de *host*

Juntos estos dos tipos de direcciones podían identificar univocadamente cualquiera de las computadoras conectadas vía Internet. Es posible que las necesidades de una pequeña comunidad conectada en red pudieran satisfacerse sólo con direcciones de *host*, como en el caso de la LAN. Las direcciones de red sin embargo, son necesarias para que los sistemas finales de diferentes redes puedan comunicarse entre sí. Es la combinación única de dirección de *host* y de red lo que hace posible acceder a cualquier *host* de una *internetwork*.

En lugar de hacer un seguimiento de las rutas a cada *host* conocido, Internet publica sólo las direcciones de red. Los sistemas finales que necesitan acceder a los *hosts* de otras redes direccionan sus datagramas con la dirección completa, incluyendo tanto el número de red como el de *host*, pero los *routers* de la *internetwork* podrían suponer que la red de destino sabe cómo entregar datagramas a todos los sistemas finales que hay dentro de su domino. Por tanto, los *routers* de Internet sólo tendrían que seguir las rutas a cada red conocida.

Para poder apreciar el concepto de la publicación de direcciones de red, se utilizará una dirección ficticia de dos niveles. Estas direcciones ficticias identifican las redes con un solo carácter alfabético, y los sistemas finales con un solo carácter numérico. Estos componentes de la dirección siguen la convención familiar de las direcciones IP, y separan las componentes con un punto. Por lo tanto, A.2 únicamente identifica al Sistema final 2 de la Red A.

Un *router* de *backbone* de Internet quedaría pronto sobrecargado si siguiera las rutas por Internet a cada sistema o *host*. En su lugar, los arquitectos de Internet y de IP implementaron una arquitectura física de dos niveles. Esta se acompañaba con una dirección de red de dos niveles, que constaba de una dirección de red y una de *host*. La implicación más práctica de semejante esquema era que los *routers* de *backbone* de Internet podían reducir mucho su cantidad de trabajo al tener que hacer un seguimiento tan sólo de las rutas de direcciones de red.

Los *routers* que comprende el *backbone* de Internet podrían calcular las rutas a través de Internet para cada uno de los *hosts* de la figura 3.1. La tabla 3.1 presenta sus tablas de enrutamiento de forma muy simplificada y homogenizada.

Dirección de red	Dirección de *host*	*Gateway* de destino
A	2	A.1
	3	A.1
B	2	B.1
	3	B.1
C	2	C.1
	3	C.1
	4	C.1

Tabla 3.1. Contenido de la tabla de enrutamiento al usar enrutamiento basado en *host*.

Como se puede ver en la tabla 3.1, el *gateway* de destino identificado por los *routers* de Internet no varía si se tuviera en cuenta la dirección de *host*. Por lo tanto, hacer un seguimiento de las rutas a los *host* individuales (enrutamiento basado en *host*) sólo supondría trabajo innecesario para los *routers* de la *internetwork*. El *gateway* de destino, sin embargo, si variaría en función de la dirección de red. Así pues, los *routers* de Internet pueden reducir su cantidad de trabajo e incrementar su eficacia al no tener que memorizar las rutas de cada *host*. Pueden publicar rutas a los números de red sin comprometer su capacidad de distribuir datagramas. La tabla 3.2 muestra cómo la publicación de la ruta de red puede reducir el tamaño de las tablas de enrutamiento.

Dirección de red	Enviar datagramas a
A	A.1
B	B.1
C	C.1

Tabla 3.2 Contenido de la tabla de enrutamiento al usar enrutamiento basado en la red.

El tamaño, muy reducido, de las tablas de enrutamiento, basadas en la red no compromete la capacidad de los *routers* de Internet para enviar datagramas a sus destinos. Sin embargo, la publicación de las rutas de red

tiene otras numerosas implicaciones. Puede mejorar el rendimiento de un *router*, por ejemplo. Cuantas más entradas existan en la tabla de enrutamiento de un *router*, más se tardará en determina a dónde enviar un datagrama. El datagrama debe ser almacenado en un búfer de memoria del *router* hasta que se tome esta determinación. Por lo tanto, cuanto mayor sean las tablas de enrutamiento de una red, mayores serán las demandas sobre los recursos físicos de los *routers* de la red, especialmente sobre los ciclos de memoria de acceso aleatorio (RAM) y de la unidad central de procesamiento (CPU), aumentar la cantidad de ambos recursos puede resultar caro.

Estrechamente relacionada con el rendimiento, pero mucho más importante está la escalabilidad. La publicación de rutas de red permite a las *internetworks* ser altamente escalables. Prueba de esto es el tamaño inmenso de la Internet Actual. Sin la capacidad de publicar las rutas de red, el crecimiento de Internet se hubiera visto muy limitado. Internet fue ayudado en su escalabilidad por su sofisticada arquitectura de direcciones. Sus arquitecturas previeron el potencial de crecimiento y desarrollaron una arquitectura de direccionamiento flexible y extensible a la vez. Esta arquitectura fue implementada en IP.

El esquema de direccionamiento utilizado hoy en día en Internet se basa en la versión del Protocolo Internet (IPv4), conocido normalmente como IP.

3.2 Direccionamiento IP básico

Una dirección IP es un valor único de 4 octetos (32 bits) expresado en notación decimal con puntos de la forma W.X.Y.Z, donde los puntos se utilizan para separar cada uno de los 4 octetos de la dirección. El campo dirección de 32 bits consta de dos partes: un número de red o enlace (que representa la

parte de red de la dirección) y un número de *host* (que identifica un *host* en el segmento de red).

Los limites de la red y el *host* se definían tradicionalmente basándose en la clase de dirección IP, con cinco clases definidas (tres de las cuales se utilizan para direccionamiento de unidifusión): A, B, C, D y E. La tabla 3.3 ilustra las diferentes clases de espacio de direcciones y sus funciones.

Clase	**Rango de direcciones**	**Bits de Orden alto**	**Bits de red**	**Bits de *host***	**Función**
A	0.0.0.0 a 127.255.255.255	0	7	24	Unidifusión
B	128.0.0.0 a 191.255.255.255	10	14	16	Unidifusión
C	192.0.0.0 a 223.255.255.255	110	21	8	Unidifusión
D	224.0.0.0 a 239.255.255.255	1110			Multidifusión
E	240.0.0.0 a 255.255.255.255	1111			Reservado

Tabla 3.3. Funciones y clases de direcciones IP.

Solo las direcciones de clase A, B y C se utilizan para unidifusión. Las direcciones de clase D para multidifusión y las de clase C están reservadas. Este esquema de direccionamiento basado en clases se conoce como modelo con clase. Las diferentes clases se prestan a diversas configuraciones de red, dependiendo de la proporción deseada entre redes y *hosts*.

3.2.1 Direccionamiento de Clase A

La dirección IPv4 de Clase A fue diseñada para dar cabida a redes extremadamente grandes. Como la necesidad de redes de gran tamaño se estimaba mínima, se desarrolló una arquitectura que maximizaba el número posible de direcciones de *host*, pero que limitaba severamente el número posible de redes de Clase A que podían definirse. Las redes de Clase A están

representadas por un 0 en el bit más a la izquierda de la dirección. El primer octeto (bits 0 a 7) de la dirección, comenzando por el bit situado más a la izquierda, representa el número de red, y los siguientes octetos (bits 8 al 31) representan un número de *host* en dicha red. Dentro del rango de clase A se tienen las siguientes consideraciones dado que 0.0.0.0 no es número de red válido, sólo son posibles 127 (2^7-1) direcciones de Clase A y técnicamente 127.0.0.0 es también una dirección de red de Clase A. Sin embargo, está reservada para pruebas *loopback*, y no puede asignarse a una red.

3.2.2 Direccionamiento de Clase B

Las direcciones de Clase B fueron diseñadas para dar respuesta a las necesidades de redes de tamaño moderado a grande. El rango de direcciones posibles de red de Clase B va de 128.1.0.0 a 191.254.0.0.Las redes de Clase B están representadas por un 1 y un 0 en los dos bits situados más a la izquierda de la dirección. Los dos primeros octetos de la dirección (bits 0 al 15) representan la parte de red de la dirección, y los dos octetos restantes (bits 16 al 31) representan el número de *hosts* de dicha red.

3.2.3 Direccionamiento de Clase C

El espacio de direcciones de Clase C es, el más comúnmente utilizado de las clases de direcciones IPv4 originales. Este espacio de direcciones fue creado para dar lugar a muchas redes pequeñas. Esta clase de dirección podía considerarse la inversa de direcciones de Clase A. Las redes de Clase C se representan por 1, 1 y 0 en los tres bits situados más a la izquierda de la dirección. Los primeros tres octetos (bits 0 al 23) representan el número de red, y el último octeto (24 al 31) representa el número de *hosts* de las red.

En la figura 3.2 se resume la asignación de bits para la porción de red como de *hosts* de las clases mencionadas anteriormente.

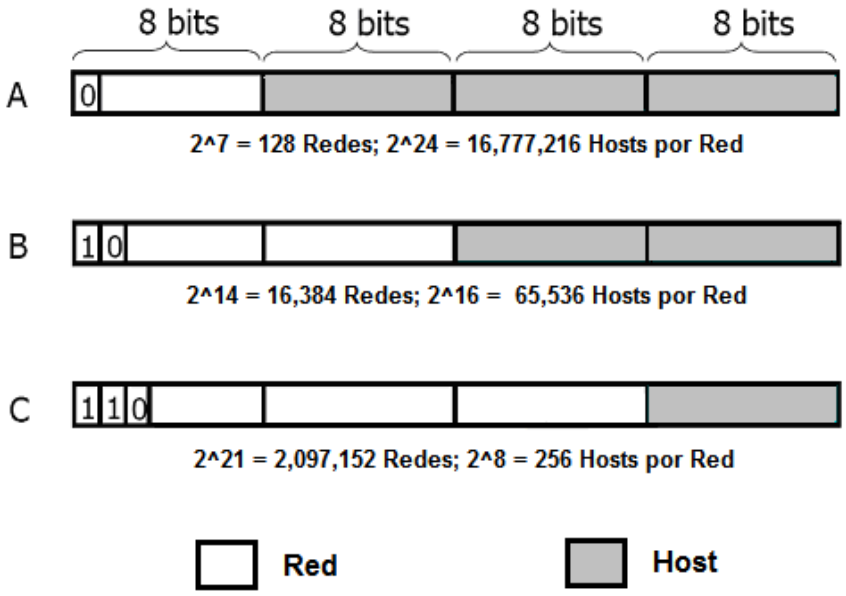

Figura 3.2 Clases de Direcciones IP.

3.2.4 Direccionamiento de Clase D

La dirección de Clase D se creó para permitir la multidifusión en una red IP. Los mecanismos de multidifusión de Clase D han tenido un uso limitado. Una dirección de multidifusión es una dirección de red única que dirige paquetes con esa dirección de destino a grupos predefinidos de direcciones IP. Por lo tanto una sola estación puede transmitir simultáneamente un mismo flujo de datagramas a múltiples receptores. La necesidad de crear flujos separados de datagramas, uno por cada destino, es eliminada. Los *routers* que soportan la multidifusión deberían duplicar los datagramas y enviarlos según fuera necesario a los sistemas finales predeterminados. La multidifusión se ha considerado durante mucho tiempo como una característica deseable de una red IP, porque puede reducir sustancialmente el tráfico en la red. Las redes de Clase D se representan por 1, 1, 1 y 0 en los cuatro bits situados más a la izquierda de la dirección. El espacio de las direcciones de Clase D está reservado para multidifusión, utilizado para representar números de grupo de

multidifusión. El espacio de direcciones de clase D oscila entre 224.0.0.0 y 239.255.255.254.

3.2.5 Direccionamiento de Clase E

Las redes de Clase E se representan por 1, 1, 1 y 1 en los cuatro bits situados más a la izquierda de la dirección. El espacio de las direcciones de Clase E está actualmente reservado para uso experimental.

En el direccionamiento IP, el 0 y el 255 son valores de dirección de *host* reservados. Las direcciones IP que tienen todos los *bits* de la dirección de *hosts* iguales a cero identifican la red local. De forma similar, las direcciones IP que tienen todos los bits de la dirección del *host* iguales a 255 se usan para transmitir a todos los sistemas finales que hay dentro de ese número de red.

3.2.6. Direcciones IP Privadas.

Estas direcciones, se utilizan para uso privado en un ambiente LAN, es decir direccionamiento que no va a salir a Internet. En la tabla 3.4 se enlistan las direcciones IPs privadas.

Rando de Direcciones IP	**Clase de Red**	**Numero de Redes**
10.0.0.0 a 10.255.255.255	A	1
172.16.0.0 a 172.31.255.255	B	16
192.168.0.0 a 192.168.255.255	C	256

Tabla 3.4. Direcciones IPs Privadas.

Los grandes vacíos entre estas clases de direcciones han malgastado un número considerable de direcciones potenciales a lo largo de los años. Quizá la práctica menos provechosa fuera que los espacios de las direcciones

se suministren bajo demanda. Cualquier organización que quería un espacio de direcciones sólo tenía que pedirlo. No se intentaba siquiera verificar su necesidad. En consecuencia, muchas organizaciones bloquearon porciones sustanciales del espacio de direcciones IPv4 como protección frente a una imprevisible y no especificada necesidad futura. Debido a esta problemática y a la escasez que se presentarían de direcciones IP fue necesario definir nuevas soluciones a estos inconvenientes, las cuales se mencionan a continuación.

3.3 Extensiones para IP

Afortunadamente, esto ya no sucede. Se ha desarrollado numerosas extensiones para IP que están específicamente diseñadas para mejorar la eficacia con la que puede usarse el espacio de direcciones de 32 bits, que a continuación se mencionan:

- Máscaras de subred
- VLSM
- Enrutamiento entre dominios sin clase CIDR
- NAT

Estos son mecanismos muy diferentes, que fueron diseñados para resolver diferentes problemas. Las máscaras de subred, tanto fijas como de longitud variable (VLSM), se desarrollaron para adaptarse a las múltiples redes lógicas que pudieran existir dentro de un sitio físico conectado a Internet. CIDR se desarrolló para eliminar la ineficacia inherente a las rígidas clases de direcciones originales. Esto permitió a los *routers* de Internet agregar de manera más eficaz muchas direcciones de red diferentes en una sola entrada de la tabla de enrutamiento. Es importante observar que estos dos mecanismos no son mutuamente exclusivos, sino pueden y deben usarse juntos. El organismo que actualmente se encarga de regular y suministrar las

direcciones IPv4 restantes es la IANA (Agencia de asignación de números Internet), esto para que no se produzca la duplicación de las direcciones utilizadas públicamente. Dicha duplicación provocaría inestabilidad en Internet y comprometería su capacidad de distribuir datagramas a redes utilizando las direcciones duplicadas. Otro objetivo cumplido por esta cuidadosa administración del espacio de direcciones es que la tasa de agotamiento del espacio de direcciones (que fomentó el desarrollo de IPv6) se ha reducido considerablemente. En consecuencia, se espera que el espacio de direcciones IPv4 siga siendo adecuado en los años siguientes.

3.3.1 Máscaras de subred (*Subnetting*)

La jerarquía de dos niveles original de Internet suponía que cada sitio tendría una única red. Por lo tanto, para cada sitio se necesitaría una sola conexión a Internet. Inicialmente, estas suposiciones se cumplieron. Sin embargo, con el tiempo. La computación en red maduró y se expandió. Hacia 1985 no se podía suponer que una organización tendría una sola red, ni que estuviera satisfecha con una sola conexión a Internet. Cuando los sitios empezaron a desarrollar múltiples redes, se hizo obvio para el IETF que era necesario algún mecanismo para diferenciar entre las múltiples redes lógicas que estaban emergiendo dentro de los sitios de segundo nivel de Internet. De otro modo, puede que no hubiera un modo eficaz de enrutar datos a sistemas finales específicos en sitios con múltiples redes. Una respuesta era dar a cada red lógica, o subred, su propio intervalo de direcciones IP. Esto funcionaría, pero sería un uso tremendamente ineficaz del espacio de direcciones IP. No pasaría mucho tiempo hasta que este método amenazara con disminuir por completo los intervalos de direcciones IP restantes, no asignados. Un impacto más inmediato sería la expansión de las tablas de enrutamiento en los *routers* de Internet. Cada red necesitaría su propia entrada en la tabla de enrutamiento. Estaba claro que era necesario encontrar un método mejor.

Una subred es un subconjunto de una red de Clase A, B, o C, como ya se comentó, las direcciones IP constan de una parte de red y una de *host*, representando un modelo jerárquico de direccionamiento estático de dos niveles (redes y *hosts*), el *subnetting* IP introduce un tercer nivel de jerarquía con el concepto de máscara de red. La máscara de red sirve como máscara de bits con el conjunto de bits correspondiente a los bits utilizados para el número de red IP con clase, así como el conjunto adicional de bits correspondiente al número de subred.

Cada dirección de Clase A, B y C tiene lo que se llama una máscara natural, que es la máscara creada por la definición de la red y la parte de *host* de cada clase. Las máscaras naturales para las direcciones de Clase A, B y C son las siguientes:

- La máscara natural de la Clase A es 255.0.0.0
- La máscara natural de la Clase B es 255.255.0.0
- La máscara natural de la Clase C es 255.255.255.0

Mediante la separación de las partes de red y de *host* de la dirección IP, las máscaras facilitan la creación de subredes. Sin ellas, los números de red estarían muy limitados en su uso. Normalmente, cada segmento físico, como Ethernet, *Token Ring* o FDDI, está asociado con uno o más números de red. Si el *subnetting* no estuviera disponible, una red de Clase A de la forma 10.0.0.0 alojaría sólo un segmento físico con unos 16 millones de *hosts*.

Con el uso de máscaras, las redes pueden ser divididas en subredes más pequeñas extendiendo la porción de red de la dirección hacia la porción de *host*. La técnica de *subnetting* proporciona un mayor número de subredes mientras se reduce el número de *hosts* en cada red. En este ejemplo 10.0.0.0 representa la subred cero. El software obsoleto de algunos *routers* no permite la utilización del espacio de direcciones de la subred cero, ni se utiliza

predeterminado en los *routers* Cisco. Con el fin de poder usar las subredes cero en IOS, se debe configurar *ip subnet-zero*.

3.3.2 VLSM

El término máscara de subred de longitud variable (VLSM) hace referencia al hecho de que una red puede configurarse con diferentes máscaras. La idea básica tras las VLSM es ofrecer más flexibilidad al dividir una red en múltiples subredes, a la vez que se optimiza la asignación de cantidades variables de espacio en *host* entre las subredes. Sin VLSM, sólo puede aplicarse una máscara de subred a toda una red. Esto restringiría el número de *hosts* dado el número de subredes requeridas. Si se selecciona la máscara de modo que se tenga suficientes subredes, quizá no se podría asignar suficientes números de *host* en cada subred. Lo mismo es cierto para los *hosts*; una máscara que permite suficientes *hosts* podría no proporcionar suficiente espacio de subred. VLSM proporciona la capacidad de asignar subredes con cantidades variables de *hosts*, permitiendo al administrador de red utilizar mejor el espacio de direcciones.

Aunque la división en subredes ha demostrado ser un valioso añadido a la arquitectura de direccionamiento de Internet, tenía una limitación fundamental que era la de una sola máscara de subred para toda una red. Por lo tanto, después de seleccionar una máscara de subred (lo que dicta el número de *hosts* soportados por cada número de subred) no podían soportarse subredes de un tamaño diferente. Cualquier necesidad de subredes de mayor tamaño significaba que había que cambiar de tamaño significaba que había que cambiar el tamaño de la máscara de subred para toda la red.

VLSM permite un uso más eficaz del espacio de direcciones IP de una organización, permitiendo a los administradores de la red personalizar el tamaño de una máscara de subred para los requisitos específicos de cada

subred. El tamaño de los prefijos de red extendidos puede ser identificado usando una barra inclinada (/) seguida por el número de bits utilizados para el direccionamiento de la red y la subred. Por lo tanto, 193.168.125.0/27 identifica una dirección con Clase C específica, con 27 bits usados para el prefijo de red extendido.

La división en subredes era una solución ideal para un problema apremiante: el rápido agotamiento del finito espacio de direcciones IP. Permitir a las redes privadas redefinir el campo de *host* de una dirección IP en direcciones de subredes y de *host* reduciría mucho la cantidad de direcciones IP desperdiciadas. Desgraciadamente en una configuración real, la necesidad de subredes no es homogénea. No es realista esperar que una organización, o sus redes sean divididas en subcomponentes de tamaño uniforme. Es mucho más probable que haya organizaciones (y subredes) de todos los tamaños. Por lo tanto, utilizar una máscara de subred de longitud fija supondría que se malgastaran direcciones IP de *host* de cada red definida.

La solución a este dilema era permitir que un espacio de direcciones IP fuera dividido en subredes de manera flexible usando máscaras de subred de diferentes tamaños. Esta solución es VLSM. No todos los protocolos de enrutamiento pueden soportar VLSM, RIP-1 e IGRP no transportan máscaras de red en actualizaciones de enrutamiento y, por lo tanto, no pueden tratar correctamente con redes divididas en subredes variablemente. Actualmente, incluso con la aparición de protocolos de enrutamiento tales como OSPF, EIGRP, RIP-2, IS-IS que soportan VLSM, los administradores todavía tienen dificultadas en adaptarse a esta técnica.

3.3.3 Enrutamiento entre dominios sin Clase CIDR

Una adición relativamente reciente a la arquitectura de direcciones IP es CIDR. Nació de la crisis que acompaño al explosivo crecimiento de Internet durante los primeros años 90, el IETF se interesó por la capacidad de Internet para crecer en respuesta a la demanda de su uso. Sus preocupaciones específicas eran:

- El agotamiento de direcciones IPv4 no asignadas. El espacio de Clase B en particular estaba en peligro de extinción.
- El rápido y sustancial aumento de las tablas de enrutamiento de Internet, como resultado de su crecimiento.

El IETF decidió que, para evitar el colapso de Internet, serían necesarias soluciones a corto y largo plazo. A largo plazo, la única solución viable era un IP completamente nuevo, con espacios y arquitecturas de direcciones muy ampliados. Esta solución se llamó IPng (Protocolo Internet de siguiente generación), o más formalmente, IP Versión 6 (IPv6).

Las necesidades a corto plazo eran reducir la tasa de agotamiento de las direcciones no asignadas que quedaban. La respuesta fue eliminar las ineficaces clases de direcciones a favor de una arquitectura de direccionamiento más flexible y el resultado fue CIDR. En 1993, los planes para CIDR se distribuyeron en las RFC 1517, 1518, 1519 y 1520. CIDR tenía tres características claves que tenían un valor incalculable para atajar el agotamiento del espacio de direcciones IPv4. Estas características son las siguientes:

- Eliminación del direccionamiento con clases.
- Adición de rutas mejoradas.
- *Supernetting*.

Direccionamiento sin clase (*classless*). Matemáticamente, el espacio de direcciones IPv4 aún contenía un número sustancial de direcciones disponibles. Desgraciadamente, muchas de estas direcciones potenciales se malgastaban porque estaban encerradas en bloques asignados, o clases de direcciones. Eliminar clases no recuperaría necesariamente las direcciones encerradas en esos espacios de direcciones que ya estaban asignados, pero permitiría un uso mucho más eficaz de las direcciones restantes. Aparentemente, este esfuerzo de tapar los agujeros ganaría el tiempo necesario para que IPv6 fuera desarrollado y desplegado.

Adición de rutas mejoradas. CIDR permite a los *routers* de Internet (o a cualquier *router* compatible con CIDR) agregar de modo más eficaz información de enrutamiento. Una sola entrada de la tabla de enrutamiento puede representar los espacios de direcciones de muchas redes. Esto puede reducir mucho el tamaño de las tablas de enrutamiento necesarias en cualquier *internetwork*, y se traduce directamente en una escalabilidad mayor. CIDR se implementó en Internet de 1994 a 1995, y fue inmediatamente eficaz para contener la expansión de las tablas de enrutamiento de los *routers* de Internet. Es dudoso que Internet hubiera continuado creciendo si no se hubiera implementado CIDR.

Supernetting. Otra ventaja de CIDR es la capacidad de crear superredes, también llamada *supernetting*. La función de *supernetting* no es nada más que usar bloques contiguos de espacios de direcciones de Clase C para simular un solo espacio de direcciones, aunque mayor. Si se dispusiera de las suficientes direcciones contiguas de Clase C, se podría redefinir la adjudicación de bits entre los campos de identificación del *host* y la red y simular una dirección de Clase B. La función de *supernetting* está diseñada para aliviar la presión que sufre el espacio de direcciones de Clase B, que se está agotando rápidamente, ofreciendo una alternativa más flexible.

Funcionamiento de CIDR

CIDR fue una gran ruptura con la tradición, porque abandonó completamente las rígidas clases de direcciones. La arquitectura de direcciones IPv4 original utilizaba un número de red de 8 bits para las direcciones de Clase A, un número de 16 bits para las direcciones de Clase B y un número de 24 bits para las direcciones de Clase C. CIDR reemplazó esas categorías con un prefijo de red más generalizado. Este prefijo podría ser de cualquier longitud, y no sólo de 8, 16 o 24 bits. Esto permitía que CIDR creara espacios de direcciones de acuerdo con el tamaño de una red, en lugar de ajustar a la fuerza las redes a espacios de direcciones de red prefijados. Cada dirección de red compatible con CIDR es publicada con una máscara de bits específica. Esta máscara identifica la longitud del prefijo de red. Por ejemplo, 192.125.61.8/20 identifica una dirección CIDR con una dirección de red de 20 bits.

La dirección IP puede ser cualquier dirección matemáticamente válida, con independencia de si era originalmente parte de un intervalo de Clase A, B, o C. los *routers* compatibles con CIDR toman lo que hay después de la barra inclinada (/) para determinar el número de red.

Una buena a comprensión de la arquitectura de direcciones IP es imprescindible para apreciar los fundamentos del *internetworking* con IP. Los temas como CIDR, el enrutamiento de subredes y VLSM tienen un uso tan generalizado que el no comprenderlos comprometería la capacidad para mantener y diseñar *internetworks*.

3.3.4 NAT

Aún con los métodos mencionados anteriormente para la optimización del uso de las IPs Homologadas o validas en Internet. Para una Empresa/Cliente poseer una dirección IP válida ya no es tan fácil precisamente por el hecho de que la Mayoría ya están asignadas a los *ISPs*, Institutos de Educación o al Gobierno.

Para ello es muy común el uso del mecanismo llamado NAT por sus siglas en Ingles *Network Address Translation*, el cual permite el uso de direcciones IP privadas de manera interna y cuando se requiera salir a Internet se asigne una IP homologada valida en Internet.

Los Mecanismos de NAT son:

- NAT Estático
- NAT Dinámico
- *Overloading* NAT con PAT

NAT Estático se resume al mapeo de direcciones IP uno a uno, es decir una IP privada contra una IP homologada para salir a Internet.

NAT Dinámico es el mapeo de direcciones IP uno a uno de manera dinámica las cuales son tomadas de un *pool* o conjunto definido de direcciones IP de acuerdo a la demanda, y esto es lo que principalmente lo diferencia con el NAT estático.

NAT *Overloading* con PAT, permite la salida a Internet de N IPs privadas usando una IP homologada, para esto hace uso de asignación de puertos virtuales para cada petición hacia Internet.

CAPITULO 4

PRINCIPIOS DE ENRUTAMIENTO

4.1 Definición del enrutamiento

El enrutamiento es un proceso de envío de paquetes en el que los elementos son reenviados de una ubicación a otra. En las redes informáticas, el tráfico generado por el usuario, como el correo electrónico o los documentos gráficos o de texto, es reenviado de un origen lógico a un destino lógico. Cada dispositivo de red posee una dirección lógica, de forma que se es posible contactar con él individualmente. En algunos casos, también se puede conectar con los dispositivos como parte de un grupo más grande de dispositivos.

Para que un *router* actúe como dispositivo de entrega de información efectivo, debe conocer la topología lógica de la red y ser capaz de comunicarse con sus dispositivos vecinos. Un *router* puede configurarse para reconocer varios esquemas distintos de direccionamiento lógico e intercambiar regularmente información sobre la topología con otros dispositivos de la red. El mecanismo de aprender y mantener el conocimiento de la topología de red se considera que es la función de enrutamiento. El movimiento real del tráfico por el *router*, desde una interfaz interna a una externa, constituye una función separada y se le considera la función de *switching*. Un dispositivo de enrutamiento debe llevar a cabo tanto las funciones de enrutamiento como las de *switching* para que sea un dispositivo de entrega efectivo.

4.2 Requisitos del enrutamiento

Un *router* debe conocer tres elementos para poder enrutar:

- El *router* debe determinar si tiene activo el paquete de protocolos.
- El *router* debe conocer la red de destino.
- El *router* debe saber qué interfaz externa constituye la mejor ruta para el destino.

Para que un dispositivo de enrutamiento tome la mejor decisión de enrutamiento, primero debe de entender la dirección de destino lógica. Para que esto ocurra, el paquete de protocolos que utiliza el esquema de direccionamiento lógico debe estar habilitado y activado en el *router* en ese momento. Algunos ejemplos de paquetes de protocolos comunes son TCP/IP, IPX y DECnet. Una vez que el *router* entiende el esquema de direccionamiento, la segunda decisión consiste en determinar si la red de destino lógica es un destino válido en la tabla de enrutamiento actual. Si la red lógica de destino no existe en la tabla de enrutamiento, los dispositivos de enrutamiento podrían estar programados para descartar el paquete y generar un mensaje de error (por ejemplo, un mensaje IP *Internet Control Message Protocol*, ICMP), para notificar el hecho al remitente del evento.

Algunos administradores de redes han logrado reducir el tamaño de las tablas de enrutamiento de sus redes incluyendo únicamente unas cuantas redes de destino y especificando luego una entrada de ruta predeterminada. Si se especifica, se seguirá una ruta predeterminada si la red de destino lógica no se incluye como parte de la tabla de enrutamiento del dispositivo.

La decisión final que debe tomar el dispositivo de enrutamiento si la red de destino está en la tabla de enrutamiento, consiste en determinar a través de qué interfaz externa va a ser reenviado el paquete. La tabla de enrutamiento

sólo contendrá la mejor ruta (o rutas) a cualquier red lógica de destino. La mejor ruta a la red de destino estará asociada con una determinada interfaz externa por el proceso del protocolo de enrutamiento los cuales usan una métrica para determinar la mejor ruta o destino. Una métrica más baja indica una ruta más adecuada; si dos o más rutas tienen una métrica igual de baja, todas esas rutas serán compartidas. A la opción de compartir tráfico de paquetes por múltiples se denomina equilibrado de la carga o balanceo de carga al destino. Cuando se conoce la interfaz externa, el *router* también deberá poder usar un método de encapsulación (un tipo trama Capa 2) al reenviar el paquete al dispositivo lógico de próximo salto de la ruta *relay*.

4.3 Funciones de un *router*

Tan importantes como proporcionar interconectividad física para múltiples redes son las funciones lógicas que realiza un *router*. Estas funciones hacen utilizables las interconexiones físicas. Por ejemplo, las comunicaciones entre redes que al menos una ruta física interconecte las computadoras de origen y destino. Sin embargo, tener y usar una ruta física son muy cosas diferentes. En concreto las computadores de origen y de destino deben hablar un lenguaje común (un protocolo enrutado). También ayuda si los *routers* que residen entre ellas hablan un lenguaje en común (un protocolo de enrutamiento) y están de acuerdo en qué ruta física específica es la mejor a usar. Por tanto, algunas de las funciones más destacadas que proporciona un *router* son:

- Interconectividad física.
- Interconectividad lógica
- Cálculo y mantenimiento de las rutas.
- Seguridad

4.3.1 Interconectividad física

Un *router* tiene un mínimo de dos puertos de E/S físicos o interfaces. que se utilizan para conectar físicamente los servicios de transmisión a un *router*. El administrador de red debe configurar cada interfaz desde la consola del *router*. La configuración incluye definir el número de puerto de la interfaz del *router*, la tecnología de transmisión y el ancho de banda disponible de la red conectada a esa interfaz, y los tipos de protocolos que se utilizarán en esa interfaz. Los parámetros que deben definirse varían en función del tipo de interfaz de red.

4.3.2 Interconectividad lógica

Tan pronto como se configura una interfaz en un *router*, puede activarse. La configuración de la interfaz identifica el tipo de transmisión al que se conecta, la dirección IP de la interfaz, y la dirección de red a la que se conecta. Tras la activación de un puerto, el *router* empieza inmediatamente a monitorizar todos los paquetes que se están transmitiendo por la red conectada al puerto recientemente activado. Esto le permite “aprender” sobre las direcciones IP de red y de *host* que residen en las redes que pueden alcanzarse a través de ese puerto. Estas direcciones se almacenan en unas tablas llamadas tabla de enrutamiento.

Las tablas de enrutamiento correlacionan el número de puerto de cada interfaz del *router* con las direcciones de la capa de red que pueden alcanzarse (directa o indirectamente) a través de ese puerto.

Un *router* también puede configurarse con una ruta predeterminada la cual se asocia a una interfaz específica del *router* con todas las direcciones de destino desconocidas. Esto permite a un *router* enviar un datagrama a destinos que todavía no ha aprendido. Además, las rutas predeterminadas pueden

tener otros usos. Pueden utilizarse para minimizar el crecimiento de las tablas de enrutamiento, por ejemplo, o para reducir la cantidad de tráfico generado entre los *routers* según intercambian información de enrutamiento.

4.3.3 Cálculo y mantenimiento de rutas

Los *routers* se comunican entre sí utilizando un protocolo predeterminado, un protocolo de enrutamiento. Los protocolos de enrutamiento permiten a los *routers* hacer lo siguiente:

- Identificar rutas potenciales a *hosts* y redes de destino específicas.
- Realizar una comparación matemática, conocida como cálculo, para determinar la mejor ruta a cada destino.
- Monitorear continuamente la red para detectar cualesquiera cambios en la topología que pueden representar rutas conocidas que no sean válidas.

Existen muchos tipos diferentes de protocolos de enrutamiento y se pueden clasificar de varias formas, Vector Distancia, Estado Enlace, etc., y algunos como RIP son bastante simples y otros como OSPF son extremadamente poderosos y con muchas características, pero complicados. Los protocolos de enrutamiento se pueden evaluar usando numerosos criterios más específicos, no sólo los métodos que usan. Algunos de los más significativos son:

- **Optimización.** Describe la capacidad de un protocolo de enrutamiento para seleccionar la mejor ruta disponible. Hay muchos modos diferentes de evaluar diferentes rutas a cualquier destino dado. Cada modo podría deparar la selección de una ruta “mejor” dependiendo de los criterios usados. Los criterios usados por los protocolos de enrutamiento para calcular y evaluar las rutas se conocen como métricas de enrutamiento.

Hay una amplia variedad de métricas, y varían ampliamente de un protocolo de enrutamiento a otro.

- **Eficacia.** Otro criterio a considerar cuando se evalúan los protocolos de enrutamiento es su eficacia operativa. La eficacia operativa puede medirse examinando los recursos físicos, incluyendo la RAM del *router* y el reloj del CPU, y el ancho de banda de red requerido por un protocolo de enrutamiento dado. Puede que sea necesario consultar el fabricante o distribuidor del *router* para determinar las eficacias relativas de los protocolos que se esta considerando.
- **Robustez.** Un protocolo de enrutamiento debería rendir eficazmente en todas las ocasiones, no sólo cuando la red es estable. Las condiciones de error, incluyendo los fallos del hardware o del servicio de transmisión, los errores en la configuración del *router* e incluso unas cargas de tráfico fuertes, afectan negativamente a una red. Por tanto, es vital que un protocolo de enrutamiento funcione adecuadamente durante los periodos de fallo y/o inestabilidad de la red.
- **Convergencia.** Como son dispositivos inteligentes, los *routers* pueden detectar automáticamente cambios en la *internetwork*. Cuando se detecta un cambio, todos los *routers* implicados deben converger en un nuevo acuerdo sobre la forma de la red y recalcular consecuentemente sus rutas a los destinos conocidos. Este proceso de acuerdo mutuo se le llama convergencia. Cada protocolo de enrutamiento utiliza diferentes mecanismos para detectar y comunicar los cambios que se producen en la red. Por tanto, cada uno converge en una porción diferente. En general, cuanto más despacio converge un protocolo de enrutamiento, mayor es la posibilidad de desestabilizar el servicio en la *internetwork*.
- **Escalabilidad.** Es la capacidad de crecimiento de una red. Aunque el crecimiento no es algo necesario en todas las organizaciones, el protocolo de enrutamiento seleccionado debe ser capaz de crecer para alcanzar el crecimiento proyectado de la red.

4.3.4 Seguridad

La seguridad está entre muchas funciones lógicas de un *router*. Asegurar una red que utiliza un protocolo intencionalmente abierto, como IP, no es una empresa fácil. El tipo de seguridad que puede proporcionar un *router* está basado en los permisos de acceso. Los permisos se pueden definir explícitamente para cada puerto del *router*. La lista de permisos se conoce como lista de control de acceso ACL.

4.4 Funciones del *router* en las WAN

Las *internetworks* son bastante extensas en términos de número de *routers*, servicios de transmisión y sistemas finales conectados. En una *internetwork* extensa, como Internet e incluso grandes redes privadas, sería virtualmente imposible para cualquier computadora dada saber de todas y cada una de las otras computadoras. Por tanto, es necesario algo parecido a una jerarquía. La organización jerárquica de las computadoras interconectadas crea la necesidad de funciones de enrutamiento especializadas. Los *routers* pueden especializarse en aprender y distribuir información de enrutamiento sobre los sistemas finales que hay dentro de su dominio. Estos *routers* se llaman *gateways* interiores. Alternativamente, los *routers* pueden especializarse en recopilar información de enrutamiento sobre las computadoras que hay más allá de su dominio. Estos *routers* se conocen como *gateways* exteriores.

El *networking* se utiliza a menudo como un término genérico o universal. Sin embargo, las computadoras interconectadas se comunican de modos muy diferentes. Los *routers* pueden funcionar con distinto rendimiento en una *internetwork*; por ejemplo, como *routers* interiores, exteriores o fronterizos. No es extraño encontrar *routers* interiores, exteriores y fronterizos descritos como

gateway interiores, exteriores y fronterizos respectivamente. El término *gateways* es tan antiguo como el enrutamiento. Con el tiempo este término ha perdido algo de su valor descriptivo. En consecuencia, ambos conjuntos de términos son técnicamente correctos. Muchos protocolos de enrutamiento fueron específicamente diseñados para desempeñar uno de estos roles. Más adelante se describirán algunos de los protocolos de enrutamiento especializados más utilizados.

Comprender las diferencias entre ellos requiere examinarlos en el contexto de una WAN. Los términos WAN, red, *internetwork* y sistema autónomo se utilizan todos de forma intercambiable, aunque cada uno tiene un significado ligeramente distinto:

- **WAN.** Una WAN es una colección de LAN relacionadas enlazadas mediante *routers* y servicios de transmisión en serie, como por ejemplo, líneas dedicadas o circuitos *Frame Relay* en esta definición está implícito que las LAN de una WAN pueden estar geográficamente dispersas, pero todavía bajo los auspicios de una sola organización, como una empresa, una universidad, etc.
- **Red.** Todo lo que va de las LAN a las WAN puede clasificarse como una red. En consecuencia una red identifica una colección genérica de mecanismos de *networking* relacionados. Por tanto una red puede ser una LAN o una WAN, pero debe de pertenecer aun sola organización y presentar una arquitectura de direccionamiento coherente.
- ***Internetwork.*** Una *internetwork* es un conjunto de redes ligeramente relacionadas, que están interconectadas. Las redes interconectadas pueden pertenecer a diferentes organizaciones. Por ejemplo, dos compañías pueden utilizar Internet para interconectar sus WAN privadas, la *Internetwork* resultante estaría formada por una red pública y dos privadas enlazadas conjuntamente.

- **Sistema Autónomo.** Un sistema autónomo (AS) es una red (LAN o WAN) relativa. Está administrado por una solo persona (o grupo de personas), presenta un protocolo enrutado único, una arquitectura de direcciones y generalmente sólo un protocolo de enrutamiento. Un sistema autónomo puede soportar conexiones con otros sistemas autónomos propiedad de la misma organización y operados por ella. Alternativamente, un AS puede tener conexiones con otras redes, como Internet, aunque mantiene su autonomía operativa.

Dadas estas definiciones, es posible definir mejor las clases funcionales de *routers*. Un *router* interior es el que puede ser usado por los sistemas finales de una red para acceder a otros sistemas finales dentro de la misma red. El *router* interior no soporta conexiones con ninguna otra red. La figura 4.1 ilustra una pequeña red e identifica aquellos dispositivos que funcionan como *routers* interiores.

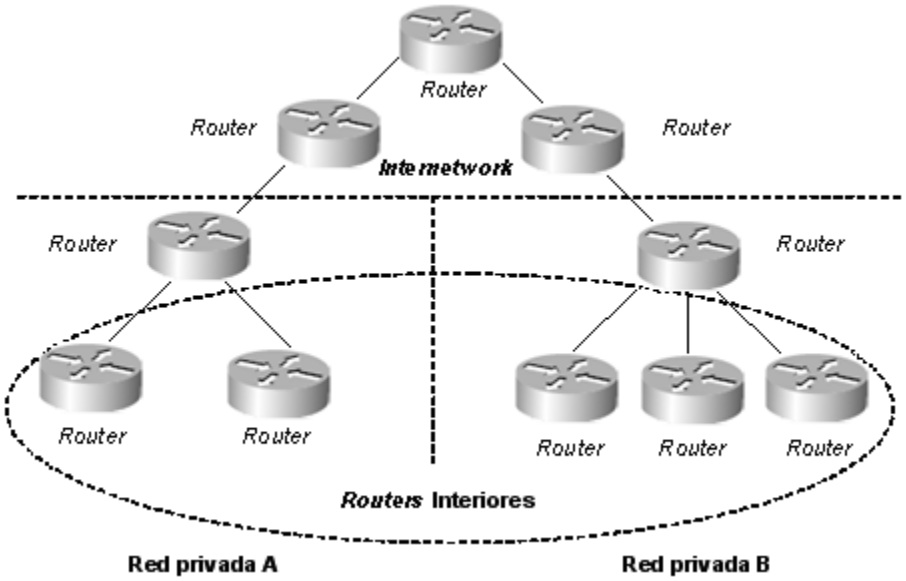

Figura 4.1. *Routers* interiores de una red.

Un *router* exterior es el que se halla más allá de los límites de cualquier red dada. La figura 4.2, aunque no pretende describir la topología real de

Internet, presenta una topología simplificada de Internet que solamente intenta demostrar lo que es un *router* exterior.

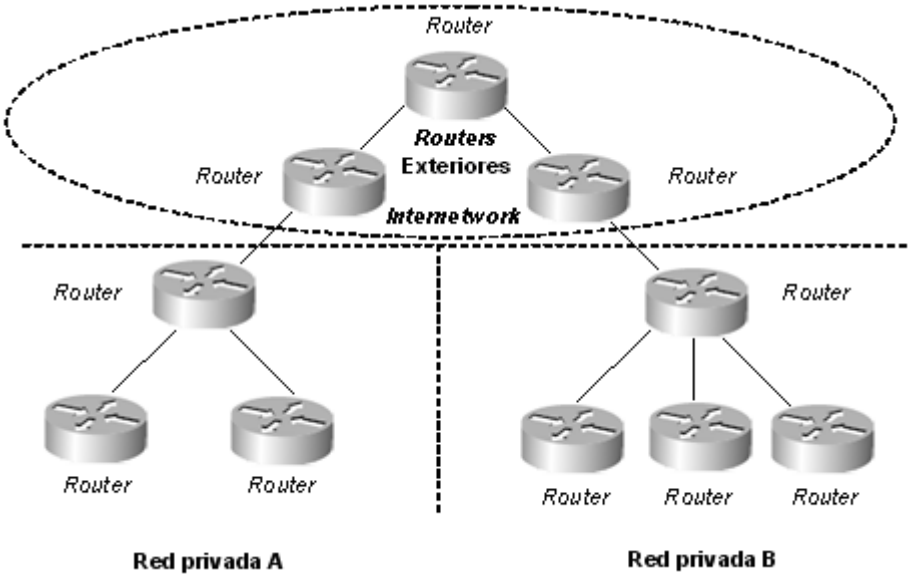

Figura 4.2. *Routers* exteriores desde la perspectiva de las redes privadas.

La última clase funcional de *routers* es el *router* fronterizo. Los *routers* fronterizos interconectan una red con otras. Es importante observar que una sola entidad puede poseer múltiples sistemas autónomos y operar con ellos. Por tanto un *router* fronterizo puede detonar el límite entre do sistemas autónomos, más que el límite lo sea entre una red privada y alguna otra red.

La figura 4.3 identifica los *routers* fronterizos en la red de ejemplo que se ha utilizado en las figuras anteriores.

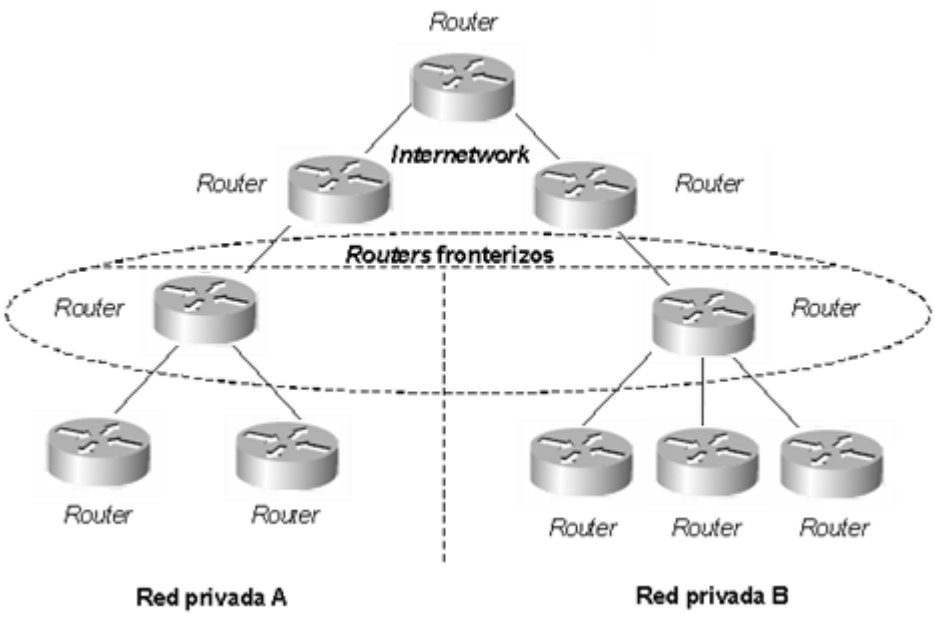

Figura 4.3. Los *routers* fronterizos desde la perspectiva de las redes privadas.

4.5 Escenarios de *Inrternetworking*

Cada caso muestra algunos de los temas que deben tenerse en cuenta en cualquier red o *internetwork*:

- Enrutamiento dentro de una red.
- Enrutamiento entre redes adyacentes.
- Enrutamiento entre redes no adyacentes.

Estos tres aspectos genéricos comprenden virtualmente cada forma de *internetworking* que probablemente existe. Cada uno tiene diferentes implicaciones para el administrador de redes, incluyendo aspectos de enrutamiento tales como el cálculo y la distribución de las rutas, la convergencia y la seguridad.

4.5.1 Enrutamiento dentro de una red

La forma más simple de enrutamiento dentro de los confines de una sola red que se compone sólo de *routers* interiores. En teoría, esta forma de red utilizaría solo un protocolo enrutado, una arquitectura de direcciones y un número mínimo de destinos. Esto reduciría en gran medida la carga de trabajo de cada *router*, y maximizaría el rendimiento potencial de la red. Por tanto, los problemas de enrutamiento en una *internetwork* están más estrechamente relacionados con el tamaño y la topología de la red que con sus arquitecturas de direcciones y sus protocolos de enrutamiento.

Si la red fuera lo suficientemente pequeña, sería posible para el administrador preprogramar estáticamente todas las rutas posibles en lugar de introducir la complejidad de un protocolo de enrutamiento dinámico. Sin embargo las rutas programadas estáticamente pueden convertirse en una carga pesada para una red en crecimiento o que sufre cambios constantemente.

4.5.2 Enrutamiento entre redes adyacentes

Un pequeño paso adelante en la complejidad que implica el enrutamiento dentro de una red es el enrutamiento "*internetwork*" entre dos redes adyacentes. La adyacencia física significa que las dos redes están directamente conectadas entre sí. Dicha adyacencia pudo haber sido diseñada para promocionar una rápida convergencia, mejorar la seguridad o satisfacer cualquier otro criterio relacionado con el rendimiento.

La separación lógica de múltiples redes implica que los *routers* fronterizos que haya entre ellos deben resumir y redistribuir la información de enrutamiento entre sí. De este modo los sistemas finales de una red pueden direccional directamente los sistemas finales de otra red. La figura 4.4 ilustra este tipo de enrutamiento.

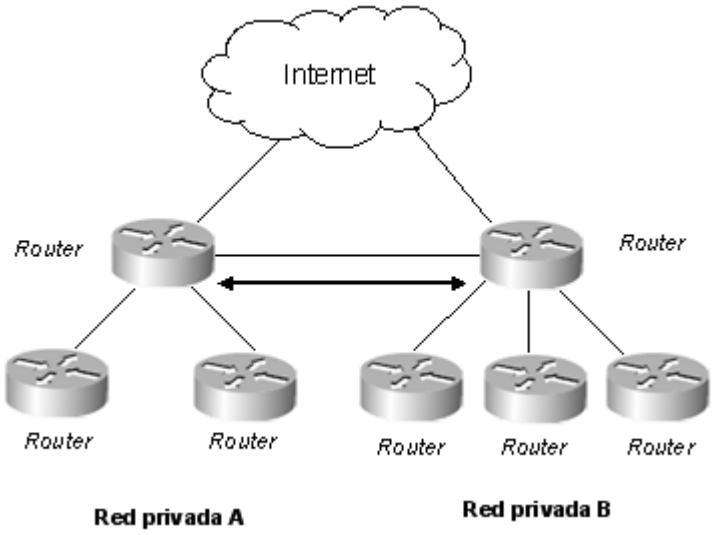

Figura 4.4 Enrutamiento entre redes adyacentes.

La topología puede afectar el enrutamiento entre redes adyacentes. Usar un solo punto de interconexión entre las dos redes, por ejemplo, facilita el control del cálculo y la redistribución de la información de enrutamiento entre las redes. Sin embargo, esta característica introduce un único punto de falla, lo que podría no ser aceptable para sus usuarios. Introduciendo un segundo (o más) punto de interconexión se resuelve el problema del único punto de falla, pero puede introducir la posibilidad de que se produzcan infinitos ciclos (*loops*) de enrutamiento. Resolver tal problema requiere conocer la tolerancia de los usuarios frente a las dificultades y el riesgo. Ya con este conocimiento, se puede evaluar los protocolos de enrutamiento específicos para que las capacidades converjan rápidamente y compensen los potenciales problemas de enrutamiento.

4.5.3 Enrutamiento entre redes no adyacentes

El enrutamiento entre redes no adyacentes es, simultáneamente, el tipo de enrutamiento más complicado y el más útil. Las dos redes pueden utilizar una tercera red como intermediaría. Es altamente probable que las dos redes,

distintas, utilicen protocolos de enrutamiento, protocolos enrutados y arquitecturas de direcciones distintas. Por tanto, la tarea del *router* fronterizo es superar esos obstáculos a la comunicación al tiempo que proteger el límite de la red. En la figura 4.5 ilustra el enrutamiento entre pequeñas redes no adyacentes.

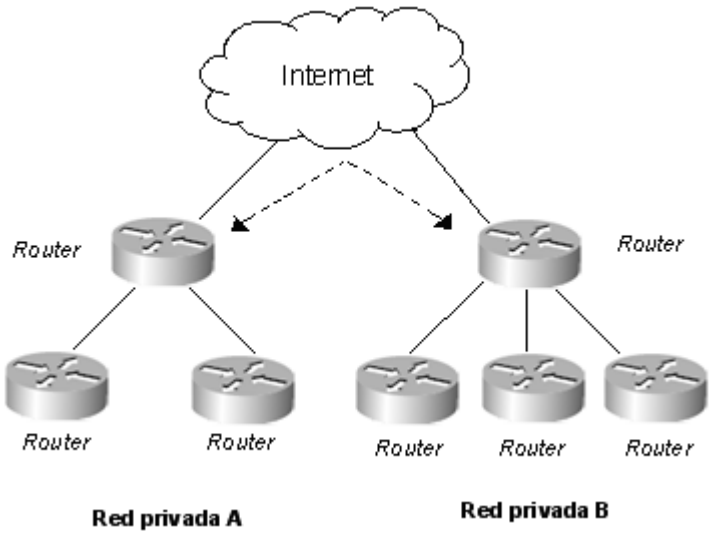

Figura 4.5. Enrutamiento entre redes no adyacentes.

El *router* fronterizo de cada red privada de esta ilustración necesita proteger el límite de su red de intrusiones no deseadas. Dado que las redes que necesitan comunicarse no son adyacentes, y que la red intermediaria está fuera de control, los riesgos de una intrusión no deseada son mucho más altos que si estuvieran directamente conectadas. Por tanto, los administradores de redes deben desarrollar un conjunto de criterios para permitir a usuarios externos específicos el acceso a la red, y no permitírselo a nadie más. El *router* fronterizo puede implementar estos criterios mediante una ACL. Otra responsabilidad del *router* fronterizo sería resumir las rutas internas y redistribuir la información a las redes externas. Esto permite a los usuarios externos al límite de la red privada acceder a los sistemas finales. Si esta información de enrutamiento no se redistribuyera, nadie fuera de esa red privada podría acceder a los sistemas

finales, es muy probable que los *routers* fronterizos tengan que configurarse para usar múltiples protocolos de enrutamiento.

4.6 Criterios de rendimiento de una WAN

Habiendo revisado algunos de los distintos modos de construir redes utilizando *routers*, también es importante establecer algunos criterios para medir la eficacia de una red. Pueden aplicarse muchos criterios o medidas diferentes. Algunos de éstos pueden extraerse automáticamente partir de los protocolos nativos de la monitorización de redes y, virtualmente, a partir de cualquier dispositivo de red. Otros son subjetivos y puede ser poco menos que imposible determinarlos por adelantado. Algunas de las medidas más comunes son las siguientes:

- Tiempo operativo de los componentes (un promedio de tiempo estimado entre fallas MTBF, estadísticas de disponibilidad).
- Volúmenes de tráfico (tráfico máximo, promedios, picos)
- Retraso.
- Proporciones de utilización de recursos (CPU, Memoria, Servicios de transmisión)

4.7 Información sobre enrutamiento

La información necesaria para llevar a cabo la operación de enrutamiento se incluye en la tabla de enrutamiento del *router*, y es generada por uno o más procesos del protocolo de enrutamiento. La tabla de enrutamiento se compone de múltiples entradas, y cada una de ellas indica lo siguiente:

- El mecanismo en virtud del cual se conoció la ruta. Los métodos de aprendizaje pueden ser dinámicos o manuales.
- El destino lógico, bien una red principal o una subred de una red principal. En casos aislados, puede haber direcciones de *host* en la tabla de enrutamiento.
- La distancia administrativa, es una medida de la fiabilidad que supone el mecanismo de aprendizaje.
- La métrica, que es una medida de “coste añadido” de la ruta, en virtud de lo que define el protocolo de enrutamiento.
- La dirección del dispositivo del próximo salto (*router*) en la ruta hacia el destino.
- Lo actualizada que está la información sobre la ruta. Este campo indica el tiempo que ha estado la información en la tabla de enrutamiento desde la última actualización. Dependiendo del protocolo de enrutamiento que se esté utilizando, la información de introducción de ruta puede ser actualizada de forma periódica para garantizar que está actualizada.
- La interfaz encargada de alcanzar la red de destino. Es el puerto a través del cual el paquete abandona al *router* y se reenvía al siguiente dispositivo de próximo salto.

4.7.1 Distancia administrativa.

El proceso de enrutamiento es el responsable de seleccionar la mejor ruta o cualquier red de destino. Dado que puede haber más de un mecanismo de aprendizaje en un *router* en un momento dado, es necesario que haya un método para elegir entre distintas rutas cuando se conoce la misma ruta desde múltiples orígenes. En el caso de IP en un *router* Cisco, el concepto de distancia administrativa se utiliza como método de selección para los protocolos de enrutamiento IP, se utiliza como medida de la confiabilidad del origen de la información de enrutamiento IP. Sólo es importante cuando un

router conoce una ruta a un destino desde más de un origen. Es mejor que haya valores bajos en la distancia administrativa que valores altos, por regla general, las distancias administrativas predeterminadas han sido asignadas con una preferencia por las entradas manuales sobre las entradas conocidas dinámicamente, y los protocolos de enrutamiento con una métrica más sofisticada sobre los que tienen una métrica más sencilla. En la tabla 4.1 se presenta un esquema comparativo de las distancias administrativas predeterminadas.

Origen de la ruta	**Distancia Administrativa predeterminada**
Interfaz conectada	0
Ruta estática fuera de una interfaz	0
Ruta estática de un próximo salto	1
Ruta de resumen EIGRP	5
BGP externa	20
EIGRP interna	90
IGRP	100
OSPF	110
IS-IS	115
RIP (v1 y v2)	120
EGP	140
EIGRP externa	170
BGP interna	200
Desconocido	255

Tabla 4.1. Distancias administrativas predeterminadas de orígenes de rutas.

4.7.2 Métrica de enrutamiento.

En una red enrutada, el proceso de enrutamiento se apoya en el protocolo de enrutamiento para mantener una topología libre de *loops* y para localizar la mejor ruta a cada red de destino.

La definición de cuál es la mejor ruta a cualquier ruta es una característica que diferencia a los distintos protocolos de enrutamiento. Cada protocolo de enrutamiento utiliza una medida diferente. Los *routers* publican la ruta a una red en términos de valor métrico. Algunos ejemplos habituales de métricas son la cuenta de salto (el número de *routers* que hay que atravesar), el coste (en base al ancho de banda), y un valor compuesto (utilizando varios parámetros en el cálculo). Si la red de destino no es local a un *router* la ruta se representará por la suma de los valores métricos que se definan en todos los enlaces que deben ser atravesados desde el *router* para alcanzar esa red. Cuando el proceso de enrutamiento conoce los valores métricos asociados con las distintas rutas (presuponiendo que existen múltiples rutas), entonces se puede tomar la decisión de enrutamiento. El proceso de enrutamiento selecciona la ruta que tenga valor métrico más bajo. En *routers* Cisco, si hay múltiples rutas bajo métricas iguales en un entorno IP, existirá la opción de compartir la carga entre las distintas rutas.

En esta sección se documenta el modo de operar y describe los dos tipos principales de enrutamiento: el estático y el dinámico. De estos dos solo el dinámico usa protocolos de enrutamiento. Como consecuencia, el enrutamiento dinámico es mucho más poderoso y complejo. Los protocolos de enrutamiento dinámico son la tecnología que permite a los *routers* realizar algunas de sus funciones más vitales. Esto incluye descubrir y mantener rutas, así como converger en un acuerdo sobre la topología de una red.

4.8 Tipos de Enrutamiento.

Los *routers* pueden enrutar de dos modos básicos. Pueden utilizar rutas estáticas preprogramadas, o pueden calcular rutas dinámicamente utilizando cualquiera de los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento dinámicos son usados por los *routers* para descubrir rutas. Los *routers* programados estáticamente no pueden descubrir rutas; carecen de

cualquier mecanismo para comunicar la información de enrutamiento a otros *routers*. Los *routers* programados estáticamente solo pueden enviar paquetes usando rutas definidas por un administrador de redes.

Además de la programación estática de las rutas, hay tres categorías de protocolos de enrutamiento dinámico:

- Vector de distancia
- Estado del enlace
- Híbridos

Las diferencias principales entre estos tipos de protocolos de enrutamiento dinámico residen en el modo en que descubren y calculan nuevas rutas a los destinos.

4.8.1 Dos Tipos de protocolos de enrutamiento dinámico.

Los protocolos de enrutamiento pueden clasificarse de muchos modos, incluso por muchas de sus características operativas, como su campo de acción, el número de rutas soportadas a cada destino redundante, etc. En esta sección se clasifican por el modo en que descubren y calculan sus rutas. Sin embargo, es útil hacer referencia a los protocolos de enrutamiento por su campo de acción. En otras palabras, dividirlos en categorías según el papel que desempeñan en una *internetwork*. Hay dos clases funcionales de protocolos de enrutamiento dinámico: los protocolos de *gateway* interior (IGP) y los protocolos de *gateway* exterior (EGP).

Quizá el modo más sencillo de explicar esto es que los IGP se utilizan dentro de sistemas autónomos, como, por ejemplo, las intranets, mientras que los EGP se utilizan entre sistemas autónomos. En consecuencia el protocolo de *gateway* fronterizo (BGP, un EGP) es el protocolo utilizado para calcular rutas a

través de Internet. Internet desde la perspectiva del enrutamiento, no es más que un *backbone* de transporte para un colección global de sistemas autónomos de propiedad y operación privadas.

4.8.2 Enrutamiento Estático.

La forma más simple de enrutamiento son las rutas preprogramadas, y en consecuencia, estáticas. La tarea de descubrir rutas y propagarlas a través de una red se deja al administrador del *internetwork*. Un *router* programado para el enrutamiento estático envía paquetes a través de Interfaces predeterminadas. Una vez configurada la relación entre una dirección de destino y un puerto del *router*, ya no hay necesidad de que los *routers* intenten descubrir la ruta e incluso comunicar la información sobre rutas.

Ventajas enrutamiento estático. Por ejemplo, las rutas programadas estáticamente pueden hacer más segura la red. Sólo puede haber un camino dentro y fuera de una red conectada con una red definida estáticamente. Esto es así, por supuesto a no ser que estén definidas múltiples rutas estáticas. Otra ventaja es que el enrutamiento estático es un recurso mucho más eficaz. El enrutamiento estático utiliza mucho menos ancho de banda de los servicios de transmisión, no gasta ningún ciclo de la CPU del *router* intentando calcular rutas, y necesita mucho menos memoria. En algunas redes tal vez sea posible utilizar *routers* más pequeños, más baratos, empleando rutas estáticas. A pesar de estas ventajas, se debe ser consciente de algunas limitaciones inherentes al enrutamiento estático.

Desventajas de enrutamiento estático. Se puede mencionar que en el caso de un fallo en la red, u otro cambio en la topología original, es responsabilidad del administrador de la red ajustar manualmente el cambio. Ya que cuando exista una falla dará lugar a que haya destinos inalcanzables a

pesar del hecho de que pueda o de que haya una ruta alternativa disponible para ser utilizada.

Para que sirve una ruta estática. Es bueno sólo para redes muy pequeñas que sólo tienen una ruta a cualquier destino concreto. En tales casos, el enrutamiento estático puede ser el mecanismo de enrutamiento más eficaz, porque no consume ancho de banda intentando descubrir rutas o comunicarse con otros *routers*.Según se hacen mayores las redes y añaden rutas redundantes a los destinos, el enrutamiento estático se convierte en una responsabilidad con mucha actividad. Cualquier cambio en la disponibilidad de los *routers* o los servicios de transmisión de la WAN deben descubrirse manualmente y programarse. Las WAN con topologías más complejas y que ofrecen múltiples rutas potenciales, requieren absolutamente enrutamiento dinámico. Los intentos de usar enrutamiento estático en WAN complejas de múltiples rutas, acabarán con el propósito de tener esa redundancia de rutas.

En ocasiones son deseables las rutas definidas estáticamente, incluso en redes grandes o complejas. Las rutas estáticas pueden configurarse para mejorar la seguridad. La conexión a Internet de una compañía podría tener una ruta definida estáticamente a un servidor de seguridad. No sería posible ninguna entrada sin haber pasado primero los mecanismos de autentificación que proporciona el servidor de seguridad.

4.8.3 Enrutamiento por vector distancia

Este enrutamiento basado en los algoritmos de vector distancia, algunas veces llamados también algoritmos de Bellman-Ford, los cuales transmiten periódicamente copias de sus tablas de enrutamiento a sus vecinos de red inmediatos. Cada receptor agrega un vector de distancia (es decir, su propio “valor” de distancia) a la tabla y lo envía a su vecinos inmediatos. Este proceso se produce de un modo omnidireccional entre los *routers* que son vecinos

inmediatos. Este proceso paso a paso hace que cada *router* aprenda sobre otros *routers* y desarrolle una perspectiva acumulativa a las “distancias” de la red. La tabla acumulativa se utiliza entonces para actualizar las tablas de enrutamiento de los *routers*. Una vez completa, cada *router* ha aprendido una vaga información sobre las “distancias” a los recursos conectados a la red. No aprende nada específico sobre otros *routers* o la topología real de la red.

Desventajas del enrutamiento por vector distancia. En ciertas circunstancias, puede crear realmente problemas de enrutamiento. Una falla o cualquier otro cambio en la red implicará algún tiempo para que los *routers* converjan en un nuevo entendimiento de la topología de la red. Durante el proceso de convergencia, la red puede ser vulnerable al enrutamiento incoherente, e incluso los *loops* infinitos. Las protecciones pueden contener muchos de estos riesgos, pero queda el hecho de que el rendimiento de las red está en riesgo durante el proceso de convergencia. Los más antiguos protocolos de vector distancia que resultan lentos para converger pueden no ser apropiados para WAN grandes y complejas e incluso en redes pequeñas, pueden ser problemáticos en el peor de los casos, o por debajo de lo óptimo en el mejor de los casos. Esto se debe a que la sencillez, que es el punto fuerte, también puede ser una fuente de debilidad.

En cualquier *internetwork* con rutas redundantes, es mejor utilizar un protocolo de vector distancia que rutas estáticas. Esto se debe a que los protocolos de enrutamiento por vector distancia pueden detectar y corregir automáticamente fallas de la red, pero no son perfectos. Si todas las variables de la red se mantuvieron constantes (incluyendo aspectos como niveles de tráfico, el ancho de banda de cada enlace e, incluso, la tecnología de transmisión), la ruta más corta geográficamente produciría la menor cantidad de retraso en la propagación. Por tanto, la lógica indica tomar la ruta más corta. En realidad, dicha lógica está más allá de las capacidades de los simples protocolos de vector de distancia. Estos protocolos no están exactamente

limitados por esto, porque el retraso en la propagación es a menudo al menos significativo de los factores que inciden en el rendimiento de una ruta. El ancho de banda y los niveles de tráfico pueden ambos tener afectos más considerables sobre el rendimiento de una red.

Funcionamiento del vector de distancia

Las actualizaciones periódicas y rutinarias del enrutamiento que generan la mayoría de los protocolos de enrutamiento por vector distancia sólo se dirigen a los dispositivos de enrutamiento que estén conectados directamente. El direccionamiento que suelen usar los dispositivos de que envían las actualizaciones es una difusión lógica, aunque, en algunos casos, se puede especificar actualizaciones unidifusión (*unicast*). En un entorno de vector distancia puro, la actualización del enrutamiento incluye una tabla de enrutamiento completa, como se observa en la figura 4.6 cuando un *router* recibe una tabla completa de un vecino, puede verificar todas las rutas conocidas y luego realizar cambios en la tabla local en base a la información actualizada recibida; este proceso es fácil de entender. La comprensión por parte de un *router* de la red se basa en la perspectiva que tiene el vecino sobre la topología de red; por tanto, el planteamiento del vector distancia suele denominarse “enrutamiento por rumor”.

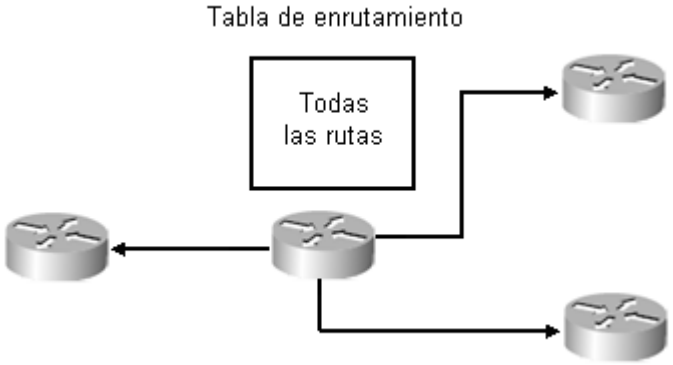

Figura 4.6. Los protocolos de enrutamiento por vector distancia envían toda su tabla de enrutamiento.

El Cisco IOS soporta varios protocolos de vector distancia, entre los que se incluyen RIPv1, RIPv2 e IGRP. Los *routers* Cisco también soportan EIGRP, un protocolo avanzado de vector distancia. Tradicionalmente, los protocolos de vector distancia, también eran protocolos con clase. RIPv2 y EIGRP constituyen ejemplos de protocolos de vector distancia más avanzados que exhiben un comportamiento sin clase.

Los protocolos de red suelen estar asociados con la capa de red de un conjunto de protocolos. Sin embargo, los protocolos de enrutamiento utilizan el mecanismo de envío de capa de red para intercambiar información de enrutamiento, pero el proceso de protocolo de enrutamiento, en sí mismo, no existe en la capa de red. La figura 4.7 muestra la ubicación de los protocolos de enrutamiento por vector distancia IP que hay en el modelo de referencia OSI.

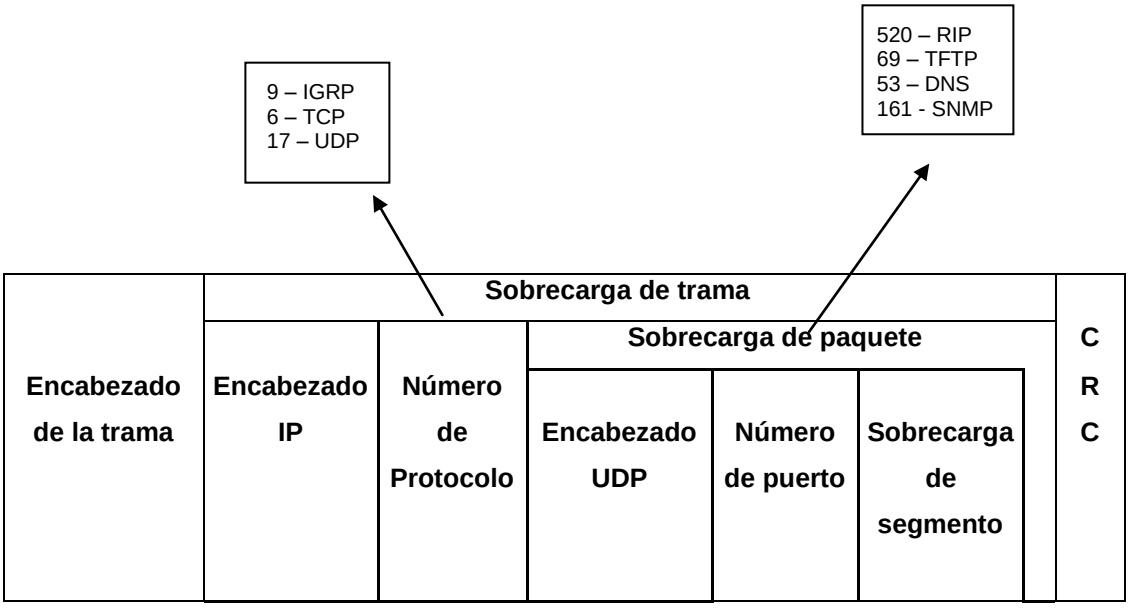

Figura 4.7. El tráfico del enrutamiento por vector de distancia se lleva a cabo en paquetes IP.

En la figura 4.7, IGRP reside en la capa de transporte, como protocolo 9. Otros números de protocolo reconocibles son el 6 y el 17, respectivamente, para TCP y UDP. RIP reside en la capa de aplicación y posee un número de

puerto UDP de 520. La tabla 4.2 compara las características de los distintos protocolos de enrutamiento por vector de distancia soportados en los *routers* Cisco.

Característica	**RIPv1**	**RIPv2**	**IGRP**	**EIGRP**
Cuenta a Infinito	X	X	X	
Horizonte dividido	X	X	X	X
Temporizador de espera	X	X	X	
Actualizaciones con ruta *poisoning*	X	X	X	X
Equilibrado de la carga-rutas iguales	X	X	X	X
Equilibrado de la carga-rutas desiguales		X	X	X
Soporte VLSM		X		X
Algoritmo de enrutamiento	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL
Métrica	Saltos	Saltos	Compuesta	Compuesta
Límite de la cuenta de salto	15	15	100	100
Escalabilidad	Pequeña	Pequeña	Mediana	Grande

Tabla 4.2. Comparación de los protocolos de enrutamiento por vector distancia IP de Cisco.

Para qué sirve el enrutamiento por vector distancia. En general, los protocolos de vector distancia son muy simples y fáciles de configurar, mantener y utilizar. En consecuencia, son bastante útiles en redes muy pequeñas que tienen pocas rutas redundantes, si tienen alguna, y no tienen requisitos restrictivos en cuanto a rendimiento de la red.

4.8.4 Enrutamiento por estado del enlace

Los algoritmos de enrutamiento por estado del enlace, más conocidos como protocolos “primero la ruta más corta” ó por las siglas en Inglés *Short Path First (SPF)*, mantienen una base de datos compleja de la topología de la red. A diferencia de los protocolos de vector distancia, los protocolos de estado

del enlace desarrollan y mantienen un conocimiento completo de los *routers* de la red, así como del modo en que se interconectan. Esto se consigue mediante el intercambio de “publicaciones del estado del enlace” (LSA) con otros *routers* de una red. Cada *router* que ha Intercambiado LSA construye una base de datos topológica usando todas las LSA recibidas. Se utiliza entonces un algoritmo SPF para computar la accesibilidad a los destinos de red. Esta información se usa para actualizar la tabla de enrutamiento.

Este proceso puede descubrir cambios en la topología de la red causados por el fallo de un componente o el crecimiento de la red. De hecho el intercambio de LSA es disparado por un evento de la red, el lugar de ejecutarse periódicamente. Esto puede liberar mucho el proceso de convergencia, porque no hay necesidad de esperar a que expiren una serie de controles temporales arbitrarios para que los *routers* de la red puedan empezar a converger.

Desventajas del enrutamiento por estado del enlace. A pesar de todas sus características y de su flexibilidad, el enrutamiento por estado del enlace despierta dos riesgos potenciales:

- Durante el proceso de descubrimiento inicial, los protocolos de enrutamiento por estado del enlace pueden inundar los servicios de transmisión de la red y, por lo tanto reducir significativamente la capacidad de la red para transportar datos. Esta degradación del rendimiento es temporal, pero puede ser muy notable. Que este proceso de inundación impida de forma notable el rendimiento de una red va a depender de dos cosas: la cantidad de ancho de banda disponible y el número de *routers* que deben de intercambiar la información de enrutamiento.
- El enrutamiento por el estado del enlace es muy intensivo en cuanto a memoria y procesador. En consecuencia, se necesitan *routers* más completamente configurados para soportar el enrutamiento por estado

del enlace que en el caso del enrutamiento por vector distancia. Esto aumenta el coste de los *routers* configurados para un enrutamiento por estado del enlace.

Difícilmente estos riesgos son fatales en el método de enrutamiento por estado del enlace. Los impactos en el rendimiento de ambos pueden manipularse y resolverse con previsión, planificación y administración.

Para que sirve el enrutamiento por estado del enlace. Puede ser bastante útil en redes de cualquier tamaño. En una red bien diseñada, un protocolo de enrutamiento por estado del enlace permitirá a la red sortear con facilidad los efectos de un cambio topológico inesperado. El uso de eventos, como los cambios, para controlar las actualizaciones (en lugar de temporizadores de intervalos fijos) permite que la convergencia empiece mucho más rápidamente después de un cambio en la topología. También se evitan los excesos de consumo de las actualizaciones frecuentes, controladas por el tiempo, de un protocolo de enrutamiento por vector distancia. Esto permite utilizar más ancho de banda para el tráfico de enrutamiento en lugar de hacerlo para el mantenimiento de la red, siempre que se haya diseñado adecuadamente la red.

Una ventaja añadida de la eficiencia del ancho de banda de los protocolos de enrutamiento por estado del enlace es que facilitan la escalabilidad de la red más que las rutas estáticas o los protocolos de vector distancia. En unión con sus limitaciones, es fácil ver que el enrutamiento por estado del enlace es mejor en redes mayores, más complejas, o en redes que deben ser altamente escalables. Puede ser un reto configurar inicialmente un protocolo de estado del enlace en una red grande, pero a la larga el esfuerzo bien merece la pena.

Funcionamiento del estado enlace

Los protocolos por enrutamiento por estado de enlace sólo generan actualizaciones cuando hay un cambio en la topología. Cuando un enlace cambia de estado, el dispositivo que detecta el cambio creará una publicación del estado de enlace (LSA) que concierna a ese enlace (ruta); luego la LSA se propaga a todos los dispositivos vecinos que utilicen una dirección de multidifusión especial. Cada dispositivo de enrutamiento toma una copia de la LSA, la reenvía a todos los vecinos (este proceso se denomina *flooding*, o técnica de inundación), y luego actualiza la base de datos de topología (una tabla que contiene toda la información sobre el estado de enlace de la red). Esta inundación de la LSA es necesaria para garantizar que todos los dispositivos de enrutamiento conozcan el cambio con el fin de poder así actualizar sus bases de datos y crear una tabla de enrutamiento que refleje la nueva topología.

La mayoría de los protocolos de estado de enlace requieren de un diseño jerárquico. El planteamiento jerárquico, como la creación de múltiples áreas lógicas en OSPF, reduce la necesidad de inundar una LSA en todos los dispositivos del dominio de enrutamiento, ya que el uso de áreas restringe la inundación al límite lógico del área en vez de a todos los dispositivos del dominio OSPF. En otras palabras, un cambio en un área debe ocasionar el recálculo de la tabla de enrutamiento pero sólo esa área, no para todo el dominio.

La tabla 4.3 compara alguna de las características que presentan los protocolos de enrutamiento por estado del enlace. Se observa que EIGRP es técnicamente un protocolo avanzado de vector distancia, pero presenta algunas características de estado del enlace.

Característica	OSPF	IS-IS	EIGRP
Topología jerárquica-necesaria	X	X	
Retiene el conocimiento de todas las rutas posibles	X	X	X
Resumen de ruta-manual	X	X	X
Resumen de ruta-automática			X
Publicaciones de activación de eventos	X	X	X
Equilibrado de la carga-rutas iguales	X	X	X
Equilibrado de la carga-rutas desiguales			X
Soporte VLSM	X	X	X
Algoritmo de enrutamiento	Dijkstra	IS-IS	DUAL
Métrica	Coste	Coste	Compuesta
Límite de la cuenta de salto	Ilimitada	1024	100
Escalabilidad	Grande	Muy Grande	Grande

Tabla 4.3. Comparación de los protocolos de enrutamiento por estado de enlace IP de Cisco.

OSPF utiliza el algoritmo de Dijkstra, también llamado algoritmo Primero la ruta más corta SPF (*Shorthest Path First*). EIGRP utiliza el algoritmo DUAL en sus cálculos de rutas. IS-IS es el algoritmo de enrutamiento que utiliza el conjunto de protocolos de la International Organization for Standardization, Organización internacional de normalización (ISO), que incluye el Conectionless Network Service, Servicio de red no orientado a conexión (CLNS).

4.8.5 Enrutamiento Híbrido

Los protocolos de enrutamiento híbridos equilibrados utilizan la métrica de vector distancia, pero subrayan una métrica más exacta que los protocolos de vector distancia convencionales. También convergen más rápidamente que los protocolos de vector distancia, pero evitan los excesos de consumo de las actualizaciones del estado de enlace. Los híbridos equilibrados son eventos dirigidos más que periódicos y, por tanto, conservan ancho de banda para las aplicaciones reales.

Aunque existen los protocolos híbridos equilibrados “abiertos”, esta forma está casi exclusivamente asociada con la creación patentada de una sola compañía, *Cisco Systems, Inc*. Su protocolo, Protocolo de enrutamiento de *gateway* interior mejorado (EIGRP), fue diseñado para combinar los mejores aspectos de los protocolos de enrutamiento por vector distancia y por estado del enlace sin incurrir en ninguna de sus limitaciones de rendimiento. Dado que esta clase de protocolo de enrutamiento dinámico está dominada por EIGRP.

Características de rendimiento del enrutamiento híbrido

Una de las tareas más difíciles, aunque críticas, que deben superarse al construir una *internetwork* es la selección del protocolo de enrutamiento. Uno de los mejores métodos de empezar a hacer más pequeña la lista de potenciales protocolos es evaluando las características de rendimiento de cada protocolo en relación con los requisitos proyectados. A diferencia del hardware, no sirve comparar los paquetes por segundo o los valores de ancho de banda de los protocolos de enrutamiento. En su lugar se deben valorar la eficacia con que cada protocolo ejecuta distintas tareas que soportan el *internetworking*.

Dos de las más importantes de entre estas tareas son la convergencia y el cálculo de rutas. Las secciones siguientes se examinan cada uno de estos conceptos con más detalle. Hay que considerar mucho otros atributos de rendimiento, incluyendo el diámetro máximo de la red y lo bien que un determinado protocolo se adapta a las cargas pesadas de tráfico. Dichas características, sin embargo, tienden a ser más aplicables a protocolos específicos que las tres clases de enrutamiento dinámico identificadas anteriormente.

4.9 Convergencia

Uno de los aspectos más fascinantes del enrutamiento es un concepto conocido como convergencia. De forma bastante simple, siempre que se produce un cambio en la topología, o forma, de una red, todos los *routers* de esa red deben desarrollar un nuevo entendimiento de lo que es la topología de esa red. Este proceso es a la vez cooperativo e independiente; los *routers* comparten información entre sí, pero deben calcular independientemente los impactos del cambio de topología en sus propias rutas. Como deben desarrollar mutuamente un acuerdo sobre la nueva topología con independencia de las diferentes perspectivas, se dice que convergen en este consenso. La convergencia es necesaria ya los *routers* son dispositivos inteligentes que pueden tomar sus propias decisiones de enrutamiento. Esto es a la vez una fuente de fortaleza y de vulnerabilidad. Bajo condiciones de operatividad normales, esta inteligencia independiente y distribuida es fuente de tremendas ventajas. Durante los cambios en la topología de la red, el proceso de converger es un nuevo consenso en cuanto la forma de la red puede realmente introducir inestabilidad y suponer problemas de enrutamiento.

Ajuste de los cambios en la topología

Por desgracia, la naturaleza independiente de los *routers* puede ser también una fuente de vulnerabilidad siempre que se produzca un cambio en la topología de red. Dichos cambios, por su propia naturaleza, cambian la topología de una red.

Tiempo de convergencia

Es virtualmente imposible para todos los *routers* de una red detectar simultáneamente un cambio en la topología. De hecho, dependiendo del protocolo de enrutamiento que se use, así como de otros numerosos factores,

puede haber un retraso de tiempo considerable antes de que todos los *routers* de esa red alcancen un consenso, o acuerdo, sobre lo que es la nueva topología. Este retraso se llama tiempo de convergencia. Es importante recordar que la convergencia no es inmediata. Lo único que no se sabe es cuanto tiempo se necesitará para que se produzca la convergencia.

Algunos factores que pueden aumentar el tiempo de retraso intrínseco de la convergencia son los siguientes:

- La distancia (en saltos) al *router* desde el punto de cambio.
- El número de *routers* de la red que utilizan protocolos de enrutamiento dinámico.
- Ancho de banda y cantidad de tráfico en los enlaces de comunicaciones.
- La carga de un *router*
- Patrones de tráfico cara a cara del cambio topológico.
- El protocolo de enrutamiento utilizado.

Dados estos factores, está claro que las dos claves para minimizar los tiempos de convergencia son:

- Seleccionar un protocolo de enrutamiento que pueda calcular eficazmente las rutas.
- Diseñar adecuadamente la red.

4.10 Cálculo de rutas

La convergencia es absolutamente crítica para determinar la capacidad de una red para responder a las fluctuaciones operativas. El factor clave de la convergencia es la comunicación entre los *routers* de la red. Los protocolos de enrutamiento son los responsables de proporcionar esta función.

Específicamente, estos protocolos están diseñados para permitir a los *routers* compartir información sobre las rutas a los distintos destinos dentro de la red.

Flapping de rutas

Un síntoma de inestabilidad de la red que puede surgir es el conocido como *flapping* de rutas. Es sólo la rápida vacilación entre dos o más rutas. El *flapping* se produce durante un cambio en la topología. Todos los *routers* de la red deben converger en un consenso sobre la nueva topología. Con este fin, empiezan a compartir información de enrutamiento.

Debido a que los protocolos de enrutamiento no están creados de la misma forma, uno de los mejores modos de valorar la adecuación de un protocolo de enrutamiento consiste en evaluar sus capacidades para calcular rutas y converger en relación con otros protocolos de enrutamiento. Sería obvio a partir de la lista anterior de factores que los tiempos de convergencia pudieran ser difíciles de calcular con algún grado de certeza.

La capacidad de convergencia de un protocolo de enrutamiento es una función de su capacidad de cálculo de rutas. La eficacia del cálculo de rutas de un protocolo de enrutamiento se basa en varios factores:

- Si el protocolo calcula, y almacena, múltiples rutas a cada destino.
- La manera en que se inician las actualizaciones de enrutamiento.
- Las medidas utilizadas para calcular distancias o costes.

4.11 Almacenamiento de múltiples rutas

Algunos protocolos de enrutamiento intentan mejorar su eficacia operativa registrando una sola ruta (idealmente, la mejor) a cada destino

conocido. La desventaja de este método es que cuando se produce un cambio en la topología, cada *router* debe calcular una nueva ruta a través de la red para los destinos afectados.Otros protocolos aceptan los excesos de consumo de procesamiento que acompañan a los mayores tamaños de tabla de enrutamiento, y almacenan múltiples rutas a cada destino. En condiciones operativas normales, múltiples rutas permiten al *router* equilibrar las cargas de tráfico a través de múltiples enlaces. Cuando se produce un cambio en la topología, los *routers* ya tienen rutas alternativas a los destinos afectados en sus tablas de enrutamiento. El tener ya asignada una ruta alternativa no acelera necesariamente el proceso de convergencia. Sin embargo, sí permite a las redes sostener mejor los cambios en la topología.

4.12 Inicio de las actualizaciones

Algunos protocolos utilizan el paso del tiempo para iniciar las actualizaciones de enrutamiento. Otras son controladas por eventos, es decir se inician siempre que se detecta un cambio topológico. Manteniendo constantes todas las demás variables, las actualizaciones dirigidas por eventos dan como resultado tiempos de convergencia más cortos que las actualizaciones temporalizadas.

4.13 Métricas de enrutamiento

Los protocolos de enrutamiento simples soportan como mínimo una o dos métricas de enrutamiento. Los protocolos más sofisticados pueden soportar cinco o más métricas. Es seguro asumir que cuantas más métricas haya, más variadas y específicas son. Por tanto, cuanto mayor es la variedad de métricas disponibles, mayor es su capacidad de ajustar el funcionamiento de la red a sus necesidades particulares. Por ejemplo, los protocolos de vector distancia

utilizan una métrica eufemística: la distancia. En realidad, esa distancia no está relacionada con el kilometraje geográfico, y mucho menos con el kilometraje de cableado físico que separa las computadoras de origen y de destino. En su lugar, generalmente sólo cuenta el número de saltos entre esos dos puntos.

Los protocolos de estado del enlace pueden aportar la capacidad de calcular las rutas basándose en varios factores:

- Carga de tráfico.
- Ancho de banda disponible.
- Retraso de la propagación.

El coste de la red de una conexión (aunque esta métrica tiende a ser más una estimación que un valor real).

La mayoría de estos factores son altamente dinámicos en una red; varían según la hora del día, el día de la semana, etc. Importa recordar que, según varían, varía en consecuencia el rendimiento de la red. Por tanto, la pretensión de las métricas de enrutamiento dinámico es permitir que las decisiones de enrutamiento óptimo se hagan utilizando la información más actual posible.

Métricas estáticas frente a dinámicas. Algunas métricas son simples y estáticas, mientras que otras son altamente sofisticadas y dinámicas. Las métricas estáticas ofrecen generalmente la capacidad de personalizar sus valores cuando se configuran. Hecho esto, cada valor permanece constante hasta que se cambia manualmente.

Los protocolos dinámicos permiten tomar decisiones de enrutamiento basadas en información en tiempo real sobre el estado de la red. Estos protocolos son soportados sólo por los protocolos de enrutamiento por estado del enlace o son híbridos más sofisticados.

CAPITULO 5

PROTOCOLOS DE ENRUTAMIENTO

En este capítulo se mencionarán los protocolos de enrutamiento los cuales serán objeto de este estudio, de acuerdo a sus características principales protocolos IGPs y EGPs, que a continuación se ilustra en la figura 5.1 un ejemplo de cómo se considerarían su ubicación dentro de una red.

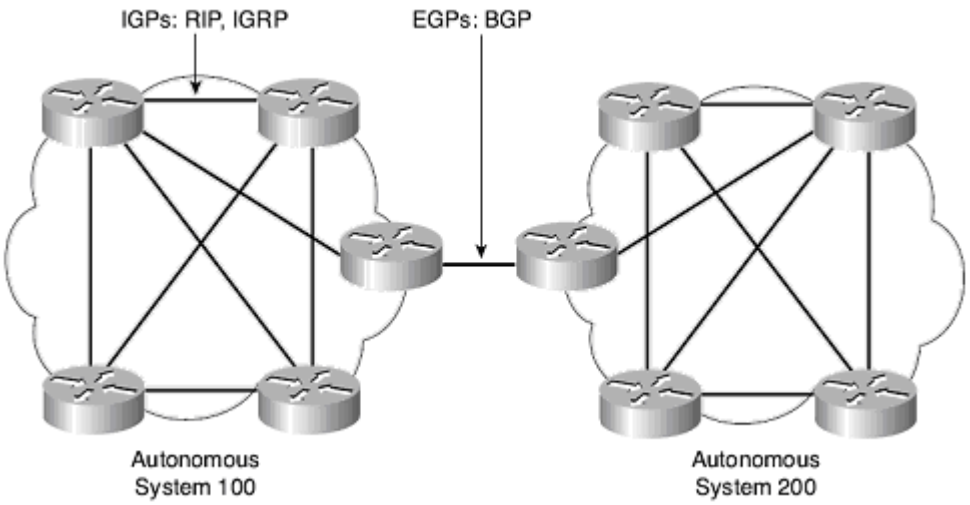

Figura 5.1. Protocolos de enrutamiento IGPs, EGPs.

5.1 Protocolo de Información de Enrutamiento RIPv1

RIP cuyas siglas en inglés *Routing Information Protocol* significan Protocolo de Información de Enrutamiento es uno de los protocolos de enrutamiento más antiguos y más utilizado para el intercambio de información de enrutamiento entre *routers* dentro de un mismo Sistema Autónomo. RIP

utiliza los algoritmos de vector distancia para calcular las rutas. Este tipo de algoritmo se ha utilizado para calcular las rutas de la red en numerosas variantes, durante décadas. Protocolo diseñado originalmente para la arquitectura XNS (*Xerox Network System*) y publicado formalmente en 1981 por la publicación “XNS Internet Transport Protocols” y en 1988 por el RFC 1058 para lo que hoy se conoce como RIP Versión 1.

Los *routers* que utilizan un protocolo de enrutamiento por vector distancia transmiten periódicamente copias de sus tablas de enrutamiento a sus vecinos inmediatos en la red. La tabla de enrutamiento de un *router* contiene información sobre la distancia entre éste y los destinos conocidos. Estos destinos pueden ser computadoras individuales, impresoras u otras redes. Cada receptor añade un vector de distancia (es decir, su propio “valor” de distancia) a la tabla, y envía la tabla modificada a sus vecinos inmediatos. Este proceso se produce de una manera omnidireccional entre *routers* que son vecinos inmediatos. La figura 5.2 utiliza una sencilla red RIP para ilustrar el concepto de vecinos inmediatos.

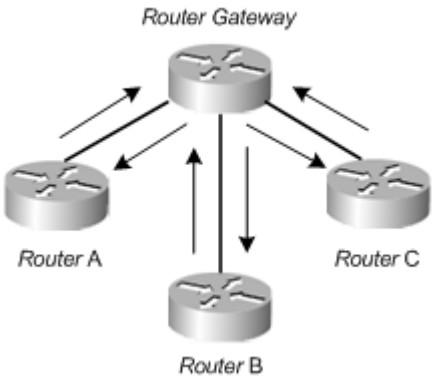

Figura 5.2. Cada nodo RIP publica el contenido de sus tablas de enrutamiento a sus vecinos inmediatos

5.1.1 Actualización de Rutas de RIP

RIP envía mensajes de actualización a intervalos regulares y cuando existen cambios en la topología de red. Cuando un *router* recibe una actualización de ruta que incluye cambios a una entrada, esta actualiza su tabla de enrutamiento para reflejar la nueva ruta. El valor de la métrica para cada salto es incrementado por 1, y el *router* que envío la actualización es señalado como el siguiente salto (*next-hop*). Los *routers* RIP solo mantienen en su tabla de enrutamiento la mejor ruta (la ruta con la métrica más baja) a un destino. RIP utiliza el puerto UDP 520 para enviar sus mensajes. Después de que se actualice la tabla de enrutamiento, el *router* inmediatamente empieza a transmitir actualizaciones de rutas a otros *routers* de la red de los cambios. Estas actualizaciones son enviadas independientemente de las regularmente programadas que RIP envía.

5.1.2 Métrica de Enrutamiento de RIP

RIP usa una sencilla métrica de enrutamiento, que es la cuenta de saltos (*hop-counts*) para medir la distancia entra la fuente y red destino. Cada salto en un camino de la fuente al destino es asignado a un contador de saltos, el cual es típicamente 1. Cuando un *router* recibe un a actualización que contiene un nuevo o cambio a un destino de red, el *router* agrega 1 al valor de la métrica indicado en la actualización y añade la red en la tabla de enrutamiento. La dirección IP del *router* que envía la información es usada como el siguiente salto (*next-hop*).

5.1.3 Funcionalidades de Estabilidad de RIP

RIP previene *loops* de enrutamiento implementando un límite de número de saltos permitidos en un camino del origen al destino. El máximo número de saltos en un camino es de 15. Si un *router* recibe una actualización que

contenga una nueva red o un cambio y si incrementando el valor de la métrica por 1 causa que la métrica tienda a infinito (que es 16), la red de destino es considerable inalcanzable. La desventaja de esta funcionalidad es que limita el máximo diámetro de una red RIP a menos de 16 saltos. RIP incluye otras funcionalidades que son comunes a otros protocolos. Estas funcionalidades estan diseñadas para proveer estabilidad debido a potenciales cambios que suceden rápidamente en la red. Por ejemplo RIP implementa los mecanismos de “Horizonte dividido” (*Split Horizon*), “Tiempos de Espera” (*holdown timers*), “Envenenamiento de ruta” (*Poison Reverse*), para prevenir que información incorrecta sea propagada en la red.

5.1.4 Temporizadores de RIP

RIP usa numerosos temporizadores para regular su desempeño. Estos incluyen un temporizador de actualización (*routing-update*), uno de tiempo terminado (*route-timeout*), uno de vacío de ruta (*route-flush*). El temporizador de actualización cronometra el intervalo entre actualizaciones periódicas de enrutamiento. Generalmente esta a 30 segundos, con un pequeño intervalo aleatorio de tiempo cuanto el temporizador es reiniciado. Esto es para prevenir congestión, el cual puede resultar en todos los *routers* simultáneamente intentando actualizar a sus vecinos. Cada entrada en la tabla de enrutamiento tiene un temporizador de espera asociado con ella. Cuando este tiempo expira, la ruta es marcada como inválida pero es retenida en la tabla hasta que el tiempo de vaciado expire. El tiempo de vida aproximadamente que tiene una ruta es de 180 segundos ya que si no se ha recibido mensajes que informen que la ruta continua activa, se borra, este tiempo corresponde a 6 actualizaciones.

RIP versión 1, se considera un protocolo de enrutamiento con clase (*Classful)*, que no admite la publicación de la información de la mascara de red por lo tanto no soporta VLSM ni CIDR.

5.2 RIP versión 2.

El Protocolo de información de enrutamiento versión 2, o RIPv2 como se le conoce comúnmente, se propuso primero como una actualización de RIP en el RFC 1388 en enero de 1993. Esta RFC fue sustituida más tarde por la RFC 1723, en noviembre de 1994. Ninguna de estas propuestas RIPv2 intentaba reemplazar a RIP. En su lugar ambas diseñaron RIPv2 como una extensión de RIP para proporcionar funcionalidad adicional. Estas extensiones se concentraron en el formato del mensaje RIP, y en proporcionar soporte para funciones de red nuevas, por ejemplo, la división en subredes, la autenticación y la multidifusión. Dado que RIPv2 es una extensión de RIP y también como su antecesor es un protocolo abierto, no es sorprendente que los protocolos de enrutamiento sean muy similares en sus mecánicas operativas y en sus características. A continuación en la tabla 5.1 se enlistan las diferencias que existen entre RIPv1 y RIPv2:

RIP versión 1	**RIP versión 2**
Es un protocolo con clase (*Classful)*	Es un protocolo sin clase (*Classless)*
No soporta CIDR, VLSM ni resumen de rutas	Soporta CIDR, VLSM y resumen de rutas
No admite mecanismos de autenticación en sus actualizaciones	Soporta mecanismos de autenticación como MD5 en sus actualizaciones
Usa *broadcast* 255.255.255.255 para la actualización de rutas.	Usa Multidifusión (*Multicasting*) para enviar sus actualizaciones, la IP reservada para esto es la 224.0.0.9

Tabla 5.1. Comparación de características RIPv1 y RIPv2.

Aún así RIP-2 sigue siendo inapropiado para entornos de red que requieren que las rutas sean seleccionadas en tiempo real basándose en cualquier retraso, carga de tráfico o cualquier otra métrica dinámica de rendimiento de la red, ya que como su antecesor RIPv1 para elegir la mejor métrica sigue utilizando el numero de saltos hacia el destino, así también

carencia de rutas alternativas ya que continúa manteniendo una ruta única a cualquier destino dado en sus tablas de enrutamiento. En caso de que una ruta fuera invalidada, el nodo RIPv1 no conoce otras rutas al destino de la ruta que ha fallado. En consecuencia, debe esperar una actualización de enrutamiento antes de poder empezar a valorar las posibles rutas alternativas a ese destino. Este método de enrutamiento minimiza el tamaño de las tablas de enrutamiento, pero puede dar como resultado la inaccesibilidad temporal de destinos durante la falla de un enlace o de un *router*. Además su tiempo de convergencia tiende a ser muy lento ya que puede tomar de 3 a 5 mins.

Existe una nueva versión para RIP llamada **RIPng** basada en RIPv2, la cual solo mencionaremos que se usará para IPv6 y se específica en el RFC 2080.

5.3 Protocolo de Información de *Gateway* Interior IGRP.

IGRP de Cisco es un protocolo de vector distancia mejorado desarrollado por *Cisco Systems* en los 80's. Fue diseñado con el objetivo de que fuera tan fácil de utilizar como RIP y con muchas de sus características, pero sin ninguna de sus limitaciones operativas, esto para proporcionar un mejor soporte a redes escalables con diferentes anchos de banda. IGRP es un protocolo de vector de distancia diseñado para su uso en *routers* gateway interiores dentro de un sistema autónomo, estos *routers* envían regularmente todas, o parte de sus tablas de enrutamiento a sus vecinos inmediatos. Este proceso se repite periódicamente y recursivamente a través del sistema autónomo hasta que todos los nodos de ese sistema están de acuerdo en la topología y las distancias a los destinos conocidos. IGRP es un protocolo de enrutamiento IP con clase (*classful*).

IGRP recibió un conjunto expandido de funciones relativas a RIP y otros protocolos de vector distancia. Una de las características más revolucionarias fue el modo en que calculaba los vectores de distancia. IGRP tiene una serie de métricas, cada una de ellas con una amplia gama de posibles valores. A cada una de estas métricas se le puede aplicar una función de tipo *hash* contra un valor matemático, o peso. Esto permite a los administradores de redes personalizar el algoritmo de cálculo de rutas según sus necesidades específicas. Estas métricas y sus pesos, se utilizan para calcular una sola métrica de enrutamiento compuesta. Esta métrica compuesta se utiliza para comparar matemáticamente las rutas a los destinos.

5.3.1 Métricas IGRP

Una de las áreas en que IGRP destaca es en su alto grado de flexibilidad que consigue a través de sus métricas de enrutamiento. A diferencia de RIP, que tiene una sola métrica estática, IGRP utiliza seis métricas:

- Cuenta de saltos (*hops*).
- Tamaño del paquete o *MTU*.
- Ancho de banda del enlace (*bandwith*).
- Retraso (*delay*).
- Carga (*load*).
- Confiabilidad (*reliability*).

Los nodos IGRP comparten información perteneciente a las seis métricas durante las actualizaciones de las tablas, pero no todas ellas se utilizan para calcular las rutas. De hecho, sólo el ancho de banda, el retraso, la carga y la confiabilidad pueden utilizarse para calcular rutas. Las otras dos, cuenta de saltos y MTU, facilitan el enrutamiento de otros modos. El administrador puede definir cada una de estas métricas usando los valores determinados o establecerlos a conveniencia.

- **Cuenta de saltos.** IGRP soporta el incremento de una cuenta de saltos como medio para determinar lo alejados que están los destinos específicos. Cada *router* de una ruta cuenta como un solo salto. El máximo predetermiando es de 100; sin embargo puede aumentar hasta 255. La cuenta de saltos es sólo un modo de protegerse contra los *loops* de enrutamiento.
- **MTU.** Identifica el datagrama de mayor tamaño que aceptará un *router* IGRP. Este valor no se utiliza para calcular rutas, ni es un factor de métrica compuesta de IGRP. Es mejor considerar la MTU como un modo de hacer un ajuste fino del rendimiento de la red. Idealmente, este valor se establecerá coherentemente con los requisitos del usuario y con todos los *routers* de un sistema autónomo.
- **Ancho de banda.** Identifica la velocidad del servicio de transmisión que está conectado a un puerto de E/S dado del *router*. Estos valores oscilan entre 1,200 bps y 10 Gbps. Si no se establece explícitamente a un valor, *Cisco IOS* supondrá que el enlace es un T1, y predeterminará la métrica del ancho de banda a 1,544 Mbps. A los efectos de cálculo de métrica, IGRP busca el ancho de banda definido en todos los puertos de interfaz exteriores de una ruta dada y selecciona el menor de estos números (que es el límite de ancho e banda para esa ruta). Este número es dividido entonces por 10^8, lo que da como resultado que el ancho de banda se exprese en kbits por segundo.
- **Retraso.** Mide la cantidad de tiempo aproximada necesaria para atravesar un enlace una red, suponiendo que el enlace esté sin usar. El retraso global de una ruta en una red IGRP es la suma de los retrasos atribuidos a cada interfaz del *router* saliente en una ruta. Esta suma es dividida por 10 para expresar el resultado en microsegundos. Esta métrica puede ser cualquier valor entre 1 y 16.77.215. Puede producirse un retraso adicional como resultado de la congestión. Los efectos de la congestión, o incluso los niveles moderados de tráfico, también pueden

ser factores de la métrica compuesta IGRP al tener en cuenta el factor de carga. La carga mide los retrasos producidos como resultado de los niveles de utilización del ancho de banda.

- **Carga.** El factor carga mide la cantidad de ancho de banda actualmente disponible a lo largo de un enlace dado. Cuanto más se utiliza un enlace, más tiempo se necesita para atravesarlo. La carga en IGRP permite factorizar los niveles actuales de utilización en el cálculo de rutas de red óptimas. El intervalo de valores soportado por esta métrica va de 1 a 255, el administrador de redes puede manipular tanto este valor de métrica como su peso, así que las cargas habituales pueden factorizarse en los cálculos de rutas. Se debe de tener cuidado extremos siempre que se modifiquen las métricas o sus pesos. Experimentar con la carga, además, puede ser particularmente peligroso en una red real, porque los efectos de su cambio podrían no ser evidentes hasta que la red tuviera que soportar grandes cargas.
- **Confiabilidad.** El administrador de redes tiene otro modo de inclinar los resultados de los cálculos de las rutas de IGRP utilizando una métrica de confiabilidad. La confiabilidad hace un seguimiento de la actual proporción de errores de cada servicio de transmisión. Una proporción de errores no es más que el número de paquetes que llegan sin dañar. Esta métrica, al igual que la carga, puede tener cualquier valor entre 1 y 255. Como valor predeterminado está establecido a 1 para todos los tipos de servicios de transmisión. Con el tiempo, este valor probablemente aumentará a medida que el nodo IGRP factoriza las proporciones de errores reales producidas, por cada servicio de transmisión. Un valor alto de la métrica de confiabilidad indica enlaces problemáticos o no fiables.

5.3.2 Uso de las métricas IGRP

La clave de la flexibilidad de IGRP no reside en ninguna de sus métricas, sino en lo que IGRP hace con sus métricas. A diferencia de RIP y la mayoría de los demás protocolos de enrutamiento, IGRP no sólo compara los valores de métrica de las rutas potenciales. En su lugar, IGRP utiliza los valores de las métricas, así como los pesos predeterminados o definidos por el administrador, para desarrollar una única métrica compuesta que describe matemáticamente las rutas posibles. Esta métrica compuesta puede utilizarse para comparar las rutas potenciales a través de la red, incluso aunque las rutas varíen ampliamente en fiabilidad, ancho de banda, retraso y niveles de utilización. La ventaja obvia de una métrica, desarrollada usando diferentes pesos de variables, es que es posible describir con más exactitud el rendimiento potencial de una ruta. El administrador de la red puede utilizar estas variables para influir en el proceso de selección de ruta dentro del sistema autónomo.

La limitación de la implementación de las métricas de IGRP es que es fácil anularlas. Aceptando todos los valores predeterminados, por ejemplo, todas las métricas de las rutas son iguales. Por tanto, matemáticamente se anulan. El proceso de cálculo de rutas será entonces poco más que una abstracta comparación del número de saltos en cada ruta potencial. Está claro que lo que más le interesa es personalizar estas métricas de enrutamiento, particularmente el ancho de banda. Se puede incluso encontrarlo útil para alterar los factores de peso a fin de acercarse más a las condiciones de una red y/o a las necesidades de los usuarios.

5.3.3 Mecanismos de IGRP

Además de su excelente métrica de enrutamiento compuesta, IGRP también se apoya en una serie de mecanismos para funcionar adecuadamente y mantener un entorno de *internetworking* estable. Estos mecanismos se

dividen en dos grandes categorías: mecanismos de temporización y mecanismos de convergencia.

Mecanismos de temporización

Igual que con otros protocolos de enrutamiento por vector distancia, IGRP mantiene la integridad de sus tablas de enrutamiento solicitando a los *routers* que compartan su información de enrutamiento. Cada *router* IGRP envía actualizaciones de su tabla de información de enrutamiento a sus vecinos inmediatos a intervalos fijos. Todas las actualizaciones recibidas sustituyen automáticamente la anterior información de ruta que estaba almacenada en la tabla de enrutamiento. IGRP se apoya en cuatro temporizadores para mantener la tabla de enrutamiento:

- Temporizador de actualización (update).
- Temporizador de espera (*holddown)*
- Temporizador de ruta no válida.
- Temporizador de eliminación de ruta.

A continuación se detallan los mecanismos de temporización:

- **Temporizador de actualización.** Se utiliza para iniciar las actualizaciones de la tabla de enrutamiento a nivel nodo. Cada nodo IGRP utiliza un único temporizador de actualización, del que realiza un seguimiento como recurso a nivel sistema. El valor predeterminado es de 90 segundos, aunque un administrador de redes puede ajustar este valor. A no ser que se modifique, los nodos IGRP intentarán actualizar sus tablas de enrutamiento compartiendo su información de enrutamiento con sus nodos vecinos cada minuto y medio.
- **Temporizador de espera.** Hace un seguimiento de la cantidad de tiempo que los nodos IGRP almacenan las tablas de enrutamiento. El

tiempo de predeterminado para los nodos IGRP es tres veces el valor máximo del temporizador de actualización más 10 segundos. Retrasar intencionalmente tales actualizaciones evita que se reinstalen accidentalmente rutas a destinos inalcanzables.

- **Temporizador de ruta no válida.** Especifica el tiempo que debe esperar un *router*, en ausencia de mensajes de actualización de enrutamiento sobre una ruta específica, antes de declarar esa ruta como no válida. El valor predeterminado es tres veces el periodo de actualización.
- **Temporizador de eliminación de ruta.** Indica el tiempo que debe transcurrir antes de que una ruta sea eliminada de la tabla de enrutamiento. El valor predeterminado de IGRP es siete veces el periodo de actualización de enrutamiento. Este mecanismo se usa para depurar, o limpiar, rutas no válidas de las tablas de enrutamiento IGRP.

Mecanismos de convergencia

IGRP incluye varias características diseñadas para reducir los tiempos de convergencia y mejorar la estabilidad de las redes IGRP:

- Flash update.
- Inmovilizaciones.
- Horizontes divididos.
- Actualizaciones de efecto inverso.

5.3.4 Enrutamiento Multirruta

Una de las características más importantes de IGRP es su capacidad de realizar enrutamiento multirruta. IGRP puede recordar hasta cuatro rutas diferentes a cualquier destino dado. Esto permite a IGRP balancear las cargas de tráfico, mientras se protege contra los impactos por las fallas en los enlaces.

Las rutas redundantes pueden ser de costes iguales o diferentes. Por tanto, IGRP puede soportar dos tipos de balanceo de carga:

- Balanceo de carga de igual coste (por paquete o por destino).
- Balanceo de carga de coste desigual.

Varianza. Es La clave del éxito del balanceo de carga en una red IGRP, es un atributo modificable por el usuario que especifica el porcentaje en que puede variar el rendimiento de diferentes enlaces, siendo aún considerados rutas validas al mismo destino. Este tributo se aplica en toda la red IGRP más que a enlaces individuales.

Sucesores factibles (*feasible succesor*). IGRP puede usarse para establecer una jerarquía de sucesión factible en un entorno de enrutamiento multirruta. Los sucesores factibles son rutas cuyos costes son mayores que la varianza especificada para la ruta óptima a un destino dado. Como tales, son inviables para el equilibrado de la carga de coste desigual. Tales rutas pueden servir todavía como sucesores factibles a esa ruta óptima; sin embargo podrían llegar a ser no usables.

5.3.5 Dominio de Proceso

IGRP usa el concepto de Dominios de Proceso. Definiendo múltiples dominios de proceso, se pueden aislar las comunicaciones con un dominio de la comunicación con otro dominio. El tráfico entre dominios puede ser regulado usando redistribución y filtrado de rutas. En a figura 5.3 Se ilustra el concepto de Dominio de Proceso en IGRP. Un AS puede especificar un dominio de enrutamiento, bajo IGRP un AS puede también especificar un número de dominio de proceso, el cual es un grupo de *router* compartiendo información de enrutamiento por medio de un sencillo proceso de enrutamiento.

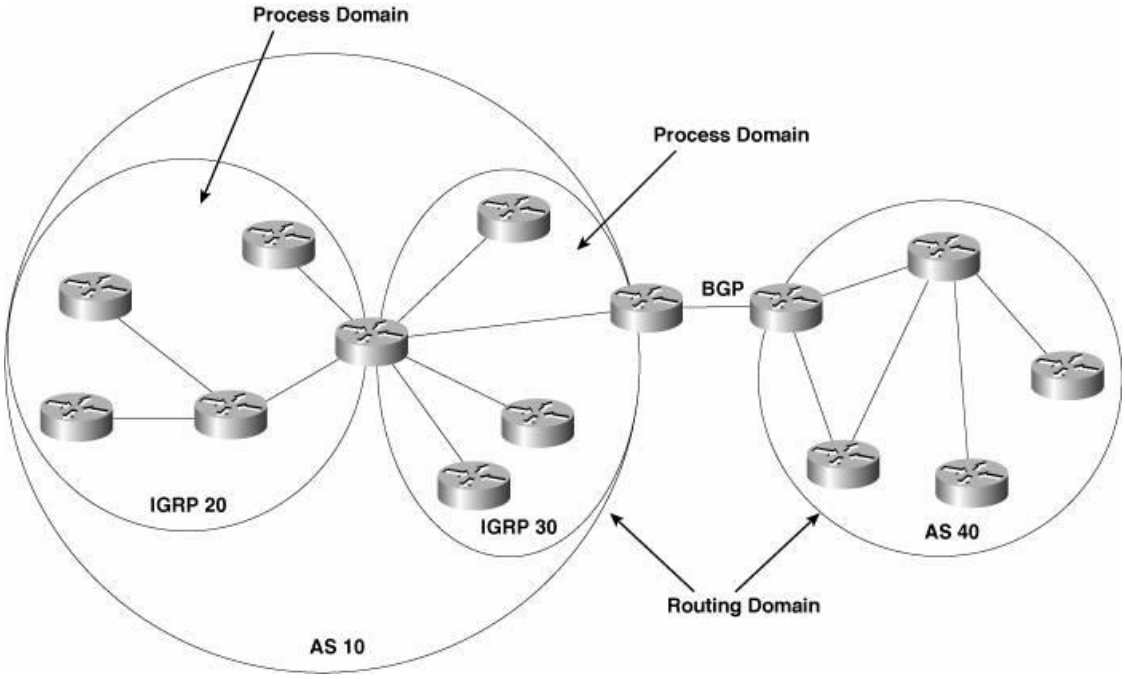

Figura 5.3. Dominio de Proceso en IGRP.

5.4 Protocolo de Enrutamiento de *Gateway* Mejorado EIGRP.

El Protocolo de Enrutamiento de *Gateway* Mejorado ó por sus siglas en Inglés EIGRP (*Enhanced Interior Gateway Routing Protocol*), es propietario de *Cisco Systems* basado en IGRP. Aunque es considerado un protocolo de enrutamiento Híbrido o un protocolo de vector distancia avanzado, ya que ofrece lo mejor de ambos algoritmos de vector distancia y estado enlace.

A diferencia de su predecesor, por ejemplo EIGRP soporta tanto las direcciones sin clase, como las direcciones IP con clase, así como otros protocolos de red. Otras actualizaciones fueron diseñadas para reducir los tiempos de convergencia y mejorar la estabilidad de la red. Una de esas actualizaciones fue un nuevo algoritmo, el Algoritmo de actualización difuso (DUAL), que permite a los *routers* EIGRP determinar si una ruta publicada por

un vecino esta en *loop* o libre de *loops*, y permite a un *router* ejecutar EIGRP para encontrar rutas alternativas sin esperar actualizaciones de otros *routers*. Esto ayuda a converger a las redes EIGRP, sin incurrir en ningún riesgo significativo de introducir o propagar *loops* de enrutamiento. También se introdujeron otras medidas que redujeron la intensidad de la convergencia de la red operando con una mayor eficiencia.

Aunque EIGRP se desarrolló como una alternativa más actualizada y eficaz a IGRP, fue también explícitamente una extensión de IGRP. En consecuencia, los dos están pensados en ser completamente compatibles. Estos dos protocolos de enrutamiento comparten incluso la misma tecnología de enrutamiento por vector distancia y utiliza la misma métrica compuesta de enrutamiento que IGRP sólo hay una diferencia en el algoritmo que calcula la métrica compuesta: la métrica IGRP tiene 20 bits de longitud, mientras que la métrica EIGRP tiene 32. Esta diferencia da como resultado que la métrica EIGRP es mayor en un factor de 256 que una métrica UGRP comparable para cualquier ruta dada. Una métrica mayor permite una comparación matemática mejor y más exacta de las rutas potenciales.

Esta diferencia menor es fácil y automáticamente compensada por EIGRP. El cual ajusta automáticamente la métrica compuesta de las rutas IGRP y ajusta su propia métrica a las rutas que se están redistribuyendo a *routers* IGRP. Las métricas de IGRP y EIGRP son directamente comparables. Por tanto, pueden utilizarse de forma intercambiable después de la traducción. EIGRP, sin embrago, hace un seguimiento de las rutas IGRP traducidas como rutas externas. IGRP no tiene ningún concepto de rutas internas y externas. En consecuencia, las rutas EIGRP traducidas y redistribuidas en una red IGRP son tratadas como rutas IGRP. La redistribución automática entre IGRP y EIGRP sólo se producirá si los dos protocolos están configurados con el mismo sistema autónomo (AS). Si tienen diferentes números de AS, supondrán que son parte de diferentes redes (es decir, sistemas autónomos).

El mecanismo de ajuste de métrica de EIGRP permite a IGRP y EIGRP estar completamente integrados a través de una simple función matemática. Las rutas IGRP externas que son automáticamente ajustadas por EIGRP pueden compararse directamente con las rutas internas EIGRP. Los *routers* Cisco siempre seleccionarán la ruta con la mejor métrica en lugar de seleccionar automáticamente la ruta de cualquier protocolo en particular. Por tanto un *router* EIGRP podría decidir que la mejor ruta es realmente una ruta IGRP externa en lugar de una ruta EIGRP interna.

EIGRP al igual que IGRP usa el siguiente cálculo de métrica:

Métrica= [K1 * ancho de banda + ((K2 * ancho de banda)/(256-carga))+ (K3 * retardo)]*[K5/(confiabilidad + K4)].

(Nota: Debido a que EIGRP utiliza un campo de métrica de 32 bits, a diferencia de IGRP que es de 24, multiplica este valor por 256).

He aquí algunas de las ventajas específicas de EIGRP:

- **Consumo mínimo de ancho de banda cuando la red es estable.** Durante el funcionamiento normal y estable de la red, los únicos paquetes EIGRP intercambiados entre los nodos EIGRP son paquetes *hello.* Este simple proceso permite a los *routers* EIGRP saber que todo sigue bien en la red.
- **Uso eficaz del ancho de banda durante la convergencia.** EIGRP sólo propaga los cambios en la tabla de enrutamiento, no la tabla de enrutamiento completa. Así mismo, las actualizaciones se publican sólo después de un cambio topológico más sobre una base periódica estricta. Estas actualizaciones se transmiten sólo a aquellos *routers* EIGRP que necesitan saber del cambio.
- **Convergencia rápida.** Los *routers* EIGRP almacenan cada ruta que han aprendido a cada destino de la red. Por tanto, un *router* que ejecute

EIGRP puede converger rápidamente en una ruta alternativamente después de cualquier cambio topológico.

- **Soporte para VLSM y CIDR.** EIGRP soporta la definición de los números de red y de *host* en cualquier límite de *bit*, por interfaz, para direcciones IP y máscaras de subred.
- **Completa independencia de los protocolos enrutados.** EIGRP está diseñado para ser completamente independiente de los protocolos enrutados. El soporte para los protocolos enrutados es a tráves de módulos individuales, específicos del protocolo. Por tanto, la evolución de un protocolo, como IP, no amenazará a EIGRP con la obsolescencia. Dichos avances tecnológicos tampoco forzarán una ardua revisión de EIGRP.

5.4.1 Nuevas características de EIGRP

EIGRP tiene de muchas tecnologías, cada una de las cuales representa una mejora en eficacia operativa, rapidez de convergencia o capacidad/funcionalidad con respecto a IGRP y otros protocolos de enrutamiento. Estas tecnologías forman parte en una de las siguientes cuatro categorías:

- Descubriendo y recuperación del vecino.
- Protocolo de transporte confiable.
- Máquina de estado finito DUAL
- Módulos específicos de protocolo.

Descubrimiento y recuperación del vecino. EIGRP, a diferencia de virtualmente casi otro protocolo de enrutamiento por vector distancia, no se apoya exclusiva y rígidamente en el uso de temporizadores para mantener su tabla de enrutamiento. En su lugar, la base para mantener las tablas de

enrutamiento es una comunicación periódica entre *routers* EIGRP, usan este proceso para:

- Aprender dinámicamente de nuevos *routers* que pueden unirse a su red.
- Identificar *routers* que llegan a ser inalcanzables o inoperables.
- Redescubrir *routers* que habían sido previamente inalcanzables.

El proceso básico de descubrimiento/recuperación del vecino consiste en transmitir periódicamente un pequeño paquete *hello* a los vecinos. El paquete *hello* establece la relación entre los vecinos inmediatos. Esta relación se utiliza para intercambiar métricas de enrutamiento e información.Un *router* EIGRP puede suponer con seguridad que, mientras esté recibiendo paquetes *hello* de los vecinos conocidos, estos vecinos (y sus rutas) permanecen viables. Sin embargo, si un *router* EIGRP deja de recibir estos mensajes desde un vecino, puede suponer que algo está pasando. Ese *router* introducirá el proceso DUAL para esas rutas.

Protocolo de transporte confiable. Una de las características más importantes de EIGRP es su capacidad de suministrar la entrega garantizada, fiable, de sus distintos paquetes. Otros protocolos evitan utilizar la distribución y confían en otros mecanismos, como el paso del tiempo, para determinar si un paquete necesita ser transmitido de nuevo. Por desgracia, la falla fundamental de tal método es que agrava el proceso de convergencia. Cuanto más le lleva a una red converger, mayor será la oportunidad de que se interrumpa el servicio a través de la red. EIGRP recibió un nuevo protocolo, Protocolo de transporte rápido (RTP), para proporcionar una entrega fiable de sus propios paquetes. RTP es un protocolo de capa de transporte que se corresponde con la funcionalidad identificada por la capa 4 del modelo de referencia OSI. Sin embrago, RTP es una innovación privada de *Cisco Sytems*, y no un estándar abierto. IP utiliza dos protocolos de transporte similares TCP y UDP. RTP puede soportar la distribución fiable y no fiable de los datagramas. Puede soportar

incluso ambos tipos simultáneamente y resecuenciar los paquetes recibidos en un orden inadecuado. En lugar de crear un nuevo protocolo de transporte, los diseñadores de EIGRP podían haber usado TCP y/o UDP como transporte para los mensajes EIGRP. Sin embargo, esto habría hecho a EIGRP demasiado específico de IP. El objetivo de los diseñadores era crear un protocolo de enrutamiento independiente que pudiera extenderse fácilmente para soportar cualesquiera protocolos de enrutamiento nuevos, como IPv6, que pudieran desarrollarse en un futuro. RTP fue desarrollado específicamente para cumplir estos requisitos. RTP puede soportar también mutidifusión y la unidifusión. Los paquetes de multidifusión son distribuidos simultáneamente a múltiples destinos específicos usando una dirección de grupo. Los paquetes de unidifusión se direccionan explícitamente a un único destino. RTP puede soportar incluso transmisiones simultáneas de multidifusión y unidifusión para diferentes iguales.

El algoritmo de actualización distribuido DUAL. Es el motor de cálculo de rutas de EIGRP. El nombre completo del motor de EIGRP es Máquina de estado finito DUAL (DUAL FSM). Este motor contiene toda la lógica usada para calcular y comparar rutas en una red EIGRP. DUAL sigue la pista de todas las rutas publicadas por los vecinos, y usa la métrica compuesta de cada ruta para compararlas. Las rutas seleccionadas den estar libres de *loops* y tener menor coste. Tales rutas son insertadas por el protocolo DUAL en una tabla de enrutamiento para su uso en el envío de datagramas. Las rutas seleccionadas para su inserción en una tabla de enrutamiento son evaluadas también sobre la base de una sucesión viable. Un sucesor factible es un *router* vecino que es el siguiente salto de una ruta de menor coste para cualquier destino dado. Un sucesor factible es una ruta libre de loops de acuerdo con DUAL FSM.

Módulos específicos de protocolo. Como se indicó anteriormente, uno de los principios de diseño claves que guía el desarrollo de EIGRP es la completa independencia de los protocolos enrutados. Por tanto, EIGRP

implementó un método modular para soportar los diferentes protocolos enrutados. Muchos protocolos están específicamente diseñados para un único protocolo enrutado o tienen mecanismos para soportar múltiples protocolos. EIGRP tiene esos mecanismos nativos, pero son completamente modulares. En teoría, EIGRP puede ajustarse fácilmente para soportar cualquiera de los nuevos protocolos enrutados que pueden desarrollarse añadiendo tan sólo otro módulo específico del protocolo. Cada módulo específico del protocolo es responsable de todas las funciones relacionadas con su protocolo enrutado específico.

IP-EIGRP puede redistribuir rutas aprendidas de otros protocolos de enrutamiento compatibles con IP, incluyendo OSPF, IS-IS (Sistema intermedio-sistema intermedio), EGP (Protocolo de *gateway* exterior) y BGP (Protocolo de *gateway* fronterizo). EIGRP tiene módulos comparables para soportar tanto AppleTalk como IPX. El módulo *AppleTalk* (AT-EIGRP) puede redistribuir rutas aprendidas del Protocolo de mantenimiento de tabla de enrutamiento (RTMP). IPX-EIGRP puede redistribuir información de enrutamiento de la versión patentada de RIP de Novell, así como del Protocolo de publicación del servicio (SAP) y del Protocolo de estado del enlace de Novell (NLSP). El módulo IP-EIGRP de EIGRP dio soporte a muchas de las actualizaciones de IP que la base de clientes IGRP de Cisco había estado pidiendo. En concreto, IP-EIGRP introdujo soporte para VLSM, así como para CIDR. IGRP no soportaba ninguna de estas características.

5.4.2 Estructuras de datos de EIGRP

EIGRP es un protocolo de enrutamiento que consume información; debe hacer un seguimiento del estado actual (o aproximadamente actual) de muchas facetas diferentes de la red. Esta información está organizada en conjuntos de información relacionada, que se almacenan en tablas. EIGRP mantiene la actualidad de esas tablas mediante una serie de tipos de paquetes

especializados. Cada tipo de paquete se utiliza para una función específica. Esta sección examina la funcionalidad básica y el uso de cada una de las tablas y los tipos de paquetes de EIGRP.

5.4.3 Tablas EIGRP

EIGRP utiliza muchas tablas diferentes, cada una de ellas dedicada a organizar, almacenar datos pertenecientes a una faceta específica de la red. La naturaleza patentada de EIGRP impide un examen exhaustivo de esas tablas, así como de sus estructuras. Es posible, sin embargo examinar el papel de las tablas de EIGRP más importantes, incluyendo:

- La tabla de vecinos.
- La tabla de enrutamiento.
- La tabla de topología.

Hay otras tablas, pero estas tres deberían representar adecuadamente el grueso de la mecánica interna de EIGRP.

La tabla de vecinos. Es La tabla más importante de EIGRP es la tabla de vecinos. Las relaciones de vecindad de las que se hace un seguimiento en esta tabla son la base de toda la actividad de actualización de enrutamiento y de convergencia. La tabla de vecinos hace un seguimiento de la información del estado de los nodos EIGRP vecinos adyacentes. Siempre que se descubre un vecino nuevo, la dirección y la interfaz de ese vecino se registran en una entrada nueva de la tabla de vecinos. En realidad, un *router* EIGRP puede contener varias tablas de enrutamiento, porque necesita una por cada módulo dependiente del protocolo. Por tanto, una red que ejecute tanto AppleTalk como IP tendría dos tablas de vecinos diferentes. Tendría que configurarse un proceso EIGRP separado por cada protocolo enrutado usado en la red.

La tabla de enrutamiento. Esta tabla contiene todas las rutas de menor coste que calculó DUAL par todos los destinos conocidos. EIGRP, como todos los protocolos de enrutamiento soportados por Cisco, hace un seguimiento de hasta seis rutas a cada destino. Siempre que un *router* detecta un cambio en una sola entrada de la tabla de enrutamiento, debe notificar a sus vecinos ese cambio. Estos vecinos deben determinar entonces el impacto que tiene el cambio en sus rutas. Para cada protocolo enrutado que EIGRP está configurado para soportar se mantiene una tabla de enrutamiento separada.

La tabla de topología. EIGRP utiliza su tabla de topología para almacenar toda la información que necesita para calcular un conjunto de distancias y vectores a todos los destinos alcanzables. Esta información incluye los siguientes campos:

- Ancho de banda (*bandwith*).
- Retraso total (*delay*).
- Confiabilidad (*reliability*).
- Carga (*load*).
- MTU
- Distancia notificada (distancia notificada por un vecino adyacente a un destino específico).
- Distancia viable (es la menor métrica calculada a cada destino).
- Origen de ruta (es el *id* del *router* que publicó originalmente esa ruta).

También queda registrada en cada entrada la interfaz a través de la cual se alcanza ese destino. La tabla de topología está ordenada. Los sucesores están en la parte superior. Seguidos inmediatamente por sucesores factibles. EIGRP almacena incluso rutas que DUAL cree que están en la tabla de topología. Estas rutas están en la parte inferior de la tabla de topología ordenada.Se crea una tabla de topología para cada módulo dependiente del

protocolo que está siendo usado por EIGRP. La información contenida en una tabla de topología se usa como entrada de la tabla de estado finito de DUAL.

Las entradas de una tabla de topología pueden estar en uno de dos estados: activo o pasivo. Estos estados identifican el estado de la ruta indicada por la entrada, en lugar del estado en sí de la entrada. Una ruta pasiva es la que es estable y está disponible para su uso. Una ruta activa es la que actualmente se está recalculando. La recalculación es el proceso de volver a calcular rutas en busca de nuevos sucesores.

EIGRP clasifica las rutas como internas o externas. Las rutas son internas son las originadas dentro de una ruta EIGRP. Las rutas externas fueron aprendidas bien desde un protocolo de enrutamiento diferente (aquellas que residen fuera del sistema autónomo de EIGRP Y fueron aprendidas por un *router* fronterizo entre los dos sistemas autónomos) o son rutas estáticas introducidas en EIGRP a través de la redistribución. Todas las rutas externas están etiquetadas en la tabla de topología e incluyen la siguiente información:

- El número de identificación (ID del *router*) del *router* EIGRP que redistribuyó esa ruta en la red EIGRP.
- El número del sistema autónomo donde reside el destino de esa ruta.
- El protocolo utilizado en esa red externa.
- El coste o la métrica recibidos desde ese protocolo externo.
- Una etiqueta que puede establecerse administrativamente y usarse en el filtrado de rutas.

El etiquetado de rutas proporciona al administrador de la red flexibilidad para establecer normas de enrutamiento. Esta flexibilidad es de la mayor utilidad cuando la red EIGRP está interconectada con un protocolo de enrutamiento basado en normas, como EGP o BGP. En EIGRP, todos los *routers* vecinos que tienen publicada una métrica compuesta (distancia

notificada) que es menor que la mejor métrica actual de un *router* (distancia viable) para cualquier ruta dada, se consideran sucesores factibles del sucesor actual (la ruta que se está utilizando actualmente). Si hay múltiples rutas con un coste igual al mejor coste, son consideradas todas sucesoras, e instaladas todas en la tabla de enrutamiento. Un destino debe tener al menos un sucesor antes de que pueda desplazarse de la tabla de topología a la tabla de enrutamiento. Un *router* EIGRP ve sus sucesores factibles como vecinos que están en el flujo descendente, o más cerca, del destino de lo que está el mismo. Siempre que ocurre un cambio en la red que afecta su topología e incluso la métrica compuesta de una sola ruta, el conjunto de sucesores y sucesores factibles de la ruta o de las rutas afectadas puede que tengan que volver a evaluarse.

Si un *router* pierde su ruta a través de su sucesor y no hay sucesores factibles, la ruta entra automáticamente en el estado activo y dispara la recomputación. El *router* consulta a sus vecinos, solicitando nueva información sobre posibles rutas alternativas a la ruta impactada. Los *routers* vecinos deben responder. Su respuesta puede contener información sobre sus sucesores o la notificación de que tampoco pueden alcanzar la ruta. La ruta sólo puede regresar a su estado pasivo después de que el router haya recibido una respuesta desde cada uno de sus routers vecinos, y pueda seleccionar un sucesor o determinar que el destino ya no es alcanzable.

5.4.4 Tipos de paquete EIGRP

EIGRP utiliza cinco paquetes especializados para mantener sus distintas tablas de enrutamiento. Cada tipo de paquete realiza una función específica en el soporte del mantenimiento de una tabla de enrutamiento:

- *Hello*.
- Acuse de recibo (*ack*).

- Actualización (*update*).
- Consulta (*query*).
- Respuesta (*reply*)

Paquetes *hello*. Se utilizan para descubrir (o redescubrir) y hacer un seguimiento de los otros *routers* EIGRP de la red. En circuitos multipunto de ancho de banda relativamente bajo (menor que T1), EIGRP utiliza un intervalo *hello* de 60 segundos. Las interfaces de ancho de banda mayor o igual a T1, y LAN. EIGRP utiliza un intervalo *hello* de 5 segundos en tales interfaces. Un router EIGRP debe de aguantar un periodo finito antes de concluir que un vecino en silencio está realmente fuera de servicio. Este periodo se conoce como *hold-time*, al que hace un seguimiento el temporizador *hold*. Si el temporizador *hold* efectúa una cuenta atrás hasta cero y no ha tenido todavía noticia de un vecino, ese *router* informa a DUAL del cambio. DUAL inicia la convergencia entre los *routers* restantes de la red. El valor de *hold* time está predeterminado generalmente a tres veces el tiempo de inmovilización de una interfaz. Por tanto, el valor predeterminado de *hold* time es 180 y 5 segundos, respectivamente, para interfaces de ancho de banda bajo y alto. Los paquetes *hello* se mandan a través de multidifusión con la IP 224.0.0.10.

Paquetes de acuse de recibo. Se usan para confirmar la entrega de cualquier paquete EIGRP que requiera entrega fiable, debe confirmarse la recepción de un paquete para que pueda considerarse una entrega fiable. La entrega de paquetes es por medio de unidifusión.

Paquetes de consulta y de respuesta. Los paquetes de consulta se utilizan siempre que un *router* necesita información específica de uno o de todos sus vecinos. Para responder a una consulta, se utiliza un paquete de respuesta, las consultas pueden ser tanto de unidifusión como de multidifusión. Con independencia de qué tipo de dirección se utilice, las consultas se transmiten siempre fiablemente y las respuestas también.

5.5 Protocolo OSPF

El Protocolo primero la ruta más corta (*Open Shortest Path First*). El IETF desarrolló el protocolo de enrutamiento OSPF durante los últimos años de 1980 en respuesta a la creciente necesidad de construir redes basadas en IP cada vez más grandes, OSPF era en cierta manera, una versión abierta de la clase SPF de protocolos de enrutamiento basados en el algoritmo matemático de Dijkstra. La primer responsabilidad de un *router* que usa estado enlace es crear una base de datos que refleje la estructura de la red. Los protocolo de estado enlace aprenden más información en la estructura de la red más que en otros protocolos, y de esta manera estar disponible para tomar mejores decisiones de enrutamiento. El OSPF fue especificado en el RFC 1131. Esta primera versión (OSPF versión 1) fue rápidamente sustituida por una versión muy mejorada que se documentó en el RFC 1247 OSPFv2 sufriendo modificaciones subsecuentes en los RFCs 1583, 2178 y 2328. OSPF es un estándar abierto, es un protocolo de enrutamiento sin clase (*classless*) y usa el coste (*bandwith*) como métrica.

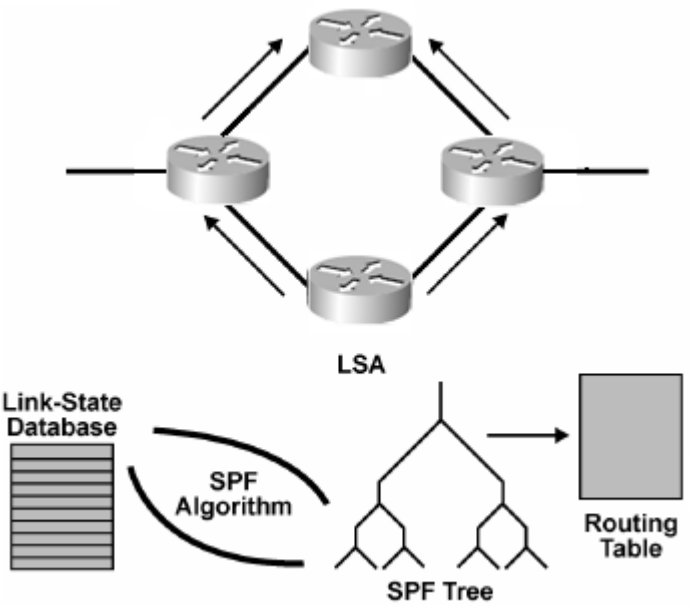

Figura 5.4. OSPF, protocolo de estado enlace.

5.5.1 Areas OSPF

Una de las razones clave para la rapidez de la convergencia de OSPF es su uso de las áreas. Los dos objetivos principales que el IETF pretendió con OSPF fueron:

- Escalabilidad de red mejorada
- Tiempos de convergencia rápidos

La clave de ambos objetivos reside en la compartimentación de una red en regiones más pequeñas. Estas regiones se conocen como áreas. Un área es una colección de sistemas finales conectados en red, routers y servicios de transmisión cada área esta definida con un número de área único configurado en cada router. Las interfaces de router definidas con el mismo número de área llegan a ser parte de la misma área. Idealmente, estas áreas no están definidas arbitrariamente. En su lugar, los límites de un área deberían seleccionarse para minimizar la cantidad de tráfico entre diferentes áreas.

El número de áreas de una red OSPF que puede soportar está limitado por el tamaño de su campo ID de área. Este campo es un número de 32 bits. Por tanto, el número máximo teórico de redes es 4.294.967.295 pero obviamente, el número práctico de áreas que puede soportar una red es mucho menor que este máximo teórico. En la práctica, el número máximo de áreas que puede soportar vendrá determinado por lo bien que esté diseñado la red. La figura 5.5 ilustra una red OSPF con tres áreas.

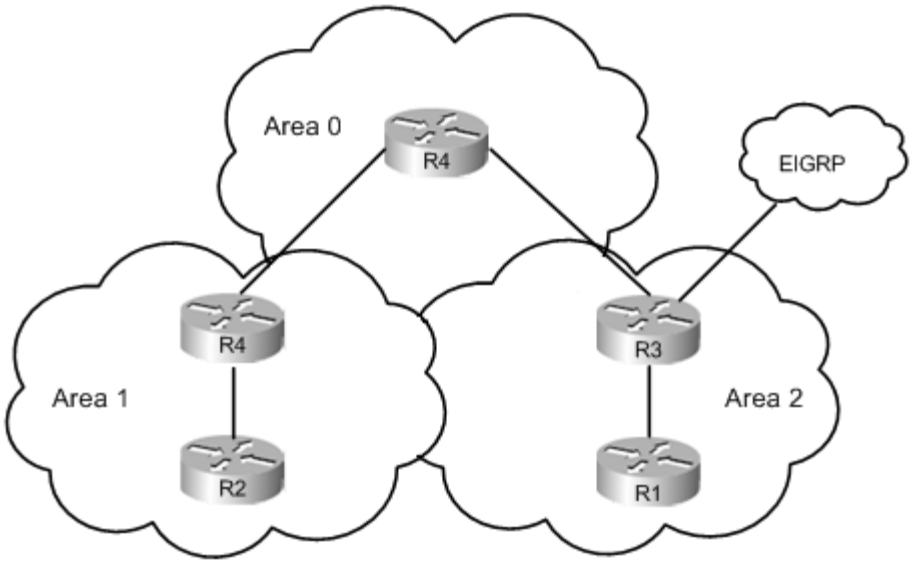

Figura 5.5 Estructura de Red OSPF.

5.5.2 Tipos de *routers* OSPF

En OSPF los enlaces y las interfaces de *router* que conecta están definidos como miembros de un área. Basándose en su pertenencia a un área, puede haber tres tipos diferentes de *routers* dentro de una red OSPF:

- Routers internos
- Routers fronterizos (*Area Border Router ABR*)
- Routers *backbone*

Tomando como referencia la figura anterior, un *router* con múltiples interfaces puede pertenecer a dos o más áreas y se denomina *router* fronterizos o ABR. Es decir, son *routers* que interconectan el *backbone* y los miembros de su área. Un *router backbone* es el que tiene al menos una interfaz definida como perteneciente al Area 0. Es posible para un *router* fronterizo ser también un *router* backbone. Cualquier *router* fronterizo que interconecte un área numerada con el Área 0 es a la vez *router* fronterizo y *backbone*. Un *router*

interno tiene todas las interfaces definidas en la misma área, pero no como área 0. Existe también Un Router Frontera de Sistema Autónomo (*Autonomous System Boundary Router ASBR*) que tiene interfaces dentro y fuera de un domino de enrutamiento de OSPF, en este caso el R3 es un ASBR porque tiene una interfaz en un dominio de enrutamiento EIGRP. Utilizando estos tipos de *routers*, es posible construir redes muy eficientes y escalables. Dividiendo una red OSPF en áreas se obtiene lo siguiente:

- Minimiza el numero de entrabas en la tabla de enrutamiento
- Contiene la inundación de LSAs a un área razonable.
- Minimiza el impacto de un cambio de topología.
- Forza el concepto de diseño de red jerárquico

5.5.3 Metrica OSPF

De manera predeterminada, Cisco asigna un coste a cada interfaz que el cual es inversamente proporcional a 100 Mbps. El coste de cada enlace es entonces aumentado conforme atraviesa la red. A continuación se muestra la formula de métrica de OSPF:

$$Cost = \frac{100\ Mbps}{\text{Bandwidth}}$$

La formula predeterminada no diferencia entre interfaces con velocidades arriba de 100 Mbps. Esta asigna el mismo coste a una interfaz FastEthernet y a una GigaEthernet por ejemplo. En muchos casos el coste puede ser ajustado en el proceso de OSPF, los valores para ancho de banda (en kbps) arriba de 4,294,967 son permitidos. El coste también puede ser manualmente asignado en la configuración de la interfaz. El coste es un número de 16-bits, así que puede ser cualquier valor de 1 a 65,535.

5.5.4 Tipos de enrutamiento OSPF

OSPF soporta dos tipos diferentes de enrutamiento:

- Enrutamiento dentro de un área.
- Enrutamiento entre áreas.

El enrutamiento dentro de un área es autocontenido y limitado sólo a los *routers* internos de una sola área.

El enrutamiento entre áreas requiere el intercambio de datos entre diferentes áreas y todo el enrutamiento debe ser conducido a través del área 0. Los números de área distintos a 0 no pueden comunicarse entre sí.

5.5.5 Enrutamiento entre redes

OSPF también puede utilizarse para comunicar la información de enrutamiento entre redes OSPF más que sólo entre áreas dentro de una sola red. Y también para interconectar redes separadas. Dichas redes pueden ser otra red OSPF completa o una que utilice un protocolo de enrutamiento completamente diferente. La interconexión de una red OSPF con un protocolo de enrutamiento diferente es una tarea complicada, y utiliza una técnica conocida como redistribución de rutas. La información de enrutamiento desde la red no-OSPF se resume y redistribuye en la red OSPF. La red OSPF etiqueta todas las rutas aprendidas de esta manera como externas. La interconexión de dos redes OSPF diferentes es más fácil, porque no hay necesidad de convertir una información de coste de ruta del protocolo de enrutamiento en un formato que el otro protocolo pueda entender. Además, OSPF permite la creación de sistemas autónomos (AS). Aparentemente, un AS presentaría un solo administrador de red o grupo de administradores, y utilizaría un solo protocolo de enrutamiento.

OSPF permite la asignación de un número de AS a una red. Una red OSPF muy grande podría segmentarse en dos o más sistemas autónomos. Estos sistemas autónomos se interconectarían mediante el cuarto tipo de *router* OSPF, el *router* ASBR quien resume toda la información de enrutamiento para su AS y envía ese resumen a su ASBR equivalente del AS vecino.

5.5.6 Actualizaciones de enrutamiento

Los OSPF *routers* OSPF intercambian *hellos* con cada vecino. Aprendiendo su *Router* ID y su costo. La información del vecino se mantiene en la base de datos de adyacencias. Una de las razones por las que OSPF es tan escalable es por sus mecanismos de actualización de enrutamiento. OSPF utiliza un LSA (*Link State Advertisements*) para compartir la información de enrutamiento entre nodos OSPF. Estas publicaciones se propagan completamente a través de un área, pero no más allá de un área. Por tanto, cada *router* dentro de un área dada conoce la topología de su área. No obstante, la topología de cualquier área concreta es conocida fuera de esa área. Dado que hay realmente cuatro tipos diferentes de *routers* OSPF (*router* interno, *router* ABR, ASBR y *router backbone*), está claro que cada tipo de *router* tiene un conjunto diferente de iguales (*peerings*) con los que debe intercambiarse los LSAs.

Cada *router* mantiene la tabla completa de LSAs en una tabla de Base de Datos de Estado Enlace (*Link State Database* LSDB). Cada *router* ejecuta el algoritmo SPF para calcular las mejores rutas. Esto para incluirlas en la tabla de enrutamiento o base de datos de reenvío (*forwarding database*).

5.5.7 Tipos de Paquete OSPF

OPSF usa diferente tipos de mensajes para establecer y mantener las relaciones de vecindad. Y mantener correcta la información de enrutamiento.El

paquete de actualización del estado del enlace se utiliza para transportar realmente los LSA a los nodos vecinos. Estas actualizaciones son generadas en respuesta a una solicitud LSA. No usa UDP o TCP para transmitir sus paquetes. En lugar de eso ejecuta sobre IP (Protocolo IP 89), usando un encabezado OSPF. Un campo en este encabezado identifica el tipo de paquete que esta siendo transportado. Hay cinco tipos de paquetes y están identificados por un número de tipo, dentro del intervalo del 1 al 5. Cada uno de ellos está destinado a soportar una función diferente, altamente específica, dentro de la red:

- Paquetes *hello* (Tipo 1).
- Paquetes de descripción de la base de datos (Tipo 2 *Database Description DBD*)
- Paquetes de solicitud del estado del enlace (Tipo 3 Link *State Request LSR*).
- Paquetes de actualización del estado del enlace (Tipo 4 *Link State Update LSU*.).
- Paquetes de acuse de recibo del estado del enlace (Tipo *5 Link State Acknowledgment LSAck*).

El tráfico OSPF se envía vía multidifusión a las direcciones: 224.0.0.5 para todos los *routers* OSPF o 224.0.0.6 para todos los OSPF DRs (*Routers* Designados).

5.5.8 Relaciones de vecindad OSPF

Los *routers* OSPF envían periódicamente paquetes multidifusión para incluirse ellos mismos a otros *routers* en un enlace. Ellos llegan a ser vecinos cuando ven su *router* ID incluido en el *hello* de otro *router*. Identificando esto le informa a cada *router* que tienen comunicación bidireccional. Adicionalmente,

dos *routers* deben estar en una subred común para que la vecindad sea formada, enlaces virtuales son algunas veces la excepción a esta regla.

Ciertos parámetros con los *hellos* de OSPF deben también coincidir para que dos routers se conviertan en vecinos, los cuales son:

- *Hello*/dead timers
- Area ID
- Tipo de autenticación y contraseña
- Stub area flag.

Los *routers* OSPF pueden ser vecinos son ser adyacentes. Solo vecinos adyacentes intercambian actualizaciones de enrutamiento y sincronizar sus bases de datos. En un enlace punto a punto, una adyacencia es establecida entre los dos *routers* cuando ellos pueden comunicarse. En un enlace multiacceso, cada *router* establece una adyacencia solo con el DR (Router Designado) y el DR de respaldo (BDR).

También los mensajes *hellos* sirven como *keepalives* para mantener la vecindad, un vecino es considerado perdido si no recibe *hellos* dentro de cuatro periodos de *hellos* (llamado *dead time*). Los tiempos predeterminados de los *hellos/dead timers* son:

10 segundos/40 segundos para LAN y para interfaces punto a punto.
30 segundos/120 segundos para interfaces *Nonbroadcast multiaccess* (NBMA).

Establecer vecinos e Intercambiar rutas.

El proceso de establecer vecindad e intercambiar rutas entre dos *routers* OSPF es como sigue:

Paso1. *Down State*. El proceso OSPF no ha empezado, así que no se envían *hellos*.

Paso2. *Init State*. El *router* envía paquetes *hello* fuera de todas las interfaces OSPF.

Paso3. *Two-way state*. El *router* recibe un paquete *hello* de otro *router* que contiene su propio *router* ID en la lista de vecinos. Si Todos los otros elementos concuerdan los *routers* pueden llegar a ser vecinos.

Paso 4. *Exstart state.* Si los *routers* llegan a ser adyacentes (intercambian rutas), ellos determinan quien empezará el proceso de intercambio.

Paso 5. *Exchange state.* Los routers Intercambian Vds. Listando los LSAs en su LSD por RID y número de secuencia.

Paso6. *Loading State.* Cada *router* compara la DBD recibida a los contenidos de su Base de datos LS.

Paso 7. *Full state.* El LSDB ha sido sincronizado con el vecino adyacente.

Router ID . El algoritmo SPF es usado para mapear el camino más corto entre una serie de nodos. Esto causa un problema con IP porque un *router* IP no esta identificado por una solo dirección IP, sus por las interfaces sí. Debido a esta razón, una sencilla dirección IP es designada como el nombre del router, es decir el RID. De manera predeterminada, el RID es la IP más alta de las *loopbacks*. Si no hay interfaces *loopbacks* configuradas, el RID es la IP más alta de las Interfaces activas cuando el proceso de OPSF inicia. El RID es seleccionado cuando OSPF inicia y por razones de estabilidad no es cambiado hasta que OSPF se reinicie.

5.5.9 Tipos de Red OSPF

El algoritmo SPF construye una ruta grafica hecha de una serie de puntos conectados por enlaces directos. Una de las consecuencias de esto es que el algoritmo no tiene manera de manejar una red multiacceso, como en una Vlan Ethernet. La solución es elegir a un *router* llamado *Router* Designado (DR)

a representar un segmento entero. Enlaces punto a punto se amoldan al modelo SPF perfectamente y no necesitan un método especial. En un enlace punto a punto, el DR no es elegido y todo tráfico es multiacceso a la IP 224.0.0.5. OSPF soporta cinco tipos de redes:

- NBMA.
- Point-to–multipoint (P2MP)
- Point-to-multipoint nonbroadcast (P2MNB)
- Broadcast.
- Point-to–point (P2P)

5.5.10 Sumarización OSPF

OSPF soporta sumarización con VLSM y CIDR, y a su vez esta característica le ayuda a manejar los recursos del *router*, ya que cuando se ejecuta el algoritmo SPF se eleva el CPU y así si la sumarización previene que cambios de topología sean comunicados fuera del área y tenga que ser ejecutado el algoritmo SPF. Las Múltiples Bases de datos usan mucha memoria, la sumarización decrece el número de rutas intercambiadas y por ende el tamaño de las bases de datos.

5.6 *Intermediate System-to-Intermediate System (IS-IS)*

IS-IS es un protocolo de estado enlace que es parte de la familia de protocolos de OSI. Usa el algoritmo SPF de Dijkstra para determinar las rutas. IS-IS es un protocolo sin clase (classless). IS-IS puede transportar información de red IP pero no usa IP como su protocolo de transporte, usa protocolos OSI como CLNS (*Connectionless Network Service*) y CLNP (*Connectionless Network Protocol*) para entregar sus actualizaciones así también usa CLNS

para identificar a los *routers* y construir la Base de Datos de estado enlace (LSDB).

Las especificaciones de ISO refieren a los *routers* como Sistemas Intermedios (ISs). Entonces IS-IS es un protocolo que permite a los *routers* comunicarse con otros *routers*. A continuación se enlistan las principales características de IS-IS.

5.6.1 Características de IS-IS:

- Protocolo de estado enlace
- Soporta VLSM
- Usa el algoritmo SPF de Dijkstra; Tiene rápida convergencia.
- Usa *Hellos* para establecer adyacencias y *LSPs* para intercambiar información de estado enlace.
- Eficiente uso de ancho de banda, memoria y CPU.
- Soporta dos niveles de enrutamiento:
    - Level 1: Construye una topología común de System IDs en area local y rutas dentro del *area* usando la ruta con más bajo coste.
    - Level 2: Intercambia información de prefijos (direcciones de *area*) entre *areas*, enruta tráfico al *area* usando la ruta con el coste mas bajo.

5.6.2 Tipos de *Routers* IS-IS

En la figura 5.6 se muestra una red IS-IS dividida en áreas. En IS-IS no hay un área en específico como en OSPF. Dentro de un área los *routers* pueden ser de 3 tipos:

- **Level 1 (L1) *router***. En la figura R1, R2 y R5 enrutan a redes solo dentro de un área local (enrutamiento intra-área). Usa una ruta predeterminada al *router* más cerca de Level 2 para que el tráfico salga del área. Mantiene una Base de Datos LSDB para el área local. Cuando se enruta compara el área destino a su área, si es el mismo enruta basado en *System* ID, si no envía el tráfico a un *router* Level 1-2.

- **Level 2 (L2) *router*.** En la figura R6, enruta a redes en otras áreas (enrutamiento interarea). El enrutamiento esta basado en el área ID. Mantiene una Base de Datos LSDB para enlutar a otras áreas.

- **Level 1-2 (L1-2) *router***. En la figura R3 and R4, actuan como un *gateway* dentro y fuera de un área. Es Level 1 dentro del área y Level 2 para enrutar entre áreas. Mantiene dos Base de Datos LSDB, una para el área local y otra para enrutamiento interarea.

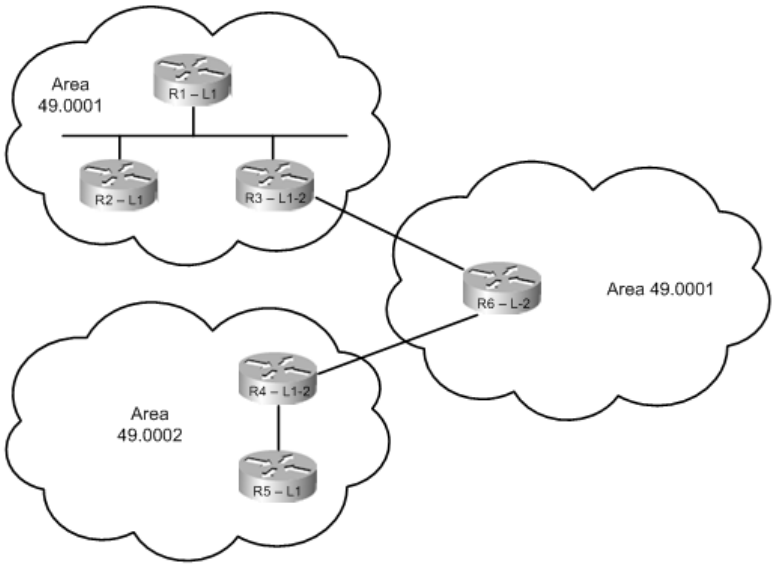

Figura 5.6. Enrutamiento entre áreas IS-IS

5.6.3 Enrutamiento IS-IS Integrado o DUAL

A continuación se enlistan algunas características del Enrutamiento IS-IS Integrado:

- Integra IS-IS para múltiple protocolos: Para IP, CLNS o ambos.
- Usa sus propio PDUs para transportar información de enrutamiento IP; las actualizaciones no se envían en paquetes IP.
- Requiere direcciones CLNS, aun si solo se esta enlutando IP.

5.6.4 Estructura de Direcciones NSAP

En la implementación CISCO de IS-IS Integrado, direcciones NSAP tienen tres partes: el área ID, el *system* ID, y el NSEL. Son escritos en hexadecimal y tienen un máximo de tamaño de 20 bytes. A continuación se ilustra la estructura de una dirección NSAP:

49.0234.0987.000.2211.00

Area ID – Longitud de 1 a 13 bytes	System ID – Debe ser exactamente de 6 bytes de longitud	NSEL – 1 byte

5.7 Protocolo de *Gateway* Fronterizo BGP

Protocolos externos

Los protocolos de enrutamiento exterior fueron creados para controlar la expansión de las tablas de enrutamiento y para proporcionar una vista mas estructurada de Internet mediante la división de dominios de enrutamiento administraciones separadas, llamadas sistemas autónomos (*Autonomous Systems* AS), los cuales tienen cada uno sus propias políticas de enrutamiento e IGP únicos.

Anteriormente cuando iniciaba Internet se utilizaba un protocolo de *gateway* exterior llamado EGP, utilizado para intercambiar información de accesibilidad entre el *backbone* y las redes regionales. Aunque el uso de EGP estaba ampliamente desplegado, sus restricciones de topología e ineficiencia en lo referente a *loops* de enrutamiento y establecimiento de políticas de enrutamiento, crearon la necesidad de un protocolo nuevo y más robusto. Actualmente BGP-4 es el estándar para el enrutamiento entre dominios en Internet.

La principal diferencia entre el enrutamiento dentro de un AS y entre un AS es que el enrutamiento dentro de un SA normalmente se optimiza de acuerdo con las demandas técnicas exigidas, mientras que el enrutamiento entre SA normalmente refleja relaciones políticas y de negocios entre las redes y las empresas involucradas.

Un sistema autónomo (AS). Es un conjunto de *routers* que tiene una única política de enrutamiento, que se ejecuta bajo una única administración técnica, y que habitualmente utiliza un único IGP (el AS podría ser también un conjunto de IGPs trabajando juntos para proporcionar enrutamiento interior). Para el mundo exterior, el AS es visto como una única entidad. Cada AS tiene

un número identificador, que se le asigna mediante un Registro de Internet, o un proveedor de servicios en el caso de AS privados. La información de enrutamiento entre varios AS se intercambia mediante un protocolo de *gateway* exterior como BGP-4, según se muestra en la figura 5.7.

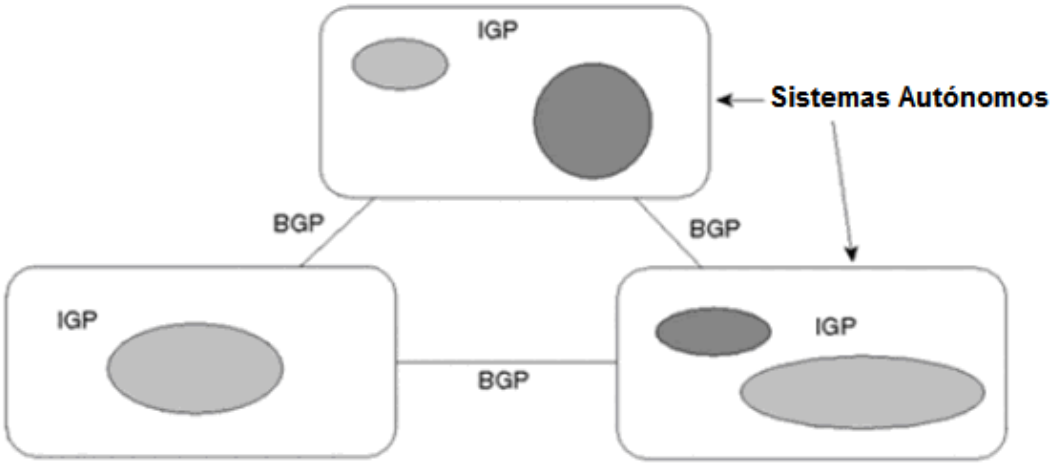

Figura 5.7 Intercambio de Información de enrutamiento entre ASs.

Lo que se ha obtenido de dividir el mundo en administraciones es la capacidad de tener una gran red dividida en redes más pequeñas y manipulables. Dichas redes, representadas como AS, pueden implementar su propio conjunto de reglas y políticas que distinguirán particularmente sus redes y los servicios asociados ofrecidos de otras redes. Cada AS puede ejecutar su propio conjunto de IGP, independientemente de los IGP de otros SA. A continuación se mencionan algunas modalidades en que un AS se interconecta a Internet:

AS de conexión única. Es cuando un AS alcanza las redes exteriores a su dominio a través de un único punto de salida. Estos AS se denominan también como de conexión única con respecto a otros proveedores. Un AS de conexión única no tiene que aprender realmente las rutas de Internet de su proveedor. Dado que sólo hay una salida, todo el tráfico puede ir por defecto al

proveedor. Cuando se usa esta configuración, el proveedor puede utilizar diferentes métodos para publicar las rutas del cliente a otras redes. Una posibilidad para el proveedor es enumerar las subredes del cliente como entradas estáticas en su *router*. El proveedor publicará entonces dichas entradas a Internet a través de BGP. Este método escalaría muy bien si las rutas del cliente pudieran representarse mediante un conjunto pequeño de rutas agregadas. Cuando el cliente tiene demasiadas subredes no contiguas, enumerar todas esas subredes por medio de rutas estáticas resulta ineficaz.

Alternativamente, el proveedor puede emplear IGP para publicar las redes del cliente. Puede utilizarse un IGP entre el cliente y el proveedor para que el cliente publique sus rutas. Esto tiene todos los beneficios de enrutamiento dinámico donde la información de red y los cambios son enviados dinámicamente al proveedor. Sin embargo, esto es muy poco común, principalmente porque no se escala muy bien debido a que la inestabilidad del enlace del cliente puede dar lugar a inestabilidades IGP.

El tercer método por el cual el ISP puede aprender y publicar las rutas del cliente consiste en utilizar BGP entre el cliente y el proveedor. En la situación de un AS de conexión única, es difícil obtener el número de un AS registrado porque las políticas de enrutamiento del cliente son una extensión de las políticas de un único proveedor. En su lugar. El proveedor puede otorgar al cliente un número de SA de la colección de sistemas autónomos (65412-65535), asumiendo que las políticas de enrutamiento del proveedor ha establecido soporte para usar espacio privado de los AS con los clientes.

AS de múltiples conexiones sin transito. Un AS es de múltiples conexiones si tiene más de un puerto de salida hacia el exterior. Un AS puede tener múltiples conexiones hacia un único proveedor o hacia varios proveedores. Un AS sin tráfico no permite tráfico de tránsito a través de él. El tráfico de tránsito es cualquier tráfico que tenga origen y destino fuera del AS.

Un SA sin tránsito sólo publicará sus propias rutas y no propagará rutas que haya aprendido de otros AS. Esto asegura que el tráfico hacia cualquier destino que no pertenezca al AS no será dirigido hacia el SA. Los AS sin tránsito y con múltiples conexiones no necesitan realmente ejecutar BGP con sus proveedores, aunque es recomendable y la mayor parte del tiempo es requerido por el proveedor. Ejecutar BGP-4 con los proveedores tiene muchas ventajas, como controlar la propagación y el filtrado de rutas.

SA de tránsito con múltiples conexiones. Un SA de tránsito con múltiples conexiones tiene más de una conexión con el exterior y todavía puede ser utilizado para el tráfico de tránsito por otros AS. El tráfico de tránsito (relativo al AS con múltiples conexiones) es cualquier tráfico que tenga un origen y un destino que no pertenezca al AS local. Aunque BGP es un protocolo de *gateway* exterior, también puede utilizarse dentro de un AS como un conducto para intercambiar actualizaciones de BGP. Las conexiones BGP entre *routers* dentro de un sistema autónomo son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre *routers* en sistemas autónomos separados son denominadas BGP externo (EBGP). Los *routers* que están utilizando IBGP se denominan *routers* de tránsito cuando transportan el tráfico de tránsito que va a través del AS.

Un AS de tránsito publicará a un AS las rutas que haya aprendido de otro AS. De esta forma, el AS de tránsito se abrirá al tráfico que no le pertenezca, es aconsejable que los AS de tránsito de múltiples conexiones utilicen BGP-4 para sus conexiones a otros AS y para proteger sus *routers* internos sin tránsito de las rutas de Internet. No todos los *routers* dentro de un dominio necesitan ejecutar BGP; los *routers* internos sin tránsito pueden ejecutar un enrutamiento predeterminado hacia los *routers* BGP, lo que alivia el número de rutas que los *routers* internos sin tránsito deben transportar. Sin embargo, en la mayoría de las grandes redes de los proveedores de servicios, todos los *routers* transportan habitualmente un conjunto lleno de rutas BGP internamente.

BGP ha definido las bases de las arquitecturas de enrutamiento a Internet. La división de las redes en sistemas autónomos ha definido lógicamente las fronteras administrativas y políticas entre las empresas. Los Protocolos de *gateway* interior pueden ejecutarse independientemente unos de otros, pero las redes todavía pueden interconectarse a través de BGP para proporcionar enrutamiento global.

BGP versión 4

El protocolo de *gateway* fronterizo (*Border Gateway Protocol* BGP) ha pasado por diversas fases y mejoras desde su versión original, BGP-1, en 1989. La distribución de BGP-4 comenzó en 1993. Es la primera versión de BGP que administra la agregación (enrutamiento entre dominios sin clase CIDR) y las superredes. BGP no impone restricciones sobre la topología de red subyacente. Asume que el enrutamiento dentro de un sistema autónomo se hace mediante un protocolo de enrutamiento intra-sistema autónomo (Protocolo de *gateway* interior IGP). BGP construye un gráfico de sistemas autónomos basados en la información intercambiada entre los *routers* BGP. Este entorno grafico se denomina en ocasiones árbol. En lo que concierne a BGP, Internet es un gráfico de ASs, con cada AS identificado por un número de AS único. Las conexiones entre dos AS juntos forman una ruta de acceso, y el conjunto de información de rutas de acceso forma una ruta para llegar a un destino específico. BGP utiliza la información de ruta de acceso asociada con un destino dado para asegurar el enrutamiento entre dominios libre de *loops*.

5.7.1 Como trabaja BGP

BGP es un protocolo por vector de ruta utilizado para transportar información de enrutamiento entre sistemas autónomos. El término vector de ruta viene del hecho de que la información de enrutamiento de BGP transporta una secuencia de números de SA que identifica la ruta de SA que un prefijo de

red ha seguido. La información de ruta de acceso asociada con el prefijo se utiliza para activar la prevención de *loops*. BGP utiliza TCP como su protocolo de transporte (puerto 179). Esto asegura que toda la seguridad del transporte (como la retransmisión) queda al cuidado de TCP y no necesita ser implementada en BGP, simplificando así la complejidad asociada con la fiabilidad de diseño en el propio protocolo. Los *routers* que ejecutan un proceso de enrutamiento BGP a menudo se conocen como portavoces (*speakers*) BGP. Dos portavoces (*speakers*) BGP que forman una conexión TCP entre ambos con el propósito de intercambiar información de enrutamiento se denominan vecinos (*neighbors*) o iguales (*peers*). Los *routers* de iguales intercambian mensajes abiertos para determinar los parámetros de conexión. Estos mensajes son utilizados para comunicar valores como el número de versión del portavoz BGP.

BGP también proporciona un mecanismo para cerrar elegantemente una conexión con un igual. En otras palabras, en caso de desacuerdo entre iguales, sea resultante de configuración, incompatibilidad, intervención de operador u otras circunstancias se envía un mensaje de error NOTIFICATION, y la conexión al igual no se establece o se corta si ya estaba establecida. El beneficio de este mecanismo es que ambos iguales comprenden que la conexión no puede ser establecida o mantenida, por lo que no se desperdician recursos que de otra forma serían requeridos para mantener o reintentar establecer la conexión a ciegas. El mecanismo de cierre elegante simplemente asegura que todos los mensajes pendientes, principalmente mensajes de error NOTIFICATION, sean entregados antes de que se cierre la sesión TCP.

Inicialmente, cuando se establece una sesión de BGP entre un conjunto de portavoces BGP, todas las rutas BGP candidatas son intercambiadas. Después de haber establecido la sesión y se haya producido el intercambio de la ruta inicial, sólo se envían las actualizaciones incrementales como cambios en la información de la red. El enfoque de actualización incremental ha

demostrado una mejora enorme en el gasto de CPU y asignación de ancho de banda en comparación con las periódicas actualizaciones completas utilizadas por los anteriores protocolos, como EGP.

5.7.2 Características de BGP

- BGP es más apropiado cuando al menos una de las siguientes condiciones existe:
    - Un AS permite a los paquetes a transitar a través de él a otro AS.
    - Un AS tiene múltiple conexiones a otro AS.
    - Políticas de enrutamiento y selección de ruta para entrante y saliente al AS puede ser manipulado.
- BGP no es siempre apropiado. No se tiene que usar BGP si se tienen las siguientes condiciones:
    - Limitado entendimiento de filtrado de rutas y del proceso de selección de la mejor ruta.
    - Una sencilla conexión a Internet u otro AS.
    - Carencia de recursos en el *router* (Memoria, CPU) para manejar constantes actualizaciones en los *routers* BGP.
- BGP es un protocolo vector ruta con las siguientes mejoras sobre los protocolos vector distancia:
    - Actualizaciones Confiables: BGP ejecuta sus mensajes por TCP (puerto 179).
    - Incrementa, solo actualizaciones disparadas.
    - Periódicos mensajes *keepalives* para verificar conectividad TCP.
    - Métricas enriquecidas (llamadas vectores de ruta o atributos).
    - Diseñado para escalar grandes *internetworks*.

5.7.3 Bases de Datos de BGP

- **Tabla de Vecinos.** Lista la tabla de Vecinos BGP.
- **Tabla BGP (Base de datos de envío).** Lista todas las redes aprendidas de cada vecino. Puede contener múltiples rutas a redes destino. Contiene los atributos BGP para cada ruta.
- **Tabla de enrutamiento IP.** Lista las mejores rutas a redes destino.

5.7.4 Mensajes BGP

BGP define los siguientes tipos de mensajes:

- ***Open.*** Incluye el tiempo de espera y el *Router* ID BGP.
- ***Keepalive.***
- ***Update.*** Información para una sola ruta (puede ser a múltiples redes). Incluye atributos de ruta y redes.
- ***Notification***. Cuando un error es detectado. También cuando la conexión es cerrada después de haber sido enviado.

- Los términos clave para describir relaciones entre *routers* ejecutando BGP son las siguientes: BGP Altavoz (*speaker*) o BGP *router*; BGP igual (*peer*) o vecino (*neighbor*)
- IBGP y EBGP
  Los vecinos EBGP están directamente conectados a *routers* en diferente AS.
  Los vecinos IBGP son vecinos en el mismo AS que están alcanzables por rutas estáticas o algún IGP.
- Todos los *routers* en la ruta de transito dentro de un AS se deben ejecutar en alta disponibilidad

5.7.5 Selección de ruta BGP

IGPs como EIGRP u OSPF, escogen las rutas basadas en la métrica más baja, ellos intentan encontrar el más corto, el más rápido camino para llegar al destino. BGP sin embargo tiene una forma diferente de selección de ruta. Este asigna varios atributos para cada ruta, estos atributos pueden ser administrativamente manipulados para controlar la ruta que es seleccionada.

5.7.6 Atributos BGP

Well-known mandatory. Deben ser reconocidos por todos los *routers* BGP, presentes en todas las actualizaciones BGP, y pasados a otros *routers* BGP. Por ejemplo: *AS path*, *origin*, y *next hop*

Well-known discretionary. Deben ser reconocidos por todos los *routers* BGP y pasados a otros *routers* BGP. Pero no necesitan estar presentes en una actualización. Por ejemplo: *local preference*.

Optional transitive. Puede o no puede ser reconocido por un *Router* BGP, pero es pasado a otros BGP *routers*, si no es reconocido, es marcado como parcial. Por ejemplo: *aggregator, community*.

Optional nontransitive. Puede o no puede ser reconocido por un *Router* BGP, pero no es pasado a otros BGP *routers*, si no es reconocido, es marcado como parcial. Por ejemplo: *MED, originator ID*.

Los atributos (*attributes*) de BGP informan a los *routers* BGP de recibir actualizaciones acerca de cómo tratar las rutas a la red final. Los Atributos BGP son las métricas para seleccionar la mejor ruta. Los atributos BGP incluyen los siguientes:

- AS path *
- Next-hop *
- Origin *
- Local preference
- MED
- Others

**Well-Known mandatory*

Atributo	**Significado**
AS path*	Una lista ordenada de todos los AS a través de los cuales la actualización ha pasado.
Origin*	Como BGP aprendió la red.
Next hop*	La IP del *router* vecino de BGP.
Local preference	Un valor que indica a los *peers* IBGP cual ruta seleccionar para el tráfico saliente al AS.
MED	Sugiere al AS vecino cual de las múltiples rutas a seleccionar para tráfico seguro en el AS.
Weight	Propietario de Cisco, le dice al *router* cual de las múltiples rutas locales seleccionar para trafico saliente al AS

Tabla 5.1. Atributos BGP.

5.7.7 Criterios para selección de ruta en BGP

- Prefiere el peso (*weight*) más alto (local al *router*).
- Prefiere la preferencia local (*local preference*), global dentro del AS.
- Prefiere las rutas que el *router* originó.
- Prefiere las rutas del AS mas corto (solo la longitud es comparada).
- Prefiere el código origen más bajo (IGP < EGP < Incompleta)
- Prefiere el MED más bajo.
- Prefiere rutas externas (EBGP) sobre rutas internas (IBGP).

- Para rutas IBGP, prefiere rutas a través del vecino IGP más cerca.
- Para rutas EBGP prefiere la ruta más antigua (más estable).
- Prefiere rutas del *router* con el BGP *Router* ID más bajo.

5.7.8 Autenticación BGP

BGP soporta autenticación MD5 entre vecinos, usando una contraseña compartida.

5.7.9 Multihomming

Significa conectarse a más de un *ISP* al mismo tiempo. Esto es por redundancia en caso de que un *ISP* falle y para un mejor desempeño si uno de los *ISPs* provee una mejor ruta a redes que se usan frecuentemente.

Existen tres formas de recibir rutas de cada ISP:

Rutas predeterminadas de cada ISP. Esto resulta en un bajo uso del ancho de banda y de los recursos del router, La métrica interna de la red IGP determina el router de salida para todo el trafico fuera del AS.

Rutas predeterminadas más algunas rutas específicas al ISP. Esto resulta en un uso medio de ancho de banda y recursos. Esto permite manipular la ruta de salida para específicas redes usando BGP, pero la métrica IGP escoge la ruta de salida para rutas predeterminadas.

Todas las rutas de todos los proveedores. Esto requiere un alto uso de ancho de banda y de recursos del *router*. Es típicamente utilizado por grandes empresas e *ISPs*. La selección para todas las rutas externas puede ser controlada vía herramientas de políticas de enrutamiento BGP.

CAPITULO 6

POLITICAS DE ENRUTAMIENTO

Optimizar el Enrutamiento

A veces que se necesita más que activar un protocolo de enrutamiento en la red, se necesita usar múltiples protocolos, controlar exactamente que rutas son anunciadas o redistribuidas o cuales caminos escoger hacia el destino.

6.1 Usando Múltiples Protocolos de enrutamiento

Hay varias razones por las que se puede necesitar ejecutar múltiples protocolos de enrutamiento en la red, algunos son:

- Migrar de un protocolo de enrutamiento a otro, donde ambos protocolos se ejecuten en la red simultáneamente.
- Aplicaciones que se ejecutan bajo cierto protocolo de enrutamiento y no en otros.
- Áreas de la red bajo diferente control administrativo.
- Un ambiente multi-fabricante en el cual algunas partes de la red requieran un protocolo estándar.

6. 2 Configurar Redistribución de rutas

Sí la información de enrutamiento debe ser intercambiada a través de de diferentes protocolos o dominios de enrutamiento, la redistribución puede ser utilizada. Solo rutas que están en la tabla de enrutamiento y aprendidas vía un específico protocolo son redistribuidas.

Protocolo	**Características de Redistribución**
RIP	La métrica debe de ser fijada, excepto cuando se redistribuyen rutas estáticas o conectadas, las cuales tienen métrica de 1.
OSPF	La métrica predeterminada es 20. Se puede especificar el tipo de métrica, la predeterminada es E2. Se debe usar subredes claves o solo redes *classful* son redistribuidas.
EIGRP	La métrica debe ser fijada, excepto cuando se redistribuyen rutas estáticas o conectadas, las cuales consiguen su métrica de las interfaces. El valor de métrica es ancho de banda, retraso, confiabilidad, carga, MTU. Rutas redistribuidas tienen una distancia administrativa más alta que las internas.
IS-IS	La métrica predeterminada es 0. Se puede especificar el Nivel, de manera predeterminada es L2. Se puede escoger distribuir solo rutas internas o externas en IS-IS provenientes de OSPF y viceversa.
Estática/Conectada	Incluir redes locales que no están ejecutando ningún protocolo se debe redistribuir interfaces conectadas. Y también rutas estáticas en un protocolo dinámico.

Tabla 6.1. Protocolos de enrutamiento y características de distribución.

Se puede usar redistribuir solo entre protocolos que usen la misma pila de protocolos, ejemplo; protocolos IP no pueden anunciar rutas IPX.

A continuación se mencionan algunas herramientas para controlar y prevenir actualizaciones de enrutamiento:

- Interfaces Pasivas (*passive-interfaces*).
- Rutas predeterminadas o rutas estáticas.
- Listas de distribución (*Distribute lists*).
- Mapas de Ruta (*route-maps*).
- Cambiar la distancia administrativa.

6.3 Interfaces Pasivas (*passive-interface*)

Evita que todas las actualizaciones de enrutamiento de un determinado protocolo sean enviadas a una red, pero no impide que la interfaz específica reciba actualizaciones.

6.4 Rutas predeterminadas o rutas estáticas

Las rutas estáticas son rutas susceptibles de ser configuradas manualmente en el *router*, las rutas estáticas se utilizan con frecuencia para lo siguiente:

- Definir rutas específicas a usar cuando dos AS deban intercambiar información de enrutamiento, en lugar de que se intercambien tablas de enrutamiento enteras.
- Definir rutas a destinos en un enlace WAN para que desaparezca la necesidad de recurrir a un protocolo de enrutamiento dinámico (es decir, cuando no se quiera que las actualizaciones se habiliten o atraviesen el enlace).

6.5 Listas de distribución (*Distribute lists*)

Mediante el uso de listas de acceso ACLs, se filtra el tráfico de actualización sobre redes específicas, esto dentro del protocolo de enrutamiento y puede ser tanto de entrada como de salida.

6.6 Mapas de Ruta (*route-maps*)

Son listas de acceso complejas que permiten que se aprueben algunas condiciones, es posible llevar a cabo algunas acciones con el fin de modificar los atributos del paquete o de la ruta.

Los *route-maps* se pueden acompañar de los siguientes mecanismos:

Access-lists
Prefix-lists
As-path-lists
comunity

6.7 Cambiar la distancia administrativa

En algunos casos, se observa que un *router* selecciona una ruta subóptima, ya que cree que un protocolo de enrutamiento tiene una ruta peor, aunque tenga una distancia administrativa mejor. Una forma de asegurarse de que se seleccionan las rutas del protocolo deseado consiste en asignar a las rutas no deseadas de un protocolo de enrutamiento una distancia administrativamente mayor.

CAPITULO 7

CONCLUSIONES

Una vez revisado los diferentes protocolos de enrutamiento existentes y de acuerdo a sus características mencionadas a lo largo del proyecto de Tesis y a las necesidades planteadas como *ISP*. Las conclusiones son las siguientes:

Como se mencionaba al principio del proyecto de Tesis, se tienen las consideraciones de que el ISP pueda tener o intercambiar tráfico de Internet con proveedores Locales (de cable por ejemplo) a nivel cliente o clientes de Internet dedicado y a nivel proveedor con un ISP Nacional de la dimensión de un *Telmex, Axtel-Avantel, Alestra* o proveedores medianos que solo tienen cierto radio de cobertura como puede ser *Bestel, Metronet, Marcatel*, por mencionar algunos y así también pueda tener su propio proveedor Internacional para proveer el Servicio de Internet.

Tipo de Enrutamiento: Dinámico/Estático

Como ISP independientemente del tamaño de su red es indispensable que se utilice enrutamiento dinámico en la red ya que usar rutas estáticas no es nada práctico tomando en cuenta lo cambiante que puede ser la red a cada instante ya no tener esa dependencia de que el administrador de red tenga que estar al pendiente de cada cambio y hacer las modificaciones correspondientes a nivel configuración. Sin embargo en algunos casos si es necesario utilizar ese enrutamiento estático, más adelante se comentaran en que casos puede aplicar.

Protocolo de Enrutamiento IGP: Vector Distancia/Híbrido/Estado enlace.

Las características que se buscan en el IGP son:

-Optimización
-Eficacia.
-Robustez.
-Convergencia.
-Escalabilidad
-Fácil Administración
-Control sobre el Enrutamiento
-Simplicidad
-Seguridad

La evaluación realizada a los Protocolos de manera independiente enrutamiento fue la siguiente:

RIPv1 y RIPv2. Estos protocolos tienden a ser muy fáciles de configurar y tienen la ventaja que son protocolos abiertos y que muchos fabricantes los soportan, sin embargo por sus otras características de ser protocolos de Vector Distancia y teniendo como métrica el número de saltos hasta llegar al destino final con un máximo de 15, tienen la limitante en cuanto a ser escalables y además que discriminan otros criterios importantes como el ancho de banda de los enlaces. Además ser muy lento en cuanto a velocidad de convergencia ya que puede tomar de 3 hasta 5 mins. en converger. Otro punto negativo es que la actualización de rutas es hacia todos sus vecinos por medio de *broadcast*.

IGRP. Este protocolo aunque actualmente es muy utilizado, no es complicado de configurar, pero tiene la desventaja de que no soporta VLSM, su escalabilidad es mediana, y no presenta algún mecanismo de autentificación en las sesiones, su velocidad de convergencia sigue siendo lenta. Un detalle

adicional es que como ser propietario de Cisco, y no un estándar no puede interactuar con equipos *routers* que no sean Cisco y eso de alguna manera es una limitante en cuanto a crecimiento o migración de tecnología.

EIGRP. Como es una extensión de IGRP, mejora muchas de las características de su antecesor, ya soporta VLSM, autenticación, ya no se apoya en temporizadores como IGRP para sus actualizaciones, usa métricas compuestas, ahora solo se mandan actualizaciones cuando se produce un cambio, por lo mismo optimiza los recursos de CPU por ya no usar actualizaciones periódicas, es multiprotocolo ya que maneja varios tipos de protocolos IP, IPX por ejemplo, de manera independiente y por ende esta preparado para nuevas tecnologías en cuanto a protocolos enrutados como IPv6, es el protocolo que converge más rápido debido al manejo de tablas de respaldo, es escalable y permite balanceo de cargas, sin embargo aun tiene el inconveniente de ser propietario de Cisco limitando su implementación exclusivamente a equipos de esa tecnología.

OSPF v2. Usa una base datos centralizada en la que describe la topología entera de la red y la convergencia es tan rápida como actualizada este la base datos y cada *router* mantiene una base de datos idéntica, la información acerca de las adyacencias son enviadas a los *routers* solamente cuando hay un cambio, es ideal para una topología *jerárquica*, posee las ventajas de los protocolo de enrutamiento estado enlace, el calculo y el enrutamiento permanecen distribuidos, es relativamente fácil de configurar, es muy escalable, es un protocolo abierto lo que permite usar cualquier tecnología en cuanto equipos de red, es muy estable y permite la autenticación usando MD5, permite el balanceo de cargas y utilización óptima de las rutas. Es una de las posibles de acuerdo a todos los beneficios que puede ofrecer.

IS-IS. Como protocolo de estado enlace, tiene posee características muy similares a OSPF, es un estándar abierto y puede soportar tanto IP como

CLNP, aunque es muy robusto y escalable, además el protocolo se usa mucho actualmente en *ISPs* y proyectos a gran escala, además de estar preparado para MPLS, y poseer algunas características superiores a EIGRP u OSPF, aun así la configuración no es tan fácil de realizar así también el aislamiento de fallas tiende a ser complicado, para los fines propuestos y con el modelo de *ISP* que se pretende no se considera el indicado.

Por lo tanto el IGP seleccionado es un protocolo de estado enlace y por todas las características mencionadas anteriormente y de acuerdo a las necesidades planteadas es OSPF, y siguiendo con sus bases jerárquicas, se puede usar como base la topología jerárquica de capas de Cisco (Core, Distribución y Acceso).

El EGP la opción disponible es BGPv4 sin embargo el hecho de que sea la única opción no significa que carezca de importancia, ya que se pueden combinar las diversas funcionalidades que ofrece BGP con prácticas y políticas de enrutamiento con el fin de optimizar el desempeño y personalizar la red del *ISP*.

Topología de Red. Debido a los Servicios que puede ofrecer un *ISP* se considera el modelo de Capas de Cisco, ya que esta topología jerárquica permite realizar funciones específicas por Capa y con una mejor administración para el *ISP.*

- Capa de Core
- Capa de Distribución
- Capa de Acceso

Tomando como base un *ISP* Nacional, y utilizando el modelo de Capas de Cisco, y seccionalizando la red por áreas por ciudad tomando en cuenta ciudades principales, es decir por lo regular un *ISP* no tiene un *Router* de

acceso en cada punto de presencia en el que ofrece el servicio, o en cada cubicación cerca del sitio del cliente, posiblemente haya un punto de presencia cerca del cliente pero este solo sirve de interconexión de los equipos de transporte, es decir el medio de transmisión, por lo regular todo se centraliza en equipos llamados *Bunkers* y así que continuando con las bases de OSPF es necesario crear un área de *backbone* o Core, que siempre es el área 0 y crear áreas de acuerdo a una cd. principal (por ejemplo México, Monterrey, Guadalajara) siendo las ciudades más importantes y en donde se concentra estadísticamente el mayor número de usuarios, la idea de esta topología es tener la mejor administración posible, en caso de que se anexe un *router* de otra cd. Importante con un gran número de usuarios se puede crear un área consecutiva y que tenga conectividad directa al área 0 o agregar ese *router* a un área ya existente que se acomode a un *router* geográficamente.

Capa Core

***Router* Core** (ciudad principal): Su función sería procesar el reenvío de paquetes entre las ciudades, alcanzando conectividad entre las ciudades y dejando paso a tráfico para los servicios, la idea es que el *router* solo tenga funciones de reenvió de tráfico obteniendo así un mejor desempeño. El protocolo IGP que su utilizará es OSPF que servirá para comunicar con lo demás *routers* de la red.

***Route Reflector*.** Se pueden asignar igualmente por cd. principal, y se encargarían de reflejar todas las rutas aprendidas a los *routers* clientes, siendo todos redundantes entre ellos y teniendo sesiones de IBGP a todos sus clientes, que en este caso serían los *routers* de acceso y distribución, la idea es tener solo sesiones a los *route reflectors* para evitar que se tengan que establecer sesiones a todos los equipos de la red, con esto optimizando y siendo más rápido para los *routers* y para las actualizaciones de BGP. Para

facilitar la tarea se puede hacer uso de la herramienta de *peer-groups*, con la finalidad de reunir clientes con las mismas características y al momento de que se envíen actualizaciones de BGP no se haga de manera independiente por *router* consumiendo recursos, si no solo al *peer-group* correspondiente.

Domestic Internet Gateway. Este es el concepto utilizado para destinar un *router* específicamente para que contenga enlaces de *peer agreement* que son enlaces de intercambio de tráfico con los Proveedores de Internet Nacionales, esto con el fin de optimizar el uso de los enlaces Internacionales a Internet (que tienen un costo para el proveedor), un ejemplo; si el cliente del Proveedor Nacional A requiere ir a una red del Proveedor Nacional B, no tenga que hacer uso de los enlaces internacionales hacia Internet, ya que implicaría que los paquetes viajen del proveedor internacional del proveedor A hasta el proveedor Internacional del proveedor B a las redes del proveedor B ocasionando con esto consumo de los enlaces Internacionales y tiempos de respuesta altos en el sentido de que tiene que atravesar todo Internet para llegar a un destino que probablemente este en la misma ciudad, de ahí la finalidad de usar los enlaces de mutuo acuerdo, y por lo regular cada proveedor paga un 50% de la interconexión de esos enlaces, llevando un beneficio para ambos en el ancho de banda ahorrado y un mejor desempeño en cuanto a tiempos de respuesta, las sesiones establecidas son EBGP ya que se tratan de AS diferentes, y por lo tanto también se manejan entre el *peer-agreement* ciertas políticas de enrutamiento enfocadas a BGP, por ejemplo:

- No anunciar redes del Proveedor Internacional de Internet al *peer-agreement*.
- No anunciar redes de otro *peer-agreement*.
- Solo anunciar redes del *ISP* y de sus clientes.
- Filtrar las redes de clientes en común tanto de entrada como de salida.

Internet Gateway. Es el *Router* que tiene la interconexión con el Proveedor Internacional, es decir el *router* donde se concentran los enlaces Internacionales a Internet. Se establecen sesiones de EBGP y así mismo existen ciertas políticas de enrutamiento a aplicar como son:

- Anunciar solo las redes del *ISP* y de sus clientes
- No anunciar redes de los *peer-agreement* Nacionales

*Por seguridad también el Proveedor Internacional debe filtrar los anunciamientos de entrada del *ISP*, solo permitiendo las redes del *ISP* y de sus clientes.

Adicional a esto, se aplican políticas para las redes del *ISP* como de sus clientes con el fin de balancear tráfico en los enlaces internacionales y a su vez se tenga redundancia entre los mismos enlaces como en otros IGs.

Para la manipulación de redes y de preferencias de rutas se pueden etiquetar ya sea con el proveedor internacional o en con el proveedor Nacional por medio del uso de comunidades.

Capa Dsitribución

***Router* de Distribución.** Tiene la finalidad de interconectar las capas de acceso y Core, y es donde concentran los *routers* de acceso, a nivel OSPF se consideran ABRs ya que conectan tanto al área 0 de Core como a las respectivas áreas por ciudad que existan.

Capa Acceso

***Routers* de Acceso.** Son los *routers* que se interconectan a los *routers* de los clientes, de los cuales también se manejan ciertas políticas de enrutamiento, el *router* puede usar el concepto de *route-maps* para hacer la respectiva redistribución de las rutas por ejemplo: redes de clientes o de servicios conocidas como estáticas o directamente conectadas que concuerden con un *prefix-list* redistribuirlas en BGP, así también redes estáticas de *backbone* redistribuirlas en OSPF.

Enrutamiento estático hacia clientes.

El cliente puede tener acceso a Internet vía enrutamiento estático hacia el *ISP* y viceversa, por seguridad el *ISP* puede aplicar una ACL de entrada con el fin de que solo salgan a Internet las redes que pertenecen o fueron asignadas al cliente. En caso de que el cliente posea sus propias direcciones IPs es necesario que el *ISP* las anuncie hacia Internet como propias.

Enrutamiento BGP hacia clientes

Clientes que cuentan con su propio AS y por ende sus propias redes, establecen una sesión de EBGP con el *ISP*, aplicando el *ISP* sus políticas para que solo permita el anunciamiento de las redes del cliente así como los *prepends* correspondientes.

También se pueden manejar conceptos hacia el cliente de:

- *Full Routing* (anunciar todos los prefijos)
- *Partial Routing* sin redes de clientes (anunciar solo los prefijos del ISP)
- *Partial Routing* con redes de clientes (anunciar redes de clientes y del ISP pero no de los proveedores Internacionales)

- Rutas por *default* o predeterminadas

Para hacer más eficientes las políticas de BGP es necesario utilizar una combinación de los siguientes mecanismos para filtrar la información de las rutas que se quieren anunciar o recibir anunciamientos, esto para poder manipular las rutas según sea conveniente.

- ACL.
- Prefix Lists.
- Route-Maps.
- As-Path Filters.

BIBLIOGRAFIA

[Ariagnello, 2004] Ariagnello Ernesto, Redes Cisco: Guía de estudio para la Certificacion CCNA 640 801, Primera Edición, Ra-Ma, Madrid.

[Deal, 2006] Deal, Richard, Introduction to Cisco Router Configuration: Student Guide Cisco Internetwork Operating System, Versión 11.2, Cisco Press, 2006

[Gough, 2004] Gough Clare, CCNP BSCI Exam Certification Guide, Tercera Edición, Cisco Press, Estados Unidos, 2004

[Halabi, Mc Pherson 2000] Halabi Sam, Danny Mc Pherson, The definitive BGP resource: Internet Routing Architectures, Segunda Edición, Cisco Press, Estados Unidos, 2000

[Paquet, Teare 2001] Paquet Catherine, Diane Teare , Building Scalable Cisco Networks, Cisco Press Estados Unidos, 2001

[Raveendran, Smith 2002] Barry Raveendran, Philip Smith, Cisco ISP Essentials, Cisco Press, Estados Unidos 2002.

[Sportack, 2003] Mark A. Sportack, Fundamentos de enrutamiento IP, Cisco Pearson Educación, Estados Unidos, 2003

[Wendell, 2004] Odom Wendell, CCNA INTRO Exam Certification Guide, Cisco Press, Estados Unidos, 2004.

[Wendell, 2004] Odom Wendell, CCNA ICND Exam Certification Guide, Cisco Press, Estados Unidos, 2004.

Internetworking Technologies Handbook, Tercera edición, Cisco Press, Estados Unidos 2001

Configuring BGP, Student Guide version 3.0, Cisco. Estados Unidos, 2005

www.cisco.com

LISTADO DE FIGURAS

Figura 2.1. Configuración de acceso dedicado a Internet.

Figura 2.2. Limites de rendimiento del enlace más débil de un ISP.

Figura 2.3. Punto de demarcación.

Figura 3.1. Internet usaba una jerarquía de dos niveles.

Figura 4.1. *Routers* interiores de una red.

Figura 4.2. *Routers* exteriores desde la perspectiva de las redes privadas.

Figura 4.3. Los *routers* fronterizos desde la perspectiva de las redes privadas.

Figura 4.4. Enrutamiento entre redes adyacentes.

Figura 4.5. Enrutamiento entre redes no adyacentes.

Figura 4.6. Los protocolos de enrutamiento por vector distancia envían toda su tabla de enrutamiento.

Figura 4.7. El tráfico del enrutamiento por vector de distancia se lleva a cabo en paquetes IP.

Figura 5.1. Protocolos de enrutamiento IGPs, EGPs.

Figura 5.2. Cada nodo RIP publica el contenido de sus tablas de enrutamiento a sus vecinos inmediatos

Figura 5.3. Dominio de Proceso en IGRP.

Figura 5.4. OSPF, protocolo de estado enlace.

Figura 5.5 Estructura de Red OSPF

Figura 5.6. Enrutamiento entre áreas IS-IS

Figura 5.7. Intercambio de Información de enrutamiento entre ASs.

LISTADO DE TABLAS

Tabla 3.1. Contenido de la tabla de enrutamiento al usar enrutamiento basado en host.

Tabla 3.2. Contenido de la tabla de enrutamiento al usar enrutamiento basado en la red.

Tabla 4.1. Distancias administrativas predeterminadas de orígenes de rutas.

Tabla 4.2. Comparación de los protocolos de enrutamiento por vector distancia IP de Cisco.

Tabla 4.3. Comparación de los protocolos de enrutamiento por estado de enlace IP de Cisco.

Tabla 5.1. Comparación de características RIPv1 y RIPv2.

Tabla 5.2. Protocolos de enrutamiento y características de distribución.

Tabla 6.1. Atributos BGP.

GLOSARIO

Algoritmo. Procedimiento matemático o lógico para realizar un cálculo o para resolver un problema.

Ancho de banda (*Bandwidth*). Define la cantidad de información que puede ser transmitida en un periodo de tiempo determinado a través de una Red.

ANSI (*American National Standards Institute*). El Instituto Nacional Norteamericano de Normalización es la organización responsable de aprobar las normas de los EEUU en muchas áreas, computadoras y comunicaciones, y es miembro de ISO.

Arbol. Estructura de representación de la información que consiste en un único registro "padre" del que dependen cero o más registros "hijos" que, a su vez, pueden dar origen a nuevos subárboles.

ATM. *Asynchronous Transfer Mode.* Modo de Transferencia Asíncrona. Técnica de conmutación por paquetes de alta velocidad adecuada para

ARPANET (*Advanced Research Projects Agency Network*). Red pionera de larga distancia financiada por ARPA (hoy DARPA) con finalidades militares, que fue el eje central del desarrollo de Internet.

Backup. Copia de Seguridad.

Backbone. Red principal de una red de comunicaciones.

Base de datos (*Database*). Conjunto de datos no redundantes, almacenados en un soporte informático, organizados de forma independiente de su utilización y accesibles simultáneamente por distintos usuarios y aplicaciones. La diferencia de una BD respecto a otro sistema de almacenamiento de datos es que estos se almacenan en la BD de forma que cumplen tres requisitos básicos: no redundancia, independencia y concurrencia.

Bit. *Binary Digit.* Dígito binario. Unidad mínima de información con la que trabajan los ordenadores. Es un dígito del sistema binario que puede tener el valor 0 o 1.

Buffer. Segmento reservado de memoria que se usa para almacenar datos mientras se procesan. Conjunto de registros conectados en paralelo que actúan como memoria intermedia para almacenar datos temporalmente para compensar y adaptar diferencias de velocidad entre emisor y receptor.

Byte. Agrupación fundamental de información binaria formada por 8 bits.

Código binario. Código en el que los elementos se representan solamente por los valores "1" y "0". Es el código empleado principalmente dentro de los circuitos de los equipos físicos.

Contraseña. Véase Password.

CPU. *Central Procesor Unit*. Unidad Central de Proceso. Parte principal de una computadora que incluye la unidad aritmético-lógica (ALU) y la unidad de control (UC).

DECnet. Red de comunicaciones de Digital, que soporta RAL de estilo Ethernet y WAN de banda base y de banda ancha en líneas públicas y privadas.

Encriptado: Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.

Frame. Secuencia, trama

Frame Relay. Sistema de transporte para la transmisión de datos (paquetes) a alta velocidad (hasta 45 Mbits/s) mediante celdas de longitud variable.

Gateway. **Puerta de acceso, pasarela.** Unidad de interfuncionamiento Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red LAN.

Host. En una red informática, es una computadora central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red, también se le llama nodo.

IP. ***Internet Protocol.*** Protocolo internet. Protocolo sin conexión (connectionless) encargado de controlar la información por la red. Permite la integración de otras subredes. Véase TCP/IP.

ISDN. **Integrated Services Digital Network**. Véase RDSI.

Jerarquía. Red ordenada de conceptos u objetos en la cual unos están subordinados a otros.

Kbps. Kilobits por segundo. Medida de velocidad de transmisión.

KiloByte. ***KB*.** Unidad de medida de memoria. Equivalencia: 1 KByte = 1.024 Bytes.

LAN. **Local Area Network**. Red de área local.

MAN. **Metropolitan Area Network**. Red de Area Metropolitana. Red de comunicaciones que cubre un área geográfica como una ciudad o un suburbio.

Mbps. **Megabits por segundo.** Medida de velocidad de transmisión.

MegaByte. **MB.** Unidad de medida de memoria que equivale a 1,024 KB.

Memoria caché. Memoria intermedia de acceso aleatoria muy rápida entre la unidad central de proceso y la memoria principal que almacena los datos o instrucciones extraídos más frecuente y recientemente de la memoria principal.

Módem. Modulador/demodulador. Equipo para la transmisión de datos que convierte señales analógicas en digitales y viceversa. Elemento físico que permite transmitir información entre dos ordenadores mediante una línea telefónica.

Paquete. Secuencia de dígitos binarios, incluyendo datos y señales de control, que se transmite y conmuta como un todo.

Password. **Contraseña.** Palabra clave que identifica al usuario para proteger y definir el acceso a un equipo y por la que se identifica al usuario.

PC. **Personal Computer**. Computadora Personal que utiliza como CPU un microprocesador. Tradicionalmente asociado a los computadoras de uso personal o doméstico.

Protocolo de comunicaciones. Reglas preestablecidas para efectuar la conexión electrónica entre dos sistemas de comunicación.

Protocolo Internet. Véase IP.

RAM. **Random Access Memory.** Memoria de Acceso Aleatorio; memoria de acceso directo; memoria viva. Memoria volátil de escritura y lectura, habitualmente utilizada como almacén temporal de datos.

RDSI (ISDN). Red Digital de Servicios Integrados (**Integrated Services Digital Network**). Red que evoluciona a partir de la red telefónica; permite la conectividad digital de usuario a usuario, proporcionando servicios telefónicos y no-telefónicos.

ROM. **Read Only Memory.** Memoria permanente sólo de lectura. Memoria sólo accesible para la lectura de su contenido, no para su modificación.

Router. Enrutador de paquetes hacia su destino por la ruta óptima. Dispositivo que se encarga de dirigir el tráfico en una red.

Sesión. En la arquitectura de red, conjunto de actividades que tienen lugar durante el establecimiento, mantenimiento y liberalización de una conexión, con vistas a permitir una comunicación de datos entre unidades funcionales.

TCP/IP. **Transmission Control Protocol/Internet Protocol**. Protocolo de Control de Transmisión/Protocolo Interredes. Protocolo para el control de la transmisión orientado a la conexión (**connection-oriented**) TCP, establecido sobre el protocolo internet (IP).

Token Bus. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en anillo. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.4 del IEEE y en la norma 8802.4 de la ISO.

Token Ring. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en bus. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se establece en la norma IEEE 802.5 del IEEE y en la norma 8802.5 del ISO.

Topología. La lógica colocación física y geométrica de una red.

WAN. **Wide Area Network**. Red de área extensa.

X.25. Interfaz para la transmisión de datos en redes de conmutación de paquetes (PSDN, Packed Switched Data Network). Permite circuitos virtuales as í como recuperación de datos y recuperación de errores.

RESUMEN AUTOBIOGRAFICO

Aldemar Gerardo Suárez Morales
Nacido 17 de Agosto de 1976
Padres: Alfonso Suárez Ruiz y Gloria Morales Ruiz

Estudios:
Universidad Autónoma Veracruzana.
Facultad de Ingeniería Electrónica y Comunicaciones con Especialidad en Telecomunicaciones.
Tesis: *Creación de una estación de Radio MP3 con Shoutcast en Internet*

Universidad Autónoma de Nuevo León.
Facultad de Ingeniería Mecánica Eléctrica. División de Estudios de Posgrado.
Maestría en Ciencias de la Ingeniería con especialidad en Telecomunicaciones.
Tesis: *Análisis de Protocolos y Políticas de Enrutamiento para el Proveedor de Servicios de Internet*

Certificaciones CISCO:
CCNA (*Cisco Certified Network Associate*)
BSCI (*Building Scalable Cisco Internetworks*)
QoS (*Implementing Cisco Quality of Service*)

Experiencia Profesional:
Servicios Profesionales en Radiocomunicación
Ingeniero de Servicio (2000)

Servicios alestra-at&t
Soporte Técnico Internet Dial Up Residencial y Negocios (2001)
Ing. de Operación y Mantenimiento de Internet (2001-2003)
Ing. Senior de Operación y Mantenimiento de Internet (2004-2006)
Ing. Senior de Operación y Mantenimiento de Core Datos (2007)