

ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE
INGENIERÍA

GUÍA DE PRÁCTICAS DE LABORATORIO DE REDES DE ÁREA
EXTENDIDA, PARA EL DEPARTAMENTO DE ELÉCTRICA Y
ELECTRÓNICA DE LA ESPE

AUTOR: FERNANDO DAVID SUÁREZ SÁNCHEZ

SANGOLQUÍ-ECUADOR

2008

CERTIFICACIÓN

Certificamos que el presente trabajo de graduación titulado GUÍA DE PRÁCTICAS DE LABORATORIO DE REDES DE ÁREA EXTENDIDA, PARA EL DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA DE LA ESPE, fue realizado por el señor Fernando David Suárez Sánchez.

Ing. Carlos Romero
DIRECTOR

Ing. Ramiro Ríos
CODIRECTOR

RESUMEN

El presente documento muestra una visión detallada del proceso de configuración de equipos para redes de área extendida, los cuales permiten la transmisión de datos a nivel mundial, la internet desde su implementación ha tenido un avance insospechado; en todas las actividades que efectúa el ser humano en su accionar científico, cultural, social, empresarial, tecnológico, utilizando las redes en el marco de las telecomunicaciones propias de un mundo más interrelacionado.

Durante la investigación se ha agregado material que permita al lector tener una percepción mayor sobre la configuración de equipos con la cual estará en capacidad de emprender nuevos estudios e incluso continuar utilizando tecnologías nuevas que cada día siguen apareciendo en el mundo de las redes de computadoras.

El capítulo I, da una breve introducción y explicación de tecnologías que han dado paso a las comunicaciones como el sistema telefónico, ISDN, ATM, X25 entre otros, además se explican los procesos de conmutación y comunicación usados para enviar información a través de la red, con ayuda de los modelos de Referencia OSI y TCP/IP.

El capítulo II, trata de forma muy detallada la instalación del simulador de Red, también presenta formas para mejorar el desempeño del mismo, y para terminar, una guía de cómo se debe programar e implementar algunas tecnologías de red.

El capítulo III, encierra todo lo referente a protocolos de enrutamiento interiores como RIP, EIGRP, OSPF, y protocolos de enrutamiento exteriores como BGP, dando una buena explicación de su funcionamiento, en este capítulo existen cinco prácticas con un detallado proceso de verificación para cada red.

El capítulo IV, siguiendo el mismo esquema habla sobre la transmisión serial, el uso de encapsulamiento *HDLC* -Control de enlace de datos de alto nivel- y el protocolo *PPP* -Protocolo punto a punto-, con su respectiva práctica, y verificación.

El capítulo V, se ha enfocado en la tecnología Frame Relay debido a que ésta, al igual que ATM y X25 usa circuitos virtuales, las prácticas encierran una implementación de protocolo de enrutamiento bajo Frame Relay con su respectiva guía y verificación.

El documento también presenta en su sección de anexos ayuda muy importante de cómo se configuró el simulador. Debido al carácter investigativo, las referencias bibliográficas se encuentran disponibles. El manejo de términos y siglas que trata el documento se explica en pie de página y también en el glosario. Este libro enfoca su material a estudiantes y profesionales los cuales deseen aprender y emprender investigación en redes de área extendida.

DEDICATORIA

A la memoria de mis padres y mi hermana...

AGRADECIMIENTO

Hay tantas personas a las que quisiera agradecer por su apoyo y ayuda para la elaboración de este documento, por la culminación de mis estudios universitarios y por su guía en el camino de la vida.

Gracias, Ñaño Living, Michita, Washin, abuelita Lucy, tíos, primos, Familia.

Gracias a todos
por adornar con música y color cada paso de mi vida

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN.....	II
RESUMEN.....	III
DEDICATORIA.....	V
AGRADECIMIENTO.....	VI
ÍNDICE DE CONTENIDOS.....	VII
ÍNDICE DE TABLAS.....	XII
ÍNDICE DE FIGURAS.....	XIV
ÍNDICE DE HOJAS TÉCNICAS.....	XX
GLOSARIO.....	XXI
CAPÍTULO 1.....	1
INTRODUCCIÓN.....	1
1.1 CONCEPTO DE RED.....	1
1.2 CLASIFICACIÓN.....	2
1.2.1 Según su Tamaño.....	2
1.2.2 Según su Distribución Lógica.....	3
1.3 CONMUTACIÓN DE CIRCUITOS, MENSAJES Y PAQUETES.....	4
1.3.1 Conmutación de Circuitos.....	4
1.3.2 Conmutación de Mensajes.....	4
1.3.3 Conmutación de Paquetes.....	5
1.4 MODELOS DE REFERENCIA.....	5
1.4.1 MODELO DE REFERENCIA OSI.....	5
La Capa Física.....	7
La Capa de Enlace de Datos.....	8
La Capa de Red.....	8
La Capa de Transporte.....	8

La Capa de Sesión.....	8
La Capa de Presentación	9
La Capa de Aplicación.....	9
1.4.2 MODELO DE REFERENCIA TCP/IP	10
Capa de Acceso de Red e Internet.	11
Capa de Transporte.	11
Capa de Aplicación.	11
1.5 TIPOS DE ENLACES WAN	12
1.6 TECNOLOGÍAS WAN	12
1.6.1 CONEXIÓN TELEFÓNICA ANALÓGICA.....	12
1.6.2 ISDN.....	13
1.6.3 LÍNEA ALQUILADA	15
1.6.4 X.25.....	17
1.6.5 FRAME RELAY	19
1.6.6 ATM	26
1.6.7 DSL <i>Digital Subscriber Line</i>	27
1.6.8 CABLE MÓDEM.....	29
1.7 ALGORITMOS DE ENRUTAMIENTO	31
1.7.1 TIPOS DE ALGORITMOS DE ENRUTAMIENTO.....	31
1.8 TABLAS DE ENRUTAMIENTO	35
1.9 PROTOCOLO DE INTERNET IP.....	36
1.10 PROTOCOLOS DE PUERTA INTERIOR Y EXTERIOR IGP/EGP	37
1.11 CONEXIONES WAN.....	38
1.12 ENCAPSULAMIENTO WAN	40
1.12.1 HDLC –High Level Data Link Control-	40
1.12.2 PPP –PEER TO PEER PROTOCOL-	42
CAPÍTULO 2	47
SIMULADOR DYNAMIPS/DYNAGEN.....	47
2.1 INTRODUCCIÓN.....	47
2.2 INSTALACIÓN	48
2.3 IMÁGENES DEL SISTEMA OPERATIVO IOS –Image Operative System-.....	49
2.4 CONFIGURACIÓN DE CLIENTE TELNET	49

2.5 ARCHIVOS DE RED	50
2.6 EJECUCIÓN DE DYNAMIPS/DYNAGEN	53
2.7 CÁLCULO DE VALORES Idle-PC	55
2.8 FRAME RELAY	58
2.9 CAPTURA DE PAQUETES.....	59
CAPÍTULO 3	62
PRÁCTICAS DE PROTOCOLOS DE ENRUTAMIENTO	62
3.5 PRÁCTICA 1:	63
Tema: CONFIGURACIÓN DE RUTAS ESTÁTICAS.....	63
3.5.1 OBJETIVOS:.....	63
3.5.2 MARCO TEÓRICO.....	63
3.5.3 ESQUEMA DE LA RED	65
3.5.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	66
3.5.5 VERIFICACIÓN DE CONFIGURACIÓN.....	69
3.6 PRÁCTICA 2	75
Tema: CONFIGURACIÓN DE RIP -ROUTING INFORMATION PROTOCOL-.....	75
3.6.1 OBJETIVOS:.....	75
3.6.1 MARCO TEÓRICO.....	75
3.6.3 ESQUEMA DE LA RED	77
3.6.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	78
3.6.5 VERIFICACIÓN DE CONFIGURACIÓN –RIP-	79
3.7 PRÁCTICA 3	87
Tema: CONFIGURACIÓN DE OSPF -OPEN SHORT PATH FIRST-	87
3.7.1 OBJETIVOS	87
3.7.2 MARCO TEÓRICO.....	87
3.7.3 ESQUEMA DE LA RED	94
3.7.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	94
3.7.5 VERIFICACIÓN DE OSPF MULTIAREA	96
3.8 PRÁCTICA 4	102
Tema: CONFIGURACIÓN DE EIGRP –ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL-.....	102
3.8.1 OBJETIVOS.....	102

3.8.2 MARCO TEÓRICO.....	102
3.8.3 ESQUEMA DE LA RED	111
3.8.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	112
3.8.5 VERIFICACIÓN DE EIGRP	113
3.9 PRÁCTICA 5	123
Tema: CONFIGURACIÓN DE BGP -BORDER GATEWAY PROTOCOL-.....	123
3.9.1 OBJETIVOS	123
3.9.2 MARCO TEÓRICO.....	123
3.9.3 ESQUEMA DE LA RED	129
3.9.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	130
3.9.5 VERIFICACIÓN DE BGP.....	132
CAPÍTULO 4	138
PRÁCTICAS DE ENCAPSULAMIENTO WAN	138
4.1 PRÁCTICA 6	138
Tema: CONFIGURACIÓN DE PPP	138
4.1.1 OBJETIVOS	138
4.1.2 MARCO TEÓRICO.....	139
4.1.3 ESQUEMA DE LA RED	142
4.1.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	143
4.1.5 VERIFICACIÓN DE PPP.	145
CAPÍTULO 5	150
PRÁCTICAS FRAME RELAY	150
5.1 PRÁCTICA 7	150
Tema: CONFIGURACIÓN DE FRAME-RELAY CON OSPF.....	150
5.1.1 OBJETIVOS	150
5.1.2 MARCO TEÓRICO.....	151
5.1.3 ESQUEMA DE LA RED	155
5.1.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	156
5.1.5 VERIFICACIÓN DE FRAME RELAY.....	160
5.2 PRÁCTICA 8	165
Tema: CONFIGURACIÓN DE FRAME-RELAY CON EIGRP	165
5.2.1 OBJETIVOS	165

5.2.2 MARCO TEÓRICO.....	165
5.2.3 ESQUEMA DE LA RED	167
5.2.4 LABORATORIO –PASOS DE CONFIGURACIÓN-	168
5.2.5 VERIFICACIÓN DE FRAME RELAY.....	169
CONCLUSIONES Y RECOMENDACIONES	172
CONCLUSIONES.....	172
RECOMENDACIONES	173
ANEXOS.....	1
Archivos de RED DYNAGEN.....	2
Laboratorio Rutas Estáticas	2
Laboratorio de protocolo de enrutamiento RIP	3
Laboratorio de protocolo de enrutamiento OSPF.....	4
Laboratorio de protocolo de enrutamiento EIGRP	5
Laboratorio de protocolo de enrutamiento BGP.....	6
Laboratorio de encapsulamiento PPP	7
Laboratorio de encapsulamiento Frame Relay	8
Tabla de Costos en enlaces usados por OSPF:.....	9
REFERENCIAS BIBLIOGRÁFICAS	10
FECHA DE ENTREGA	11

ÍNDICE DE TABLAS

CAPÍTULO I

Tabla 1.1 Cables Seriales WAN.....	33
------------------------------------	----

CAPÍTULO III

Tabla 3.1 Datos de la Red WAN Rutas Estáticas.....	56
Tabla 3.2 Lista de Comandos	65
Tabla 3.3 Valores de Distancias Administrativas	68
Tabla 3.4 Datos de la Red WAN RIP.....	69
Tabla 3.5 Datos de la Red WAN -OSPF multiareas-	83
Tabla 3.6 Datos de la Red WAN EIGRP.....	100
Tabla 3.7 Mensaje OPEN BGP.....	113
Tabla 3.8 Mensaje Update.....	114
Tabla 3.9 Mensaje de Notificación.....	115
Tabla 3.10 Subcódigos de Error.....	115
Tabla 3.11 Subcódigos de Error.....	115
Tabla 3.12 Subcódigos de Error.....	116
Tabla 3.13 Datos de la Red WAN.....	117

CAPÍTULO IV

Tabla 4.1 Tipos de Protocolos para enlace	127
Tabla 4.2 Datos de la Red WAN.....	136

CAPÍTULO V

Tabla 5.1 Características de OSPF en distintos tipos de Red.....152
Tabla 5.2 Datos de la Red Frame Relay.....153
Tabla 5.3 Datos de la Red Frame Relay.....164

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1.1 Red de Área Extensa - <i>Wide-Area Network</i> -.....	3
Figura 1.2 Comunicación par a par del modelo OSI.....	7
Figura 1.3 Modelos OSI y TCP/IP.....	10
Figura 1.4 Enlaces WAN	12
Figura 1.5 Interfaz de acceso Básico y Principal	14
Figura 1.6 Tributarios para transmisión	16
Figura 1.7 Interfaz de acceso Básico y Principal	17
Figura 1.8 Ejemplo de Red tipo X.25	17
Figura 1.9 Ejemplo de una Red tipo Frame-Relay	19
Figura 1.10 Esquema de una Red Frame Relay	21
Figura 1.11 Esquema de una Red Frame Relay	21
Figura 1.12 Tasa de Información Comprometida.....	24
Figura 1.13 Entramado Frame Relay	25
Figura 1.14 Ejemplo de una Red ATM	26
Figura 1.15 Tipos de Servicio DSL	27
Figura 1.16 Ejemplo de una Red DSL	28
Figura 1.17 Esquema de Red de una instalación por Cable Modem	30
Figura 1.18 (a) y (b) Grafo de Algoritmo de Dijkstra.....	34
Figura 1.18 (c) y (d) Grafo de Algoritmo de Dijkstra.....	34
Figura 1.18 (e) y (f) Grafo de Algoritmo de Dijkstra.....	35
Figura 1.19 Protocolos de Enrutamiento en distintos sistemas autónomos.....	38
Figura 1.20 Conectores de Red WAN	39
Figura 1.21 Trama HDLC	40
Figura 1.22 PPP proceso de capas OSI	43

Figura 1.22 PPP proceso de capas OSI	43
Figura 1.23 Trama de PPP	44

CAPÍTULO II

Figura 2.1 Íconos Dynagen del Escritorio.....	48
Figura 2.2 Archivo de Configuración Simple1.net	50
Figura 2.3 Inicialización de Dynamips Server.....	53
Figura 2.4 Dynagen Dispositivos de Red.....	54
Figura 2.5 Comandos de Dynagen.....	54
Figura 2.6 Apagado y Encendido de Routers en Dynagen	55
Figura 2.7 Comando Idlepc, Estadísticas del PC	56
Figura 2.8 Procedimiento para elección del valor de Idlepc	57
Figura 2.9 Caída del Uso del CPU	57
Figura 2.10 Consola de Administrador Dynagen Frame Relay Switch.....	59
Figura 2.11 Ícono de Recarga del archivo de captura	60
Figura 2.12 Analizador de Paquetes Wireshark	60

CAPÍTULO III

Figura Red de Area Extendida WAN	63
Figura 3.1 Ejemplo para uso de Enrutamiento Estático	64
Figura 3.2 Diagrama de Red	65
Figura 3.3 Prueba de Conectividad Ping	70
Figura 3.4 Comprobación de configuración comando Show Run	70
Figura 3.5 Comprobación de configuración comando Show Run	71
Figura 3.6 Comprobación de configuración comando Show Run	71
Figura 3.7 Comprobación de configuración comando Show Run	71
Figura 3.8 Comprobación de configuración comando Show Ip Route	72
Figura 3.9 Verificación de Paquetes	74
Figura 3.10 Ejemplo RIP Diagrama de Red	76
Figura 3.11 Diagrama de Red -RIP-	78
Figura 3.12 Prueba de conectividad capa dos OSI -RIP-	80

Figura 3.13 Prueba de conectividad capa siete OSI comando Telnet	80
Figura 3.14 Prueba de conectividad capa dos OSI	81
Figura 3.15 Prueba de conectividad comando Show interface –RIP-	82
Figura 3.16 Prueba de conectividad comando Show interface -RIP-	82
Figura 3.17 Prueba de conectividad comando Show ip route –RIP-	83
Figura 3.18 Prueba de conectividad comando Show ip route –RIP-	83
Figura 3.19 Esquema para comprobación de ruta	85
Figura 3.20 Prueba de conectividad Wireshark Miami.cap	85
Figura 3.21 Prueba de conectividad Wireshark Miami.cap	86
Figura 3.22 Prueba de conectividad Wireshark Miami.cap	86
Figura 3.22a Captura de paquetes IP, RIPv2.....	86
Figura 3.23 Comparación de protocolos de Vector Distancia	88
Figura 3.24 Diseño Jerárquico de Red OSPF	90
Figura 3.25 Diseño Jerárquico de Red OSPF –Tipos de Routers-	92
Figura 3.26 Diagrama de Red	94
Figura 3.27 Verificación de Conectividad	96
Figura 3.28 Show IP OSPF neighbor router Miami	96
Figura 3.29 Show IP OSPF neighbor router Quito	97
Figura 3.30 Show IP OSPF interface router Quito	97
Figura 3.31 Show IP OSPF interface router Quito	98
Figura 3.32 Show IP OSPF interface router Miami	98
Figura 3.33 Show IP OSPF interface router Miami	98
Figura 3.34 Show IP route desde el router Miami	99
Figura 3.35 Esquema para comprobación de ruta	100
Figura 3.36 Prueba de conectividad Wireshark Miami.cap	100
Figura 3.37 Prueba de conectividad Wireshark Miami.cap	101
Figura 3.38 Prueba de conectividad Wireshark Miami.cap	101
Figura 3.39 Ejemplo del Algoritmo DUAL de EIGRP	105
Figura 3.40 Ejemplo de elección de Ruta DUAL EIGRP	111
Figura 3.41 Diagrama de Red	111
Figura 3.42 Pruebas de conectividad Ping y Telnet EIGRP	114
Figura 3.43 Tablas de enrutamiento router Quito	114

Figura 3.44 Tablas de enrutamiento router Quito para alcanzar la int s1/2 en el router Londres	115
Figura 3.45 Tabla de enrutamiento router Quito para alcanzar la int s1/0 en el router Londres	115
Figura 3.46 Tabla de enrutamiento router Miami.....	116
Figura 3.47 Información de la interface s1/1 Comando show interface.....	116
Figura 3.48 Wireshark desglose de un Paquete Hello.....	117
Figura 3.49 Prueba de conectividad desde router Caracas.....	118
Figura 3.50 Tablas de enrutamiento router Caracas.....	118
Figura 3.51 Tablas de vecinos router Quito.....	118
Figura 3.52 Tablas de topología router Quito.....	119
Figura 3.53 Tablas de topología router Quito.....	120
Figura 3.54 Esquema para comprobación de ruta y resolución de Dual.....	120
Figura 3.55 Verificación Ping desde Router Londres a Router Quito.....	121
Figura 3.56 Esquema para comprobación de ruta y resolución de Dual.....	121
Figura 3.57 Esquema para comprobación de ruta y resolución de Dual.....	122
Figura 3.58 Esquema para comprobación de ruta y resolución de Dual.....	122
Figura 3.59 Esquema de red con dos sistemas autónomos.....	124
Figura 3.60 Diagrama de Red	129
Figura 3.61 Prueba de Conectividad Ping	132
Figura 3.62 Tabla de enrutamiento router Lima	133
Figura 3.63 Entradas en el router Lima	133
Figura 3.64 Redes router Caracas	134
Figura 3.65 Redes actualización Router Caracas	134
Figura 3.66 Presentación de Vecinos Router Quito	135
Figura 3.67 Presentación de Paquetes Lima	136

CAPÍTULO IV

Figura 4.1 Autenticación de dos vías PAP	140
Figura 4.2 Autenticación de tres vías CHAP	141
Figura 4.3 Diagrama de Red	142
Figura 4.4 Prueba de conectividad Ping	145

Figura 4.5 Interface serial 1/0 router Quito	146
Figura 4.6 Interface serial 1/1 router Quito	146
Figura 4.7 Interface serial 1/2 router Quito.....	147
Figura 4.8 Tabla de enrutamiento router Quito.....	147
Figura 4.9 Tabla de topología router Quito.....	148
Figura 4.10 Intercambio de paquetes PPP y EIGRP router Quito.....	149

CAPÍTULO V

Figura 5.1 Problema de actualización en una Red Frame Relay.....	151
Figura 5.2 Diagrama de Red	155
Figura 5.3 Prueba de conectividad en Frame Relay	161
Figura 5.4 Prueba de conectividad en Frame Relay	161
Figura 5.5 Verificación de configuración de Vecinos.....	161
Figura 5.6 Verificación de configuración de Vecinos.....	162
Figura 5.7 Verificación de configuración de Interfaces.....	162
Figura 5.8 Verificación de configuración de Interfaces.....	163
Figura 5.9 Verificación de DLCI y LMI.....	163
Figura 5.10 Verificación de conexión.	164
Figura 5.11 Notificación de cambio en la topología.	164
Figura 5.12 Notificación de cambio en la topología	164
Figura 5.13 Red Frame Relay multipunto.....	166
Figura 5.14 Red Frame Relay multipunto.....	167
Figura 5.15 Diagrama de Red	167
Figura 5.16 Comando show ip protocol	170
Figura 5.17 Comando show ip protocols router Lima	170
Figura 5.18 Comando show ip neighbor router Lima	170
Figura 5.19 Comando show ip protocols router Lima	171

ÍNDICE DE HOJAS TÉCNICAS

ANEXOS

Archivos de Red Dynagen.....	A2
Laboratorio de Rutas Estáticas.....	A3
Laboratorio de protocolo de enrutamiento RIP.....	A3
Laboratorio de protocolo de enrutamiento OSPF.....	A4
Laboratorio de protocolo de enrutamiento EIGRP.....	A5
Laboratorio de protocolo de enrutamiento BGP.....	A6
Laboratorio de encapsulamiento PPP.....	A7
Laboratorio de encapsulamiento FRAME RELAY.....	A8
Tabla de Costos en enlaces usados por OSPF.....	A9

GLOSARIO

ATM.- Asynchronous Transfer Mode. Modo de Transferencia Asíncrona: Tecnología WAN

CPE.- Customer Premises Equipment. Son unidades terminales asociadas a equipamientos de telecomunicaciones, localizadas en el lado del suscriptor y que se encuentran conectadas con el canal de comunicaciones del proveedor

DLCI.- Data Link Connection Identifier. Es un número de canal el cual viene junto a Frame Relay el cual dice a la red como encaminar los datos.

Frame Relay.- Técnica de comunicación mediante retransmisión de datos

HDLC.- High Level Data Link Control: Protocolo de comunicación de datos punto a punto

ISDN.- Integrated Services Digital Network: Sistema de red telefónica por conmutación de circuitos, diseñado para transmitir voz y datos, conjunto de protocolos.

ISO.- International Standard Organization: Organización Internacional de Estándares

OSI.- Open System Interconnection: Interconexión de Sistemas Abiertos.

PPP.- Peer to Peer Protocol: Protocolo Punto a Punto protocolo asociado a la Pila TCP/IP

Router.- Dispositivo de hardware para interconexión de redes de computadores que opera en la capa tres del modelo OSI –*network layer*-.

Switch.- Dispositivo de hardware para interconexión de redes de computadores que opera en la capa dos del modelo OSI –*data link layer*-.

TCP/IP.- Transfer Control Protocol/Internet Protocol: Protocolo de Control de Transferencia, Protocolo de Internet: Conjunto de Protocolos de Internet

VC.- Virtual Circuit: Es una sistema de comunicación por el cual los datos de un usuario origen pueden ser transmitidos a otro usuario destino a través de más de un circuito de comunicaciones real durante un cierto período de tiempo.

WAN.- Wide Area Network: Red de Área Amplia

X.25.- Estándar para redes de Área Amplia de conmutación de Paquetes, basado en el protocolo HDLC

CAPÍTULO 1

INTRODUCCIÓN

El estudio de redes de computadores es bastante amplio, es por esta razón que el presente capítulo pretende recordar cierta terminología usada en redes, además se cita de manera breve los tipos de tecnologías existentes, y los modelos de referencia OSI y TCP/IP base del proceso de comunicación entre dispositivos. Este conocimiento es indispensable para la comprensión de posteriores capítulos y prácticas.

1.1 CONCEPTO DE RED

Una *red* es un sistema de transmisión de datos que permite el intercambio de información entre computadores. Si bien esta definición es demasiado general, nos sirve como punto de partida. La información que pueden intercambiar los computadores de una red puede ser de lo más variada: correos electrónicos, vídeos, imágenes, música en formato MP3, registros de una base de datos, páginas web, etcétera.

La transmisión de estos datos se produce a través de un medio de transmisión o combinación de distintos medios: cables de fibra óptica, tecnología inalámbrica, enlaces vía satélite (el intercambio de información entre computadores mediante disquetes o CDs no se considera una red).

1.2 CLASIFICACIÓN

1.2.1 Según su Tamaño

Las Redes según su tamaño se clasifican de la siguiente manera:

Las redes **PAN** (*Personal Area Network*, redes de área personal) son las redes que un usuario puede operar dentro de un límite menor a 10 metros, pueden ser parte de una red de mayor tamaño, integrándose mediante puntos de acceso.

Las redes **LAN** (*Local Area Network*, redes de área local) son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio... Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto.

Las redes **MAN** (*Metropolitan Area Network*, redes de área metropolitana). Un ejemplo es la red utilizada en una pequeña población para interconectar todos sus comercios, hogares y administraciones públicas.

Las redes **WAN** (*Wide Area Network*, redes de área extensa) son redes punto a punto que interconectan países y continentes. Por ejemplo, un cable submarino entre Europa y América, o bien una red troncal de fibra óptica para interconectar dos países. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

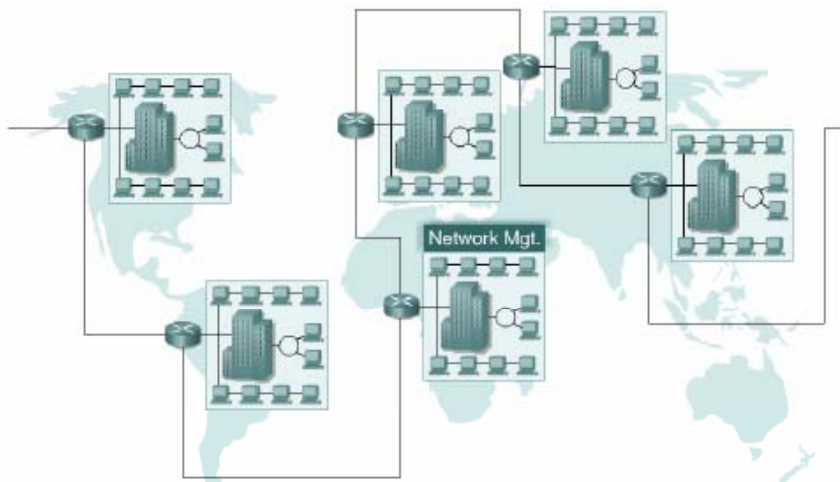


Figura 1.1 Red de Área Extensa *Wide-Area Network*

Las redes LAN son pequeñas y las redes WAN, muy grandes: debe existir algún término para describir unas redes de tamaño intermedio.

Las redes **GAN** (*Global Area Network*, redes de área global).

1.2.2 Según su Distribución Lógica

Todos los computadores tienen un lado cliente y otro servidor: una máquina puede ser servidora de un determinado servicio pero cliente de otro servicio.

Servidor. Máquina que ofrece información o servicios al resto de los puestos de la red. La clase de información o servicios que ofrezca determina el tipo de servidor que es: servidor de impresión, de archivos, de páginas web, de correo, de usuarios, de *IRC* (charlas en Internet), de base de datos...

Cliente. Máquina que accede a la información de los servidores o utiliza sus servicios. Ejemplos: Cada vez que estamos viendo una página web (almacenada en un servidor remoto) nos estamos comportando como clientes. También seremos clientes si utilizamos el servicio de impresión de un PC remoto en la red (el servidor que tiene la impresora conectada).

1.3 CONMUTACIÓN DE CIRCUITOS, MENSAJES Y PAQUETES

La comunicación entre un origen y un destino habitualmente pasa por nodos intermedios que se encargan de encauzar el tráfico. Por ejemplo, en las llamadas telefónicas los nodos intermedios son las centrales telefónicas y en las conexiones a Internet, los *routers* o enrutadores. Dependiendo de la utilización de estos nodos intermedios, se distingue entre conmutación de circuitos, de mensajes y de paquetes.

1.3.1 Conmutación de Circuitos

En la *conmutación de circuitos* se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Si no se transmiten datos o se transmiten pocos se estará subutilizando el canal. Las comunicaciones a través de líneas telefónicas analógicas (RTB) o digitales (RDSI) funcionan mediante conmutación de circuitos.

1.3.2 Conmutación de Mensajes

Un mensaje que se transmite por *conmutación de mensajes* va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos. En la vida real podemos compararlo con el correo postal.

1.3.3 Conmutación de Paquetes

Finalmente, la *conmutación de paquetes* es la que realmente se utiliza cuando hablamos de *redes*. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos (*routers*) no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

1.4 MODELOS DE REFERENCIA

Actualmente el *software* de redes está altamente estructurado, para reducir la complejidad de su diseño la mayoría de redes está organizada como una pila de capas o niveles cada una construida a partir de la que está debajo de ella. El propósito de cada capa es ofrecer ciertos servicios a las capas superiores. La capa n de una máquina mantiene una conversación con la capa n de otra máquina. Las reglas y convenciones utilizadas en esta conversación se conocen como protocolo de capa n (1).

Los modelos de referencia OSI y TCP/IP son los más usados para estudio, en el primero aunque los protocolos asociados no se usan, el modelo en si es muy general y aun es válido. Por otro lado TCP/IP tiene las propiedades opuestas, el modelo en si no se utiliza mucho pero los protocolos sí.

1.4.1 MODELO DE REFERENCIA OSI

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un

conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial (2).

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ilustra una función de red específica. - La división de la red en siete capas permite obtener las siguientes ventajas:

- ✓ Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- ✓ Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos por diferentes fabricantes
- ✓ Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- ✓ Evita que los cambios en una capa afecten las otras capas.
- ✓ Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje (2).

Cada capa del modelo OSI en el origen debe comunicarse con su capa par en el lugar destino. Esta forma de comunicación se conoce como de par-a-par. Durante este proceso, los protocolos de cada capa intercambian información, denominada unidades de datos de protocolo PDU. Cada capa de comunicación en el computador origen se comunica con un PDU específico de capa, y con su capa par en el computador destino (2).

Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella.

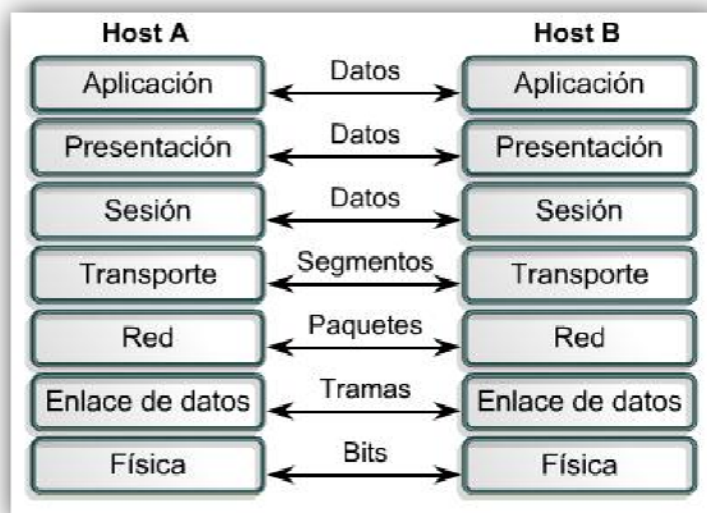


Figura 1.2 Comunicación par a par del modelo OSI

La Capa Física

En la capa física se realiza lo que es la transmisión y recepción de *bits*, multiplexación, características del medio físico, aplicaciones de modulación y demodulación, y todo lo que se refiere a características eléctricas y mecánicas, sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados, coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta) (3).

La Capa de Enlace de Datos

En esta capa se realiza el direccionamiento físico, la topología de la red, control de detección de errores, control de acceso al medio, transmisión y recepción de *frames*, y control de flujo (2).

La Capa de Red

En la capa de red se realiza direccionamiento lógico, enrutamiento, control de congestión, servicios virtuales y servicios de *datagramas* –*paquetes*–.

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea son los Routers (3).

La Capa de Transporte

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario –*segmentación*–, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes.

La Capa de Sesión

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor. Control de diálogo.

- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo). Puntos de sincronismo.
- Mantener puntos de verificación (*checkpoints*), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio. Es decir se realiza control de actividad de la sesión (3).

La Capa de Presentación

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Es decir permite la interoperabilidad de sistemas heterogéneos, y además efectúa compactación de datos y criptografía (3).

La Capa de Aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP¹ y SMTP²), gestores de bases de datos y servidor de ficheros

¹ POP: *Post Office Protocol*: Protocolo de Oficina de Correos. No necesita una conexión permanente a internet, el momento de la conexión solicita al servidor el envío de correspondencia.

² SMTP: *Simple Mail Transfer Protocol*: Protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos.

(FTP³). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente (3).

1.4.2 MODELO DE REFERENCIA TCP/IP

El departamento de defensa de los Estados Unidos creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD⁴ quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia.

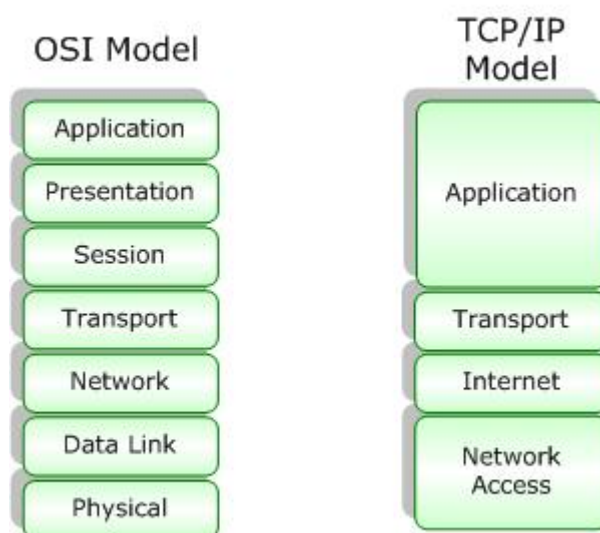


Figura 1.3 Modelos OSI y TCP/IP

³ FTP (*File Transfer Protocol*) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.

⁴ DoD: Department of Defense: Departamento de Defensa

Capa de Acceso de Red e Internet.

Estas dos capas permiten que los hosts inyecten paquetes en cualquier red y que estos viajen a su destino de manera independiente.

La capa de internet define un paquete de formato y protocolo oficial llamado IP. El trabajo de esta capa es entregar paquetes IP al destinatario. Aquí el enrutamiento de paquetes es claramente el aspecto principal, tal como vemos en la **Figura 1.3** esta capa acoge las capas física y de enlace de datos del modelo OSI.

Capa de Transporte.

Posee las mismas funciones de la capa de transporte del modelo OSI. Aquí se definen dos protocolos de transporte de extremo a extremo. El primero TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina. El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP.

Capa de Aplicación.

A continuación de la capa de transporte se encuentra la capa de aplicación. Contiene todos los protocolos del nivel más alto. Los primeros incluyeron una terminal virtual (Telnet⁵), FTP, SMTP.

⁵ Telnet: Protocolo que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos frente a ella. Para que la conexión funcione la máquina a la que se accede debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza es el 23.

1.5 TIPOS DE ENLACES WAN

En la **Figura 1.4** se presentan los tipos de enlace que ofrece una red WAN, con las distintas clases de conmutaciones y líneas. Para evitar las demoras asociadas con la configuración de una conexión, los proveedores de servicio telefónico también ofrecen circuitos permanentes. Estas líneas alquiladas o dedicadas ofrecen mayor ancho de banda que el disponible en los circuitos conmutados.

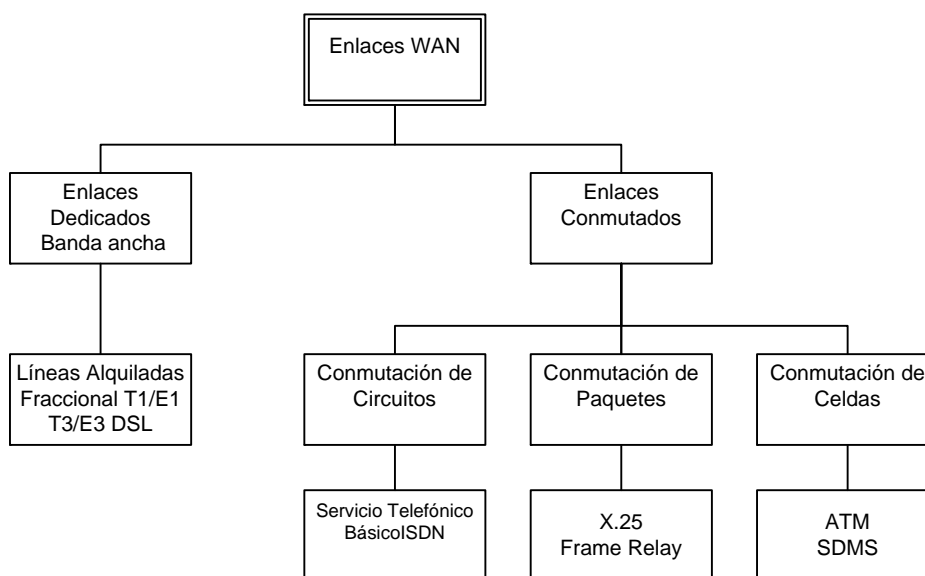


Figura 1.4 Enlaces WAN

1.6 TECNOLOGÍAS WAN

1.6.1 CONEXIÓN TELEFÓNICA ANALÓGICA

Cuando se necesitan transferencias de datos de bajo volumen e intermitentes, los módems y las líneas telefónicas analógicas ofrecen conexiones conmutadas dedicadas y de baja capacidad. La telefonía convencional utiliza cables de cobre, llamados bucle local, para conectar el equipo telefónico a las instalaciones del suscriptor a la red telefónica pública conmutada (PSTN). La señal en el bucle local durante una llamada es una señal electrónica en constante cambio, que es la traducción de la voz del suscriptor.

El bucle local no es adecuado para el transporte directo de datos informáticos binarios, pero el módem puede enviar datos de computador a través de la red telefónica de voz. El módem modula los datos binarios en una señal analógica en el origen y, en el destino, demodula la señal analógica a datos binarios. Las características físicas del bucle local y su conexión a PSTN limitan la velocidad de la señal. El límite superior está cercano 33 kbps. Es posible aumentar la velocidad a 56 kbps si la señal viene directamente por una conexión digital.

Para las empresas pequeñas, esto puede resultar adecuado para el intercambio de cifras de ventas, precios, informes regulares y correo electrónico. Al usar el sistema de conexión automático de noche o durante los fines de semana para realizar grandes transferencias de archivos y copias de respaldo de datos, la empresa puede aprovecharse de las tarifas más bajas de las horas no pico (cargos por línea) Las tarifas se calculan según la distancia entre los extremos, la hora del día y la duración de la llamada.

Las ventajas del módem y las líneas analógicas son simplicidad, disponibilidad y bajo costo de implementación. Las desventajas son la baja velocidad en la transmisión de datos y el relativamente largo tiempo de conexión. Los circuitos dedicados que ofrece el sistema de conexión telefónica tendrán poco retardo y fluctuación de fase para el tráfico punto a punto, pero el tráfico de voz o video no funcionará de forma adecuada a las velocidades de bits relativamente bajas.

1.6.2 ISDN

Las conexiones internas o troncales de PSTN evolucionaron y pasaron de llevar señales de multiplexión por división de frecuencia, a llevar señales digitales de multiplexión por división de tiempo (TDM). El próximo paso evidente es permitir que el bucle local lleve las señales digitales que resultan en conexiones conmutadas de mayor capacidad.

La red digital de servicios integrados (ISDN) convierte el bucle local en una conexión digital TDM. La conexión utiliza canales portadores de 64 kbps (B) para transportar voz y datos, y una señal, canal delta (D), para la configuración de llamadas y otros propósitos.

La interfaz de acceso básico (BRI) ISDN está destinada al uso doméstico y a las pequeñas empresas y provee dos canales B de 64 kbps y un canal D de 16 kbps. Para las instalaciones más grandes, está disponible la interfaz de acceso principal (PRI) ISDN. En América del Norte, PRI ofrece veintitrés canales B de 64 kbps y un canal D de 64 kbps, para un total de velocidad de transmisión de hasta 1,544 Mbps. Esto incluye algo de carga adicional para la sincronización. En Europa, Australia, y otras partes del mundo, PRI ISDN ofrece treinta canales B y un canal D para un total de velocidad de transmisión de hasta 2,048 Mbps, incluyendo la carga de sincronización. En América del Norte, PRI corresponde a una conexión T1. La velocidad de PRI internacional corresponde a una conexión E1.

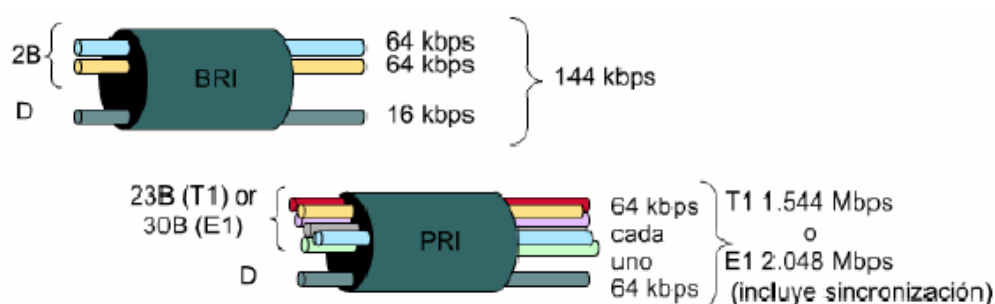


Figura 1.5 Interfaz de acceso Básico y Principal

El canal D BRI no utiliza su potencial máximo, ya que tiene que controlar solamente dos canales B. Algunos proveedores permiten que los canales D transmitan datos a una velocidad de transmisión baja como las conexiones X.25 a 9,6 kbps.

Para las WAN pequeñas, ISDN BRI puede ofrecer un mecanismo de conexión ideal. BRI posee un tiempo de establecimiento de llamada que es menor a un segundo y su canal B de 64 kbps ofrece mayor capacidad que un enlace de módem analógico. Si se requiere una mayor capacidad, se puede activar un segundo canal B para brindar un total

de 128 kbps. Aunque no es adecuado para el video, esto permitiría la transmisión de varias conversaciones de voz simultáneas además del tráfico de datos

Otra aplicación común de ISDN es la de ofrecer capacidad adicional según la necesidad en una conexión de línea alquilada. La línea alquilada tiene el tamaño para transportar el tráfico usual mientras que ISDN se agrega durante los períodos de demanda pico. ISDN también se utiliza como respaldo en caso de que falle la línea alquilada. Las tarifas de ISDN se calculan según cada canal B y son similares a las de las conexiones analógicas.

Con ISDN PRI, se pueden conectar varios canales B entre dos extremos. Esto permite que se realicen conferencias de video y conexiones de datos de banda ancha sin latencia ni fluctuación de fase. Las conexiones múltiples pueden resultar muy caras para cubrir grandes distancias

1.6.3 LÍNEA ALQUILADA

Cuando se requieren conexiones dedicadas permanentes, se utilizan líneas alquiladas con capacidades de hasta 2.5 Gbps. Un enlace punto a punto ofrece rutas de comunicación WAN preestablecidas desde las instalaciones del cliente a través de la red hasta un destino remoto. Las líneas punto a punto se alquilan por lo general a una operadora de servicios de telecomunicaciones y se denominan líneas alquiladas.

Se pueden conseguir líneas alquiladas con distintas capacidades. Estos circuitos dedicados se cotizan, en general, según el ancho de banda necesario y la distancia entre los dos puntos conectados. Los enlaces punto a punto por lo general son más caros que los servicios compartidos como Frame Relay. El costo de las soluciones de línea dedicada puede tornarse considerable cuando se utilizan para conectar varios sitios. Sin embargo, a veces los beneficios de una línea alquilada son mayores que los costos. La capacidad dedicada no presenta ni latencia ni fluctuaciones de fase entre extremos. La disponibilidad constante es esencial para algunas aplicaciones tales como el comercio electrónico. Cada

conexión de línea alquilada requiere un puerto serial de router. También se necesita un CSU/DSU y el circuito físico del proveedor de servicios.

Tipo de línea	Estándar de señal	Capacidad de la velocidad de transmisión
56	DS0	56 kbps
64	DS0	64 kbps
T1	DS1	1.544 Mbps
E1	ZM	2.048 Mbps
E3	M3	34.064 Mbps
J1	Y1	2.048 Mbps
T3	DS3	44.736 Mbps
OC-1	SONET	51.84 Mbps
OC-3	SONET	155.54 Mbps
OC-9	SONET	466.56 Mbps
OC-12	SONET	622.08 Mbps
OC-18	SONFT	933.12 Mbps
OC-24	SONET	1244.16 Mbps
OC-36	SONET	1866.24 Mbps
OC-48	SONET	2488.32 Mbps

Figura 1.6 Tributarios para transmisión.

Las líneas alquiladas se utilizan con mucha frecuencia en la construcción de las WAN y ofrecen una capacidad dedicada permanente. Han sido la conexión tradicional de preferencia aunque presentan varias desventajas. El tráfico de WAN es a menudo variable y las líneas alquiladas tienen una capacidad fija. Esto da por resultado que el ancho de banda de la línea rara vez sea el que se necesita. Además, cada punto necesitaría una interfaz en el router que aumentaría los costos de equipos. Todo cambio a la línea alquilada, en general, requiere que el proveedor haga una visita al establecimiento para cambiar la capacidad

Las líneas alquiladas ofrecen conexiones punto a punto entre las LAN de la compañía y conectan sucursales individuales a una red conmutada por paquete. Varias conexiones se pueden mutiplexar en las líneas alquiladas, dando por resultado enlaces más cortos y menos necesidad de interfaces.

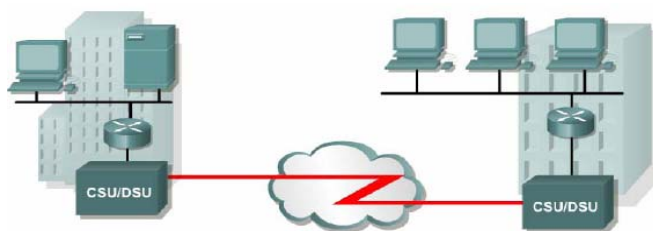


Figura 1.7 Interfaz de acceso Básico y Principal

1.6.4 X.25

Debido al costo de las líneas alquiladas, los proveedores de telecomunicaciones introdujeron las redes conmutadas por paquetes utilizando líneas compartidas para reducir los costos. La primera de estas redes conmutadas por paquetes se estandarizó como el grupo de protocolos X.25.

X.25 ofrece una capacidad variable y compartida de baja velocidad de transmisión que puede ser conmutada o permanente.

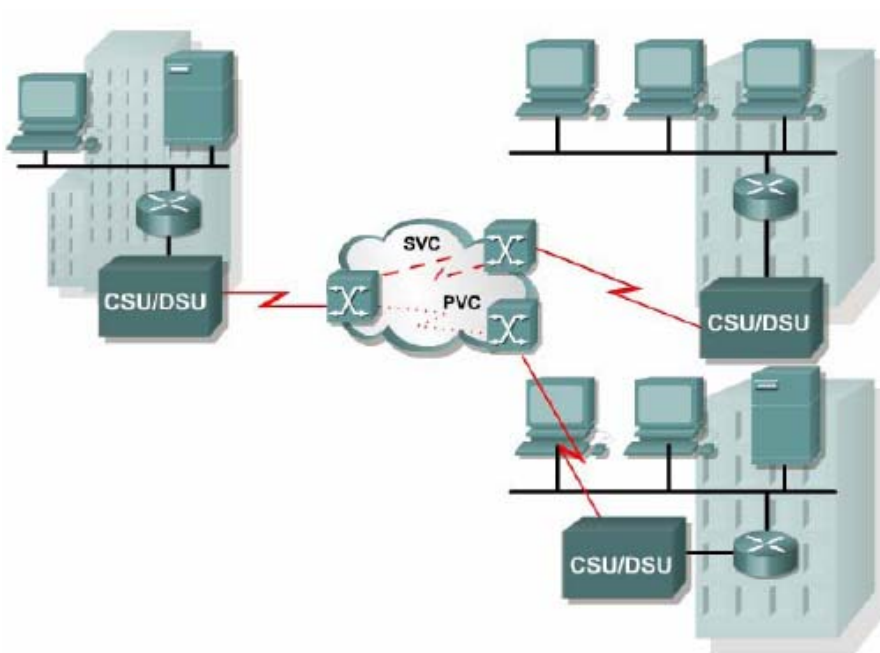


Figura 1.8 Ejemplo de Red tipo X.25

X.25 es un protocolo de capa de red y los suscriptores disponen de una dirección en la red. Los circuitos virtuales se establecen a través de la red con paquetes de petición de llamadas a la dirección destino. Un número de canal identifica la SVC resultante. Los

paquetes de datos rotulados con el número del canal se envían a la dirección correspondiente. Varios canales pueden estar activos en una sola conexión.

Los suscriptores se conectan a la red X.25 con una línea alquilada o con una conexión de acceso telefónico.

Además, las redes X.25 pueden tener canales preestablecidos entre los suscriptores que proveen un PVC.

X.25 puede resultar muy económica porque las tarifas se calculan con base en la cantidad de datos enviados y no el tiempo de conexión ni la distancia. Los datos se pueden enviar a cualquier velocidad igual o menor a la capacidad de conexión. Esto ofrece más flexibilidad. Las redes X.25 por lo general tienen poca capacidad, con un máximo de 48 kbps. Además, los paquetes de datos están sujetos a las demoras típicas de las redes compartidas (2).

En los Estados Unidos, la tecnología X.25 ya no está ampliamente disponible como una tecnología WAN.

Frame Relay ha reemplazado a X.25 en muchos sitios donde se encuentran los proveedores de servicios.

Las aplicaciones típicas de X.25 son los lectores de tarjeta de punto de venta. Estos lectores utilizan X.25 en el modo de conexión telefónica para validar las transacciones en una computadora central. Algunas empresas usan también las redes de valor agregado (VAN) basadas en X.25 para transmitir facturas, pólizas de embarque y otros documentos comerciales usando el Intercambio electrónico de datos (EDI). Para estas aplicaciones, el bajo ancho de banda y la alta latencia no constituyen un problema, porque el bajo costo de X.25 lo compensa (4).

1.6.5 FRAME RELAY

Con la creciente demanda de mayor ancho de banda y menor latencia en la conmutación de paquetes, los proveedores de comunicaciones introdujeron el Frame Relay. Aunque la configuración de la red parece similar a la de X.25, la velocidad de transmisión de datos disponible es por lo general de hasta 4 Mbps y algunos proveedores ofrecen aún mayores velocidades.

Frame Relay difiere de X.25 en muchos aspectos. El más importante es que es un protocolo mucho más sencillo que funciona a nivel de la capa de enlace de datos y no en la capa de red.

Frame Relay no realiza ningún control de errores o flujo. El resultado de la administración simplificada de las tramas es una reducción en la latencia, y las medidas tomadas para evitar la acumulación de tramas en los switches intermedios ayudan a reducir las fluctuaciones de fase.

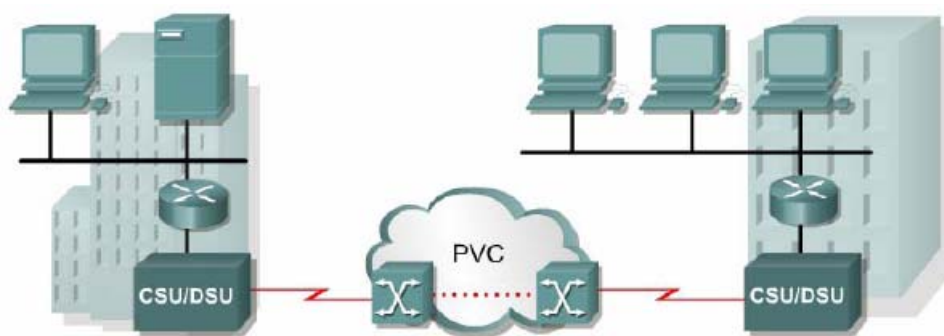


Figura 1.9 Ejemplo de una Red tipo Frame-Relay

La mayoría de las conexiones de Frame Relay son PVC y no SVC. La conexión al extremo de la red con frecuencia es una línea alquilada, pero algunos proveedores ofrecen conexiones telefónicas utilizando líneas ISDN. El canal D ISDN se utiliza para configurar una SVC en uno o más canales B. Las tarifas de Frame Relay se calculan con base en la capacidad del puerto de conexión al extremo de la red. Otros factores son la capacidad

acordada y la velocidad de información suscripta (CIR) de los distintos PVC a través del puerto.

Frame Relay ofrece una conectividad permanente, compartida, de ancho de banda mediano, que envía tanto tráfico de voz como de datos. Frame Relay es ideal para conectar las LAN de una empresa. El router de la LAN necesita sólo una interfaz, aún cuando se estén usando varios VC. La línea alquilada corta que va al extremo de la red Frame Relay permite que las conexiones sean económicas entre LAN muy dispersas.

Los switches Frame Relay (FRS) crean circuitos virtuales para la interconexión de LANs remotas a WANs. La red Frame Relay se establece entre un dispositivo de frontera de una LAN, por lo general un router, y el switch del proveedor del servicio. La tecnología utilizada por el proveedor para transportar los datos entre los switches no es importante en el caso de Frame Relay.

Una red Frame Relay puede ser privada, pero es más común que se use los servicios de una compañía de servicios externa. Una red Frame Relay consiste, en general, de muchos switches Frame Relay esparcidos geográficamente, los cuales se interconectan mediante líneas troncales

Con frecuencia, se usa Frame Relay para la interconexión de LANs. En estos casos, un router en cada una de las LANs será el DTE. Una conexión serial, como una línea arrendada T1/E1, conecta el router al switch Frame Relay de la compañía de servicio en su punto de presencia más cercano al router. El switch Frame Relay es un dispositivo DCE. Las tramas se envían y entregan desde un DTE a otro DTE utilizando la red de Frame Relay creada por los DCE de la compañía de servicios.

Otros equipos de computación que no se encuentren en la LAN pueden también enviar datos a través de la red Frame Relay. Dichos equipos utilizan como DTE a un dispositivo de acceso a Frame Relay (FRAD). (7)

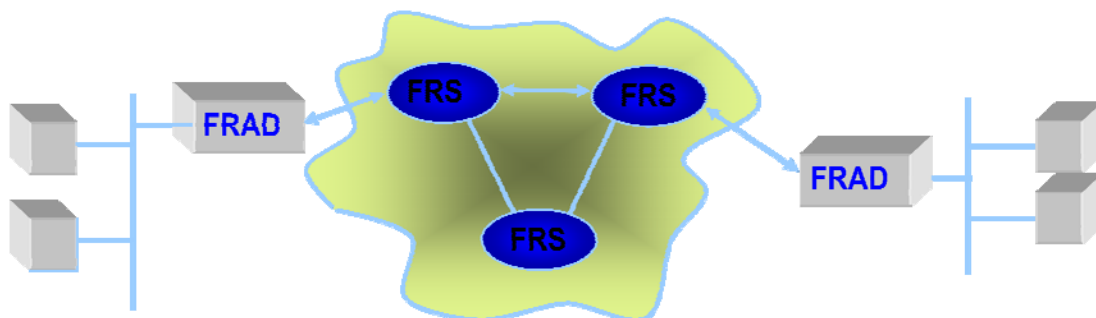


Figura 1.10 Esquema de una Red Frame Relay

FUNCIONAMIENTO DE FRAME RELAY

La conexión a través de la red Frame Relay entre dos DTE se denomina circuito virtual (VC). Los circuitos virtuales pueden establecerse de forma dinámica mediante el envío de mensajes de señalización a la red. En este caso se denominan circuitos virtuales conmutados (SVC). Sin embargo, los SVC no son muy comunes. Por lo general se usan circuitos virtuales permanentes (PVC), previamente configurados por la compañía de servicios. Un VC se crea al almacenar la información de asignación de puerto de entrada al puerto de salida en la memoria de cada switch y así se enlaza un switch con otro hasta que se identifica una ruta continua de un extremo del circuito al otro. (2)

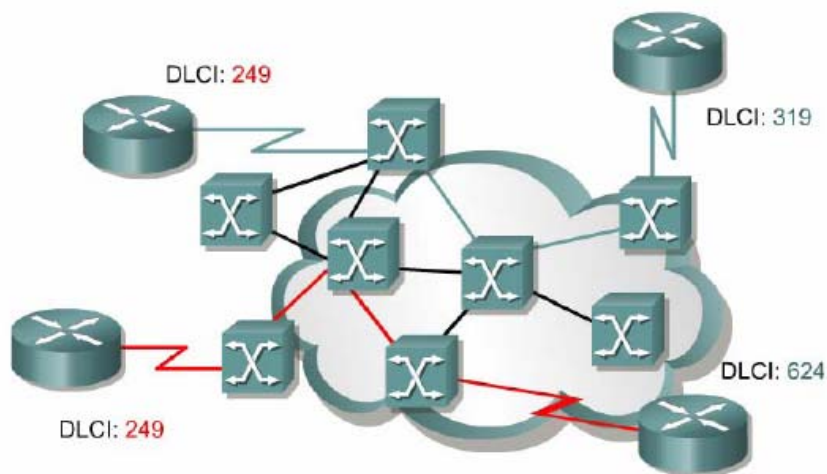


Figura 1.11 Esquema de una Red Frame Relay

La tecnología Frame Relay opera de acuerdo al siguiente esquema:

- ✓ Toma los paquetes de datos provenientes de un protocolo de capa de red como IP o IPX.
- ✓ Los encapsula con un campo de dirección que contiene información del DLCI y el *checksum*.
- ✓ Finalmente los pasa a la capa física para su envío por el cable

La Secuencia de verificación de trama (FCS⁶) se utiliza para determinar si durante la transmisión se produjo algún error en el campo de dirección de la Capa 2. La FCS se calcula antes de la transmisión y el resultado se inserta en el campo de la FCS. En el otro extremo, un segundo valor de FCS se calcula y compara con la FCS de la trama. Si los resultados son iguales, se procesa la trama. Si existe una diferencia, la trama se descarta. No se envía una notificación a la fuente cuando se descarta una trama. El control de errores tiene lugar en las capas superiores del modelo OSI (2)

La conexión serial o el enlace de acceso a la red Frame Relay se hace, generalmente, mediante una línea arrendada. La velocidad de la línea es la velocidad de acceso o velocidad de puerto. Las velocidades de puerto por lo general son de 64 Kbps y 4 Mbps. Algunos proveedores ofrecen velocidades de hasta 45Mbps.

Frame Relay - LMI

La tecnología Frame Relay fue diseñada para ofrecer transferencias de datos conmutados por paquetes con un mínimo retardo de extremo a extremo. Se omitió todo lo que pudiera contribuir a los retardos. Cuando los fabricantes implementaron la Frame Relay como una tecnología separada y no como un componente de ISDN, decidieron que era necesario disponer de DTE para obtener información sobre el estado de la red de forma dinámica. Esta característica no estaba incluida en el diseño original. Las extensiones

⁶ FCS: Frame Check Sequence

creadas para habilitar la transferencia de la información de estado se llaman Interfaz de administración local (LMI) (2).

El campo de 10 bits del DLCI permite identificadores de VC que van desde 0 hasta 1023. Las extensiones LMI se reservan algunos de estos identificadores. Esto reduce el número de VC permitidos. Los mensajes LMI se intercambian entre los DTE y los DCE utilizando los DLCI reservados.

Las extensiones LMI incluyen la siguiente información:

- ✓ El mecanismo de actividad, el cual comprueba que un VC esté en funcionamiento
- ✓ El mecanismo multicast
- ✓ El control de flujo
- ✓ La capacidad de dar significado global a los DLCIs.
- ✓ El mecanismo de estado de los VC

Existen varios tipos de LMI, todos incompatibles entre ellos. El tipo de LMI configurado en el router debe coincidir con el utilizado por el proveedor de servicios. Los routers Cisco soportan tres tipos de LMI:

- ✓ **Cisco:** las extensiones LMI originales
- ✓ **ANSI:** las correspondientes al estándar ANSI T1.617 Anexo D
- ✓ **q933a:** las correspondientes al estándar UIT Q933 Anexo A

NOTA: En las prácticas se usará el estándar ANSI LMI, ya que este es el aceptado por el simulador Dynagen.

TASA DE INFORMACIÓN CONTRATADA (CIR)

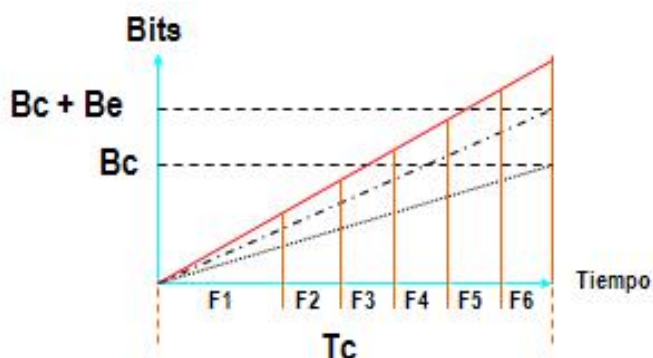


Figura 1.12 Tasa de Información Comprometida

La tasa de información contratada CIR es el valor en bits por segundo (velocidad) que un proveedor de servicio acuerda para transferencia de datos en condiciones normales.

Hay una componente de bit B_c y una componente de tiempo T_c tales que:

$$\text{CIR} = B_c / T_c.$$

Se define también un tamaño de ráfaga de datos en exceso dentro del contrato

(Be).

En un tiempo T_c , las tramas con un contenido de bits mayor que B_c y menor que $B_c + B_e$ pueden ser marcadas con el bit de descargo **DE**.

Las Tramas con un contenido de bits superior a $B_c + B_e$ pueden ser descartadas instantáneamente.

- En la **Figura 1.12**, de F1 a F4 son tramas que han sido enviadas en un tiempo T_c .
- El contenido de bits de estas tramas está en el área sombreada para cada período de transmisión de trama.
- Los valores F1 y F2 están por debajo del valor B_c y serán transmitidos normalmente.
- El valor F3 está sobre B_c , de modo que puede ser marcado con un bit DE.

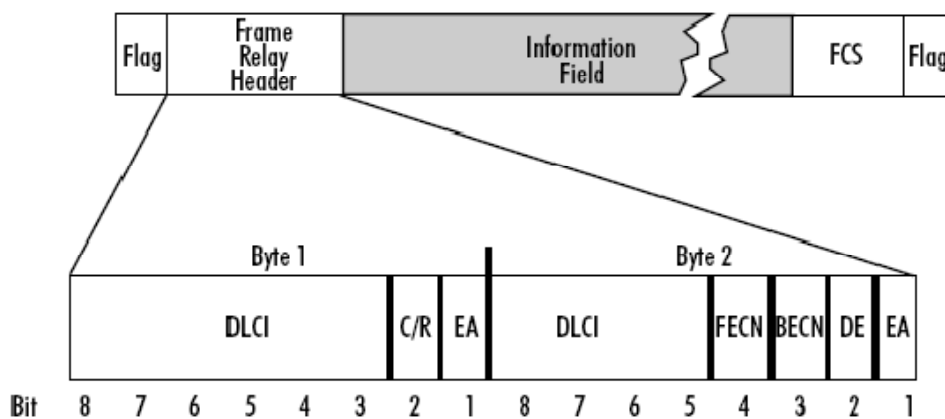
- El valor F4 está sobre $B_c + B_e$, y puede ser marcado con un bit DE o puede ser descartado.

Cuando un switch detecta el crecimiento de su cola, trata de reducir el flujo de tramas hacia él. Esto lo hace notificando a los DTE de la existencia del problema, al activar los bits de la notificación explícita de congestión (ECN) en el campo de dirección de las tramas.

El bit de Notificación explícita de congestión hacia adelante (FECN) se activa en cada trama que el switch recibe en el enlace congestionado. El bit de Notificación explícita de congestión hacia atrás (BECN) se configura en cada trama que el switch coloca en el enlace congestionado. Se espera que los DTE que reciben tramas con el grupo de bits ECN activos intenten reducir el flujo de tramas hasta que la congestión desaparezca.

Si la congestión tiene lugar en un troncal interno, los DTE pueden recibir una notificación aun cuando ellos no sean la causa.

Los bits DE, FECN y BECN forman parte del campo de dirección de las tramas LAPF **Figura 1.13**



- DCLI = Data Link Connection Identifier
- C/R = Command/Response Field Bit (application specific - not modified by network)
- FECN = Forward Explicit Congestion Notification
- BECN = Backward Explicit Congestion Notification
- DE = Discard Eligibility Indicator
- EA = Extension Bit (allows indication of 3 or 4 byte header)

Figura 1.13 Entramado Frame Relay

1.6.6 ATM -Asynchronous Transfer Mode-

Los proveedores de comunicaciones vieron la necesidad de una tecnología de red compartida permanente que ofreciera muy poca latencia y fluctuación a anchos de banda mucho más altos. Su solución fue el Modo de Transferencia Asíncrona (ATM). ATM tiene una velocidad de transmisión de datos superior a los 155 Mbps. Al igual que las otras tecnologías compartidas, como X.25 y Frame Relay, los diagramas de las WAN ATM se ven igual

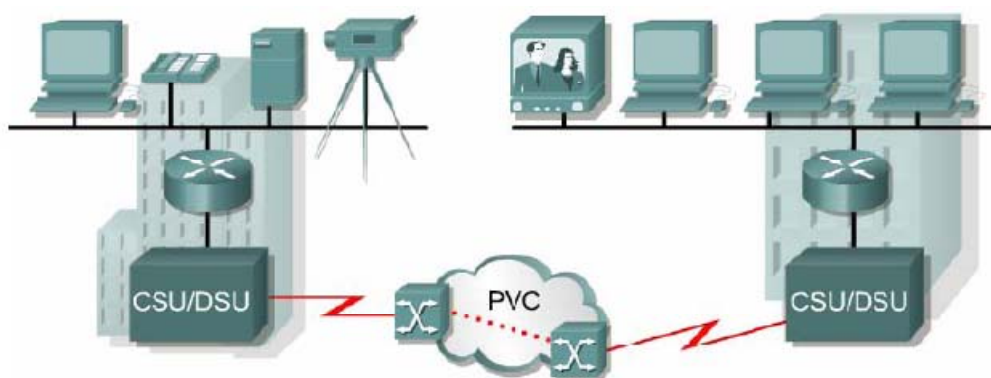


Figura 1.14 Ejemplo de una Red ATM

La tecnología ATM es capaz de transferir voz, video y datos a través de redes privadas y públicas. Tiene una arquitectura basada en celdas más bien que una basada en tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes. La celda ATM de 53 bytes contiene un encabezado ATM de 5 bytes seguido de 48 bytes de carga ATM. Las celdas pequeñas de longitud fija son adecuadas para la transmisión de tráfico de voz y video porque este tráfico no tolera demoras. El tráfico de video y voz no tiene que esperar que se transmita un paquete de datos más grande.

La celda ATM de 53 bytes es menos eficiente que las tramas y paquetes más grandes de Frame Relay y X.25. Además, la celda ATM tiene un encabezado de por lo menos 5 bytes por cada 48-bytes de datos. Cuando la celda está transportando paquetes de capa de red segmentados, la carga general será mayor porque el switch ATM tiene que poder reagrupar los paquetes en el destino. Una línea ATM típica necesita casi un 20% más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa

de red. ATM ofrece tanto los PVC como los SVC, aunque los PVC son más comunes en las WAN.

Como las otras tecnologías compartidas, ATM permite varios circuitos virtuales en una sola conexión de línea alquilada al extremo de red.

1.6.7 DSL *Digital Subscriber Line*

La tecnología de Línea Digital del suscriptor (DSL) es una tecnología de banda ancha que utiliza líneas telefónicas de par trenzado para transportar datos de alto ancho de banda para dar servicio a los suscriptores. El servicio DSL se considera de banda ancha, en contraste con el servicio de banda base típico de las LAN. Banda ancha se refiere a la técnica que utiliza varias frecuencias dentro del mismo medio físico para transmitir datos. El término xDSL se refiere a un número de formas similares, aunque en competencia, de tecnologías DSL:

- ✓ DSL Asimétrico (ADSL)
- ✓ DSL simétrico (SDSL)
- ✓ DSL de alta velocidad de bits (HDSL)
- ✓ ISDN (como) DSL (IDSL)
- ✓ DSL para consumidores (CDSL), también llamado DSL-lite o G.lite

Servicio	Descargar	Cargar
ADSL	64 kbps - 8.192 Mbps	16 kbps - 640 kbps
SDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
HDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
IDSL	144 kbps	144 kbps
CDSL	1 Mbps	16 kbps - 160 kbps

Figura 1.15 Tipos de Servicio DSL

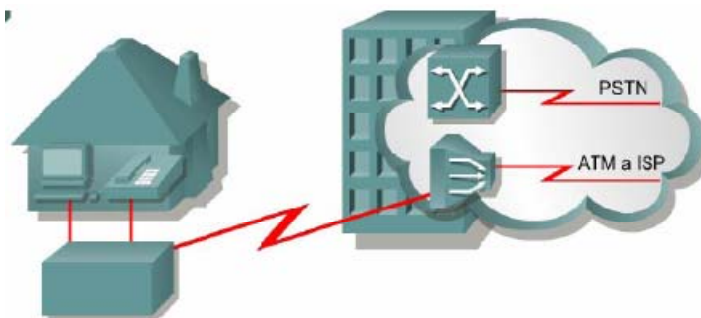


Figura 1.16 Ejemplo de una Red DSL

La tecnología DSL permite que el proveedor de servicios ofrezca a los clientes servicios de red de alta velocidad, utilizando las líneas de cobre de bucle local instaladas.

La tecnología DSL permite que la línea de bucle local se utilice para realizar conexiones telefónicas de voz normales y conexiones permanentes para tener conectividad de red al instante. Las líneas del suscriptor DSL múltiples se pueden multiplexar a un enlace de alta capacidad al usar el Multiplexor de acceso DSL (DSLAM) en el sitio del proveedor. Los DSLAM incorporan la tecnología TDM para juntar muchas líneas del suscriptor a un solo medio más pequeño, en general una conexión T3/DS3. Las tecnologías DSL están utilizando técnicas de codificación y modulación complejas para lograr velocidades de transmisión de datos de hasta 8.192 Mbps.

El canal de voz de un teléfono estándar cubre un rango de frecuencia de 330 Hz a 3.3 KHz. Un rango de frecuencia, o ventana, de 4 KHz se considera como requisito para cualquier transmisión de voz en un bucle local. Las tecnologías DSL cargan (upstream: corriente arriba) y descargan (downstream: corriente abajo) datos a frecuencia superiores a esta ventana de 4 KHz. Esta técnica es lo que permite que la transmisión de voz y datos tenga lugar de modo simultáneo. En un servicio DSL existen dos tipos básicos de tecnología DSL: la asimétrica (ADSL) y la simétrica (SDSL). Todas las formas de servicio DSL se pueden clasificar como ADSL o SDSL y existen muchas variedades de cada tipo.

El servicio asimétrico brinda mayor ancho de banda de descarga o downstream al usuario que el ancho de banda de carga. El servicio simétrico brinda la misma capacidad en ambas direcciones.

No todas las tecnologías DSL permiten el uso de un teléfono. SDSL se conoce como cobre seco porque no tiene un tono de llamada y no ofrece servicio telefónico en la misma línea. Por eso se necesita una línea separada para el servicio SDSL.

Los distintos tipos de DSL brindan diferentes anchos de banda, con capacidades que exceden aquellas de línea alquilada T1 o E1. La velocidad de transferencia depende de la longitud real del bucle local y del tipo y condición de su cableado. Para obtener un servicio satisfactorio, el bucle debe ser menor a 5,5 kilómetros (3,5 millas). La disponibilidad de DSL está lejos de ser universal, y hay una gran variedad de tipos, normas y normas emergentes. No es una opción popular entre los departamentos de computación de las empresas para apoyar a las personas que trabajan en sus hogares. Por lo general, el suscriptor no puede optar por conectarse a la red de la empresa directamente, sino que primero tiene que conectarse a un proveedor de servicios de Internet (ISP). Desde allí, se realiza una conexión IP a través de Internet hasta la empresa. Así se corren riesgos de seguridad. Para tratar las cuestiones de seguridad, los servicios DSL ofrecen funciones para utilizar conexiones la Red privada virtual VPN a un servidor VPN, que por lo general se encuentra ubicado en la empresa.

1.6.8 CABLE MÓDEM

El cable coaxial es muy usado en áreas urbanas para distribuir las señales de televisión. El acceso a la red está disponible desde algunas redes de televisión por cable. Esto permite que haya un mayor ancho de banda que con el bucle local de teléfono.

Los cable módem mejorados permiten transmisiones de datos de alta velocidad de dos vías, usando las mismas líneas coaxiales que transmiten la televisión por cable. Algunos proveedores de servicio de cable prometen velocidades de transmisión de datos de hasta 6,5 veces más altas que las líneas alquiladas T1.

Esta velocidad hace que el cable sea un medio atractivo para transferir grandes cantidades de información digital de manera rápida, incluyendo video clips, archivos de audio y grandes cantidades de datos. La información que tardaría dos minutos en descargar

usando un BRI ISDN puede descargarse en dos segundos a través de una conexión de cable módem.

El cable módem ofrece una conexión permanente y una instalación simple. Una conexión de cable permanente significa que los computadores conectados pueden estar sujetos a una ruptura en la seguridad en cualquier momento y necesitan estar adecuadamente asegurados con firewalls. Para tratar las cuestiones de seguridad, los servicios cable módem ofrecen funciones para utilizar conexiones de Red privada virtual VPN a un servidor VPN, que por lo general se encuentra ubicado en la empresa.

Un cable módem puede ofrecer de 30 a 40 Mbps de datos en un canal de cable de 6 MHz. Esto es casi 500 veces más rápido que un módem de 56 Kbps.

Con un cable módem, el suscriptor puede continuar recibiendo servicio de televisión por cable mientras recibe datos en su computador personal de forma simultánea. Esto se logra con la ayuda de un divisor de señal uno a dos.

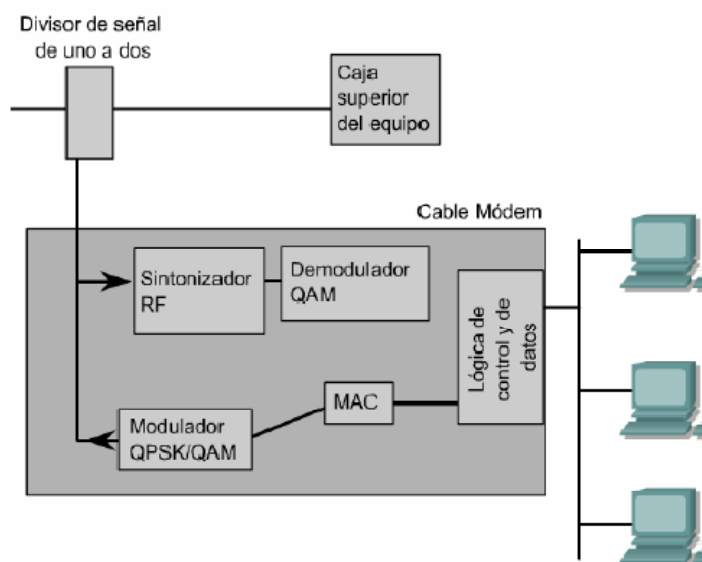


Figura 1.17 Esquema de Red de una instalación por Cable Módem

Los suscriptores de cable módem deben utilizar el ISP asociado con el proveedor de servicio. Todos los suscriptores locales comparten el mismo ancho de banda del cable. A medida que más usuarios contratan el servicio el ancho de banda disponible puede caer por debajo de la velocidad esperada.

Los dispositivos WAN como Routers o Switches de capa tres, usan protocolos de enrutamiento los cuales nos permiten llevar los paquetes a su destino, al igual que el servicio postal, existen varios los cuales se analizarán con más detalle a continuación.

1.7 ALGORITMOS DE ENRUTAMIENTO

El Algoritmo de Enrutamiento es aquella parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada, esta decisión debe tomarse cada vez que llega un paquete, dado que la mejor ruta puede haber cambiado desde la última vez.

Los algoritmos de enrutamiento pueden agruparse en dos clases principales: *no adaptativos* y *adaptativos*. Los *algoritmos no adaptativos* no basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico y la topología actuales, es decir sus decisiones se toman por adelantado, fuera de línea, y se carga en los enrutadores al arrancar la red. Este procedimiento se conoce como *enrutamiento estático*.

En contraste los algoritmos adaptativos cambian sus decisiones de enrutamiento para reflejar los cambios de topología y, por lo general también el tráfico. Los algoritmos adaptativos difieren en el lugar de donde obtienen su información, el momento de cambio de sus rutas, y la métrica usada para la optimización (distancia, número de saltos o tiempo estimado de tránsito)

1.7.1 TIPOS DE ALGORITMOS DE ENRUTAMIENTO

1.7.1.1 Enrutamiento por Vector Distancia.

En el enrutamiento por vector distancia, cada enrutador mantiene una tabla de enrutamiento indizada por, y conteniendo un registro de, cada enrutador de la subred. Esta entrada comprende dos partes: la línea preferida de salida hacia ese destino y una

estimación del tiempo o distancia a ese destino. La métrica usada podría ser la cantidad de saltos, el retardo de tiempo en milisegundos, el número total de paquetes encolados a lo largo de la ruta (1).

Características Principales:

- ✓ Los Routers cooperan en un cálculo distribuido de las rutas.
 - ✓ El algoritmo en cada router calcula el mejor camino (mínimo coste) a todos los destinos
 - ✓ Cada router informa a sus vecinos de las rutas que ha calculado
 - ✓ Informan de la dirección (vector) y el coste (la distancia) a cada destino
 - ✓ Viendo las rutas anunciadas por los vecinos puede que el router encuentre un mejor camino (menor coste)
 - ✓ El cálculo es: simple, asíncrono, incremental y distribuido
- Ejemplos: RIP, IPX-RIP, DECnet, IGRP, EIGRP*

1.7.1.2 Enrutamiento por Estado de Enlace.

El enrutamiento por vector distancia se uso en ARPANET⁷ hasta 1979, cuando fue reemplazado por el enrutamiento de estado de enlace. Dos problemas principales causaron su desaparición, primero debido a que la métrica de retardo era la longitud de la cola, no tomaba en cuenta el ancho de banda al escoger rutas, todas las líneas eran de 56Kbps por lo que el ancho de banda no era importante, pero luego de la modernización algunas líneas llegaban a 1,544 Mbps lo cual produjo problemas (1).

Características Principales:

- ✓ Aproximación de base de datos distribuida replicada en vez de un cálculo distribuido incremental
- ✓ Cada router posee información global sobre la red: nodos y enlaces existentes

⁷ ARPANET: Advanced Research Projects Agency Network: Red de computadores creado por el Departamento de Defensa, espina dorsal del internet hasta 1990

- Los Routers informan de sus enlaces a redes activas y con routers vecinos
- “Inundan” la red con esta información para que llegue a todos los Routers
- “Cómo?” hacer esta inundación es uno de los principales problemas de estos protocolos
- ✓ Todos los Routers tienen una imagen (grafo) de la red (todos la misma) y a partir de ahí eligen los caminos
- ✓ Menor tiempo de convergencia que VD –vector distancia- ante cambios en la red
- ✓ Ejemplos: OSPF, IS-IS, PNNI

1.7.1.3 Enrutamiento por la ruta más corta.

Uno de los ejemplos más claros de la utilización de los algoritmos adaptativos es el concepto de la ruta más corta, que es usada por OSPF, en si es la aplicación del algoritmo de Dijkstra (1959).

Este algoritmo usa el ancho de banda, o el retardo medio en encolamiento, como métrica, para la etiquetación de cada ruta, para luego establecer la ruta más corta y más rápida (1).

Para ilustrar el funcionamiento del algoritmo de etiquetado, observe el grafo ponderado no dirigido de la **Figura 1.18(a)**, donde las ponderaciones representan, por ejemplo, distancias. Queremos encontrar la ruta más corta posible de *A* a *D*, Comenzamos por marcar como permanente el nodo *A*, indicado por un círculo relleno. Después examinamos, por turno, cada uno de los nodos adyacentes a *A* (el nodo de trabajo), reetiquetando cada uno con la distancia desde *A*. Cada vez que reetiquetamos un nodo, también lo reetiquetamos con el nodo desde el que se hizo la prueba, para poder reconstruir más tarde la ruta final. Una vez que terminamos de examinar cada uno de los nodos adyacentes a *A*, examinamos todos los nodos etiquetados tentativamente en el grafo completo y hacemos permanente el de la etiqueta más pequeña, como se muestra en la **Figura 1.18(b)**. Éste se convierte en el nuevo nodo de trabajo (1).

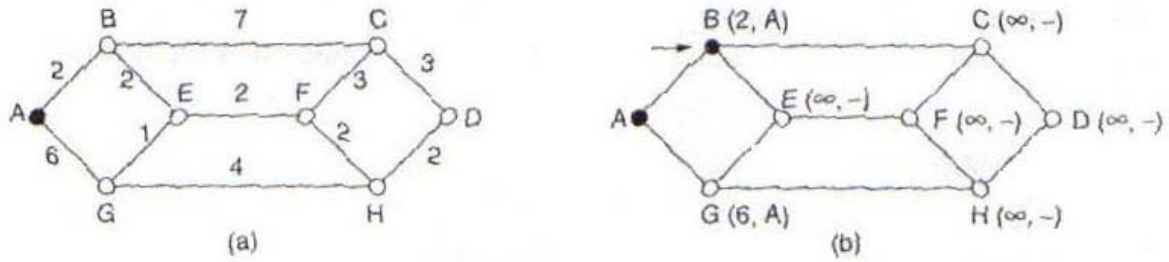


Figura 1.18(a) y (b) Grafo de Algoritmo de Dijkstra

Ahora comenzamos por B , y examinamos todos los nodos adyacentes a él. Si la suma de la etiqueta de B y la distancia desde B al nodo en consideración es menor que la etiqueta de ese nodo, tenemos una ruta más corta, por lo que se re etiqueta ese nodo.

Tras inspeccionar todos los nodos adyacentes al nodo de trabajo y cambiar las etiquetas tentativas (de ser posible), se busca en el grafo completo el nodo etiquetado tentativamente con el menor valor. Este nodo se hace permanente y se convierte en el nodo de trabajo para la siguiente ronda. En la **Figura 1.18** se muestran los primeros cinco pasos del algoritmo (1).

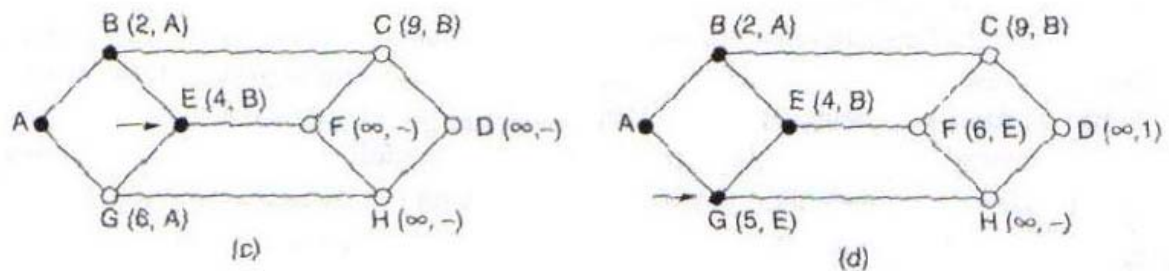


Figura 1.18(c) y (d) Grafo de Algoritmo de Dijkstra

Para ver por qué funciona el algoritmo, vea la **Figura 1.18(c)**. En ese punto acabamos de hacer permanente a E . Suponga que hubiera una ruta más corta que ABE , digamos $AXYZE$. Hay dos posibilidades: el nodo Z ya se hizo permanente, o no se ha hecho permanente. Si ya es permanente, entonces E ya se probó (en la ronda que siguió a aquella en la que se hizo permanente Z), por lo que la ruta $AXYZE$ no ha escapado a nuestra atención y, por lo tanto, no puede ser una ruta más corta (1).

Ahora considere el caso en el que Z aún está etiquetado tentativamente. O bien la etiqueta de Z es mayor o igual que la de E , en cuyo caso $AXYZE$ no puede ser una ruta más corta

que ABE , o menor que la de E , en cuyo caso Z , y no E , se volverá permanente primero, lo que permitirá que E se pruebe desde Z (1).

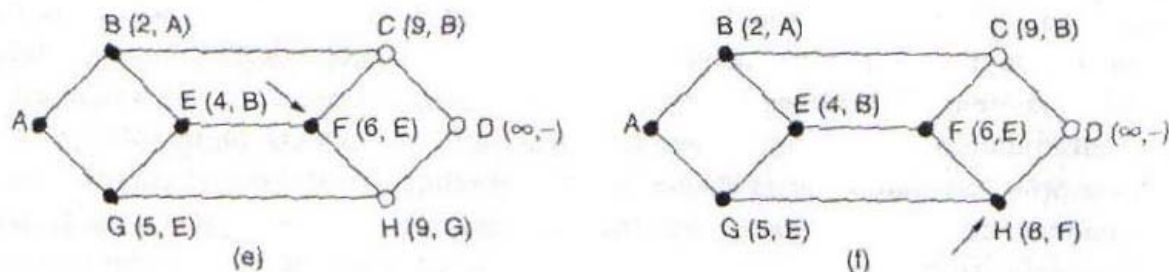


Figura 1.18(e) y (f) Grafo de Algoritmo de Dijkstra

1.8 TABLAS DE ENRUTAMIENTO

Los Routers utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo utilizado. Los dispositivos de Capa Red interconectan dominios de *broadcast*⁸ o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos (2).

Los Routers mantienen información importante en sus tablas de enrutamiento, que incluye lo siguiente:

Tipo de protocolo: el tipo de protocolo de enrutamiento que creó la entrada en la tabla de enrutamiento

Asociaciones entre destino/siguiente salto: estas asociaciones le dicen al Router que un destino en particular está directamente conectado al Router, o que puede ser alcanzado utilizando un Router denominado "salto siguiente" en el trayecto hacia el destino final. Cuando un Router recibe un paquete entrante, lee la dirección destino y verifica si hay concordancia entre esta dirección y una entrada de la tabla de enrutamiento.

⁸ Broadcast: En castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea

Métrica de enrutamiento: los distintos protocolos de enrutamiento utilizan métricas de enrutamiento distintas. Las métricas de enrutamiento se utilizan para determinar la conveniencia de una ruta. Por ejemplo, el número de saltos es la única métrica de enrutamiento que utiliza el protocolo de información de enrutamiento (RIP). El protocolo de enrutamiento de puerta interior (IGRP) utiliza una combinación de ancho de banda, carga, retardo y confiabilidad como métricas para crear un valor métrico compuesto (2).

Interfaces de salida: la interfaz por la que se envían los datos para llegar a su destino final.

1.9 PROTOCOLO DE INTERNET IP

Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host.

Algunos protocolos como los IPX⁹, requieren sólo de un número de red porque estos protocolos utilizan la dirección MAC del Host como número de Host. Otros protocolos, como el IP, requieren una dirección completa que especifique la porción de red y la porción de Host. Estos protocolos también necesitan una máscara de red para diferenciar estos dos números. La dirección de red se obtiene al realizar la operación "AND" con la dirección y la máscara de red (2).

Existen dos tipos de servicios de envío: los no orientados a conexión y los orientados a conexión. Estos dos servicios son los que realmente permiten el envío de datos de extremo a extremo en una *internetwork*. La mayoría de los servicios utilizan sistemas de entrega no orientados a conexión. Es posible que los diferentes paquetes tomen distintas rutas para transitar por la red, pero se reensamblan al llegar a su destino. En un sistema no orientado a conexión, no se comunica con el destino antes de enviar un paquete.

⁹ IPX: Protocolo de comunicaciones NetWare que se utiliza para encaminar mensajes de un nodo a otro. Los paquetes IPX incluyen direcciones de redes y pueden enviarse de una red a otra.

Una buena comparación para un sistema no orientado a conexión es el sistema postal. No se comunica con el destinatario para ver si aceptará la carta antes de enviarla. Además, el remitente nunca sabe si la carta llegó a su destino.

1.10 PROTOCOLOS DE PUERTA INTERIOR Y EXTERIOR IGP/EGP

Un sistema autónomo es una red o conjunto de redes bajo un control común de administración, tal como el dominio espe.edu.ec. Un sistema autónomo está compuesto por routers que presentan una visión coherente del enrutamiento al mundo exterior.

Los Protocolos de Enrutamiento de Gateway interior (IGP) y los Protocolos de Enrutamiento de Gateway exterior (EGP) son dos tipos de protocolos de enrutamiento.

Los IGP enrutan datos dentro de un sistema autónomo.

- ✓ Protocolo de información de enrutamiento (RIP) y (RIPv2).
- ✓ Protocolo de enrutamiento de Gateway interior (IGRP)
- ✓ Protocolo de enrutamiento de Gateway interior mejorado (EIGRP)
- ✓ Primero la ruta libre más corta (OSPF)
- ✓ Protocolo de sistema intermedio-sistema intermedio (IS-IS).

Los EGP enrutan datos entre sistemas autónomos. Un ejemplo de EGP es el protocolo de Gateway fronterizo (BGP) *Border Gateway Protocol* por sus siglas en inglés.

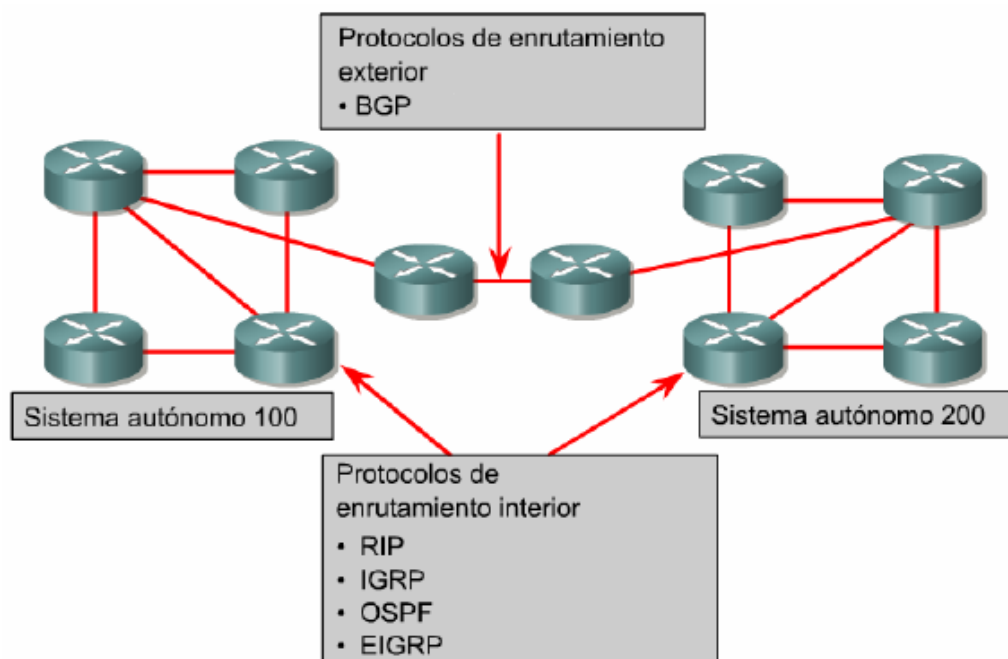


Figura 1.19 Protocolos de Enrutamiento en distintos sistemas autónomos.

1.11 CONEXIONES WAN

Para las comunicaciones de larga distancia, las WAN utilizan transmisiones seriales. Este es un proceso por el cual los bits de datos se envían por un solo canal. Este proceso brinda comunicaciones de larga distancia confiables y el uso de un rango específico de frecuencias ópticas o electromagnéticas (2).

Las frecuencias se miden en términos de ciclos por segundo y se expresan en Hercios (Hz). Las señales que se transmiten a través de las líneas telefónicas de grado de voz utilizan 4 kilohercios (KHz). El tamaño del rango de frecuencia se denomina ancho de banda. En el *networking*, el ancho de banda es la medida de bits por segundo que se transmite.

Datos (bps)	Distancia (Metros) EIA/TIA-232	Distancia (Metros) EIA/TIA-449
2400	60	1250
4800	30	625
9600	15	312
19200	15	156
38400	15	78
115200	3,7	--
T1(1.544Mbps)	--	15

Tabla 1.1 Cables Seriales WAN

Para un router Cisco, existen dos tipos de conexiones seriales que proveen la conectividad física en las instalaciones del cliente. El primer tipo de conexión serial es el conector de 60 pines. El segundo es un conector más compacto conocido como "smart serial". El conector utilizado por el proveedor varía de acuerdo con el tipo de equipo de servicios (2).

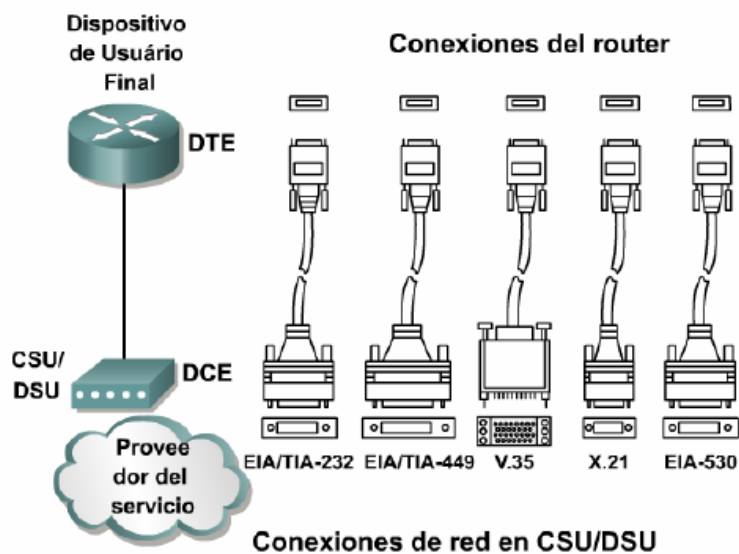


Figura 1.20 Conectores de Red WAN

Si la conexión se hace directamente con el proveedor de servicio, o con un dispositivo que provee señal de temporización tal como la unidad de servicio de canal/datos (CSU/DSU), el router será un equipo terminal de datos (DTE) y usará cable serial DTE. Por lo general, este es el caso. Sin embargo, hay situaciones en las que se requiere que el router local brinde la temporización y entonces utilizará un cable para equipo de comunicación de datos (DCE).

1.12 ENCAPSULAMIENTO WAN

1.12.1 HDLC –High Level Data Link Control-

Los datos de la capa de red se envían a la capa de enlace de datos para su transmisión en un enlace físico, que normalmente es de punto a punto en una conexión WAN. La capa de enlace de datos crea una trama alrededor de los datos de capa de red de modo que se apliquen los controles y verificaciones necesarios (2).

Cada tipo de conexión WAN utiliza un protocolo de Capa de enlace para encapsular el tráfico mientras atraviesa el enlace WAN. Para asegurarse de que se esté utilizando el protocolo de encapsulamiento correcto, se debe configurar el tipo de encapsulamiento de Capa 2 utilizado en cada interfaz serial del router. El protocolo de encapsulamiento que se debe usar depende de la tecnología WAN y del equipo. La mayoría del entramado se basa en el estándar HDLC (7).

El entramado HDLC garantiza una entrega confiable de datos en líneas poco confiables e incluye mecanismos de señalización para el control de flujo y errores. La trama siempre comienza y termina con un campo de señaladores de 8 bits, con un patrón de bit de 01111110. Como existe la posibilidad de que este patrón ocurra en los datos mismos, el sistema de envío HDLC siempre inserta un bit 0 después de cada cinco 1s en el campo de datos, de modo que en la práctica la secuencia de señaladores sólo puede tener lugar en los extremos de la trama. El sistema receptor quita los bits insertados. Cuando las tramas se transmiten de forma consecutiva, el señalador del final de la primera trama se utiliza como señalador de inicio de la trama siguiente.



General HDLC Frame

Figura 1.21 Trama HDLC

Opening Flag, 8 bits [01111110], [7E hex]
Address, 8 bits [could be more]
Control, 8 bits, or 16 bits
Data [Payload], Variable, not used in some frames, or may be padded to complete the fill
CRC, 16 bits, or 32 bits
Closing Flag, 8 bits [01111110], [7E hex]

El campo de dirección no es necesario para los enlaces WAN, los cuales casi siempre son de punto a punto. El campo de dirección está aún presente y puede ser de uno a dos bytes de longitud. El campo de control indica el tipo de trama, que puede ser de información, de supervisión o sin enumerar (2).

- ✓ Las tramas sin enumerar transportan mensajes de configuración de la línea.
- ✓ Las tramas de información transportan datos de la capa de red.
- ✓ Las tramas de supervisión controlan el flujo de tramas de información y peticiones de retransmisión de datos si hubiera algún error (2).

El campo de control, por lo general, consta de un byte, pero en los sistemas de ventanas deslizantes extendidos, tendrá dos bytes. Juntos los campos de control y de dirección se denominan encabezado de la trama. El dato encapsulado sigue el campo de control. Entonces, una secuencia de verificación de trama (FCS) utiliza el mecanismo de verificación por redundancia cíclica (CRC) para establecer un campo de dos o cuatro bytes (2).

Se utilizan varios protocolos de enlace de datos, incluyendo subgrupos y versiones propietarias de HDLC. Tanto PPP como la versión de Cisco de HDLC tienen un campo extra en el encabezado para identificar el protocolo de capa de red del dato encapsulado (2).

Protocolo	Uso
Procedimiento de acceso al enlace balanceado LAPB	X.25
Procedimiento de acceso al enlace en el canal D LAPD	Canal D ISDN
Trama de procedimiento al enlace LAPF	Frame Relay
Control de enlace de datos de alto nivel HDLC	Valor por defecto Cisco
Protocolo Punto a Punto	Conexión de marcacion telefonica

Tabla 1.2 Tipos de Protocolos para enlace

1.12.2 PPP –PEER TO PEER PROTOCOL-

El Protocolo punto a punto (PPP) es el protocolo de preferencia para las conexiones WAN conmutadas seriales. Puede manejar tanto la comunicación síncrona como la asíncrona e incluye la detección de los errores. Y, lo que es más, incorpora un proceso de autenticación que utiliza CHAP o PAP. PPP se puede utilizar en diversos medios físicos, incluyendo cable de par trenzado, líneas de fibra óptica o transmisión satelital.

Las tecnologías WAN se basan en la transmisión serial en la capa física. Esto significa que los bits de una trama se transmiten uno por uno a lo largo del medio físico

Los procesos de la capa física utilizan señalización para pasar los bits que componen la trama de Capa 2, uno por uno, al medio físico. Los métodos de señalización incluyen el Nivel sin retorno a cero (NRZ-L), Binario 3 de alta densidad (HDB3) e Inversión alternada de marcas (AMI). Estos son ejemplos de normas de codificación de capa física, y son similares a la codificación Manchester de Ethernet. Entre otras cosas, estos métodos de señalización pueden diferenciar un método de comunicación serial de otro. Las siguientes son algunas de las muchas normas de comunicación seriales:

- ✓ RS-232-E
- ✓ V.35
- ✓ Interfaz serial de alta velocidad (HSSI)

Arquitectura PPP en capas

PPP utiliza una arquitectura en capas. La arquitectura en capas es un modelo, diseño o plan lógico que ayuda a la comunicación entre las capas interconectadas. PPP proporciona un método para encapsular datagramas de varios protocolos en un enlace de punto a punto y utiliza la capa de enlace de datos para probar esta conexión. Por lo tanto, PPP está compuesto por dos subprotocolos:

- ✓ **Protocolo de control de enlace:** se utiliza para establecer el enlace de punto a punto.
- ✓ **Protocolo de control de red:** se utiliza para configurar los distintos protocolos de capa de red.



Figura 1.22 PPP proceso de capas OSI

Se puede configurar PPP en los siguientes tipos de interfaces físicas:

- ✓ Serial asíncrona.
- ✓ Serial síncrona
- ✓ Interfaz serial de alta velocidad (HSSI)
- ✓ Red digital de servicios integrados (Integrated Services Digital Network, ISDN)

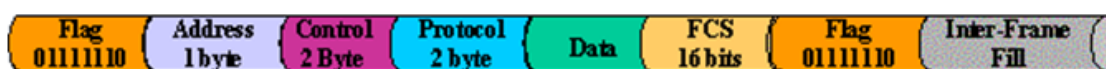
PPP utiliza el Protocolo de control de enlace (LCP) para negociar y configurar las opciones de control en el enlace de datos de la WAN. PPP utiliza el componente del Protocolo de control de red (NCP) para encapsular y negociar las opciones para los

diferentes protocolos de capa de red. El LCP se ubica en la parte más alta de la capa física y se utiliza para establecer, configurar y probar la conexión de enlace de datos.

PPP también utiliza LCP para acordar, de forma automática, opciones de formato de encapsulamiento.

PPP permite que varios protocolos de capa de red operen en el mismo enlace de comunicación. Para cada protocolo de capa de red que se utiliza, se proporciona un Protocolo de control de red (NCP) distinto. Por ejemplo: el Protocolo de Internet (IP) utiliza el Protocolo de control de IP (IPCP) y el Intercambio de paquetes en internetworking (IPX) utiliza el Protocolo de control IPX de Novell (IPXCP). Los NCP incluyen campos funcionales que contienen códigos estandarizados que indican el tipo de protocolo de capa de red que encapsula PPP.

Los campos de una trama PPP son los siguientes:



Point-to-Point Protocol HDLC Frame Encapsulation

Figura 1.23 Trama de PPP

- ✓ **Señalador:** indica el comienzo o el fin de una trama y consiste en la secuencia binaria 01111110.
- ✓ **Dirección:** está formada por la dirección de broadcast estándar, que es la secuencia binaria 11111111. PPP no asigna direcciones de estaciones individuales.
- ✓ **Control:** Secuencia binaria que requiere la transmisión de datos del usuario en una trama no secuencial. Se suministra un servicio de enlace sin conexión similar al del Control de enlace lógico (LLC) Tipo 1.
- ✓ **Protocolo:** 2 bytes que identifican el protocolo encapsulado en el campo de datos de la trama.
- ✓ **Datos:** 0 o más bytes que contienen el datagrama para el protocolo especificado en el campo de protocolo. El fin del campo de datos se detecta al encontrar la secuencia de señalador de cierre y dejando 2 bytes para el campo de la secuencia de

verificación de trama (FCS). La longitud máxima por defecto del campo de datos es 1500 bytes.

- ✓ **FCS:** en general, 16 bits o 2 bytes que se refieren a los caracteres adicionales que se agregan a la trama con el fin de controlar los errores.

Cómo establecer una sesión PPP

El establecimiento de una sesión PPP tiene tres fases: Estas son: *establecimiento del enlace, autenticación y fase del protocolo de la capa de red*. Las tramas LCP se utilizan para realizar el trabajo de cada una de las fases LCP. Las tres siguientes clases de tramas LCP se utilizan en una sesión PPP:

- ✓ Las tramas de establecimiento de enlace se utilizan para establecer y configurar un enlace.
- ✓ Las tramas de terminación del enlace se utilizan para terminar un enlace.
- ✓ Las tramas de mantenimiento del enlace se utilizan para administrar y depurar un enlace

Las tres fases para el establecimiento de una sesión PPP son:

Fase de establecimiento del enlace: en esta fase, cada dispositivo PPP envía tramas LCP para configurar y probar el enlace de datos. Los paquetes LCP contienen un campo de opción de configuración que permite que los dispositivos negocien el uso de opciones tales como la unidad máxima de transmisión (MTU), la compresión de determinados campos PPP y el protocolo de autenticación de enlace. Si no se incluye ninguna opción de configuración en un paquete LCP, se adopta el valor por defecto para esa configuración. Antes de poder intercambiar cualquier datagrama de capa de red, primero, LCP debe abrir la conexión y negociar los parámetros de configuración. Esta fase queda completa después de enviar y recibir una trama de acuse de recibo de configuración.

Fase de autenticación (optativa): una vez establecido el enlace, y seleccionado el protocolo de autenticación, se puede autenticar el dispositivo par. La autenticación, en caso de que se utilice, se lleva a cabo antes de que comience la fase del protocolo de la capa de red. Como parte de esta fase, el LCP también permite efectuar una prueba opcional de determinación de la calidad del enlace. El enlace se prueba para determinar si su calidad es suficiente para activar los protocolos de capa de red.

Fase de protocolo de capa de red: en esta fase, los dispositivos PPP envían paquetes NCP para seleccionar y configurar uno o varios protocolos de capa de red (como IP). Después de configurar cada uno de los protocolos de la capa de red elegidos, se pueden enviar paquetes de cada uno de los protocolos de capa de red a través del enlace. Si LCP cierra el enlace, informa los protocolos de la capa de red, para que puedan tomar las medidas adecuadas. El comando **show interface** en routers revela los estados de LCP y NCP bajo la configuración PPP.

El uso de Routers es primordial en el mundo de las redes además estos dispositivos usan protocolos de enrutamiento para conocer redes próximas o distantes, es por esta razón que el uso de simuladores para emular estos dispositivos es bastante útil. Un router es bastante parecido a un computador con un sistema operativo autónomo y un lenguaje versátil para la configuración de sus rutas, existen muchas marcas en el mundo de la redes los más usados por su estabilidad son Cisco. Además la configuración en otras marcas no difiere mucho porque usan los mismos conceptos.

CAPÍTULO 2

SIMULADOR DYNAMIPS/DYNAGEN

Para el estudio de redes, se han diseñado simuladores los cuales permiten el entrenamiento, con el objetivo de familiarizarse con los dispositivos en su interfaz y consola, existen varios y muy buenos, Dynagen es uno de los más avanzados ya que permite el uso de la mayoría de características de un router.

2.1 INTRODUCCIÓN

Dynamips es un programa emulador de *Routers* Cisco para PC. Hasta el momento de la publicación de este proyecto Dynagen soporta las siguientes series de Routers: 2600, 3600 y 7200. Los objetivos de este emulador son principalmente, hacer uso de una plataforma de entrenamiento con un software usado en el mundo real que permita a las personas llegar a familiarizarse con los dispositivos Cisco, ya que esta empresa hoy en día es el líder en tecnologías de redes (4).

Este emulador no puede reemplazar un router real, es simplemente una herramienta complementaria para administradores de redes cisco. Dynagen es un *text-based*¹ *front-end*² para Dynamips, el cual usa el modo “*hypervisor*”³ para comunicarse con Dynamips, el cual inicializa el sistema operativo del router que se usará en la práctica. Usa un archivo de

¹ Text-based: Se refiere a aplicaciones de computadores basados primariamente en interfaces de texto.

² Front-end: Es un tipo de interfaz que es responsable de recolectar datos de entrada del usuario

³ Hypervisor: Es una tecnología que permite utilizar, al mismo tiempo, diferentes sistemas operativos.

configuración fácil de comprender para especificar configuración de routers virtuales. Dynagen también controla simultáneamente múltiples servidores Dynamips para distribuir varias redes virtuales en varias máquinas o en el mismo sistema (5).

Además Dynagen proporciona la consola real de un router es decir el CLI, *command line interface*⁴. Es por esta razón que sirve de entrenamiento para exámenes de certificación CCNA/CCNP/CCIE.

2.2 INSTALACIÓN

El software se encuentra disponible en la página de Dynagen ya que es de libre distribución, y ya viene compilado para eliminar la necesidad de instalar el entorno de programación Python⁵ en el cual fue escrito. Antes de proceder a su instalación, se necesita instalar el paquete WinPcap 4.0 o el más reciente, el cual se encuentra direccionado en la misma página de Dynagen por un link. WinPcap es una herramienta estándar para la capa de enlace de acceso de red en ambiente Windows. Permite a las aplicaciones capturar y transmitir paquetes de red. WinPcap es un controlador *-driver-* y librería que provee al sistema operativo acceso a la red en lenguaje de bajo nivel. (6).

Luego de la descarga e instalación de la librería WinPcap, se instala el paquete de instalación de Windows el cual provee el Dynamips/Dynagen.

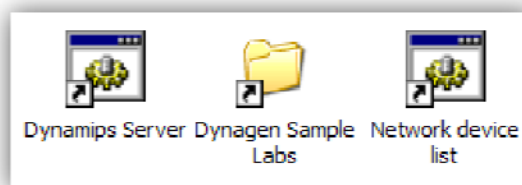


Figura 2.1 Íconos Dynagen del Escritorio

⁴ CLI: Command Line Interface: Línea de interface de comandos

⁵ Python: Es un lenguaje de programación de código abierto comparado habitualmente con TCL, Perl, Java entre otros

2.3 IMÁGENES DEL SISTEMA OPERATIVO IOS –Image Operative System-

Dynamips inicializa reales sistemas operativos de routers Cisco, Dynagen no distribuye ninguna de las Imágenes de sistema operativo, es por esta razón que para el presente proyecto se ha facilitado el IOS de Routers 3600 y 7200 para propósitos de estudio más no de distribución.

El archivo de imagen .bin del IOS debe ser colocado en la carpeta C:\Program Files\Dynamips\images, las imágenes Cisco trabajan bien en Dynamips, pero el proceso de inicialización es lento debido a que las imágenes deben ser descomprimidas, es recomendado que las imágenes sean descomprimidas para que el emulador no tenga que hacerlo. Esto podemos realizarlo con las utilidades de “Unzip” en Linux/Unix/Cygwin. Con la siguiente línea de comando (5).

```
unzip -p c7200-g6ik8s-mz.124-2.T1.bin > c7200-g6ik8s-mz.124-2.T1.image
```

Se recibirá una alerta de Unzip la cual puede ser ignorada convincentemente.

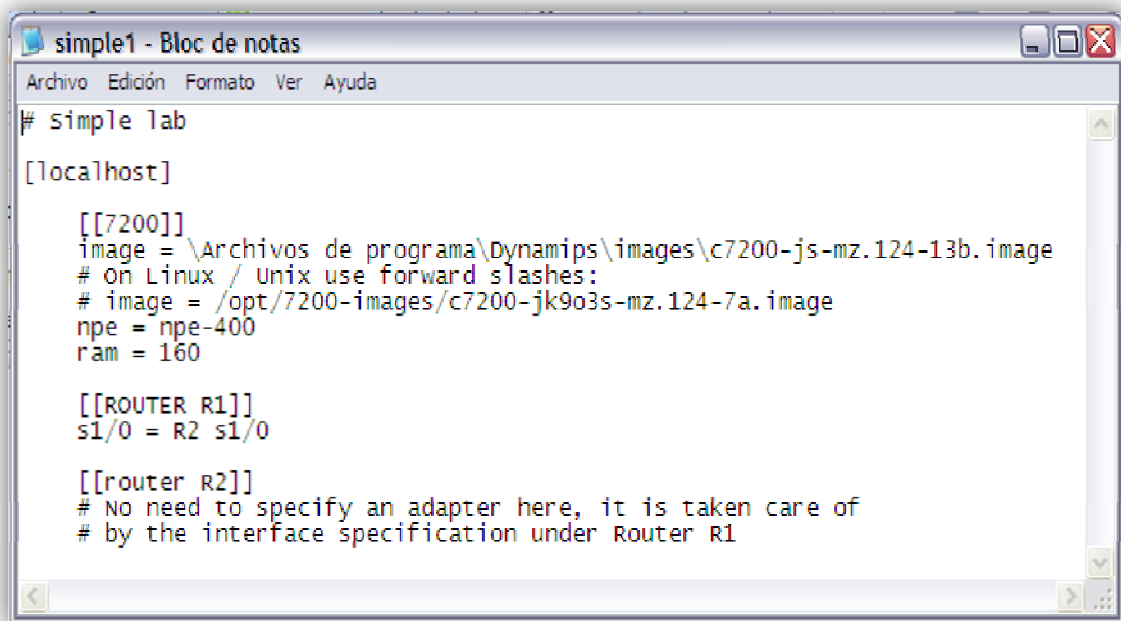
Dynamips usa gran cantidad de RAM del CPU para realizar la emulación, debido a que transforma el PC, en prácticamente un Router es decir un Cisco 7200 necesitará 256 MB en RAM, lo cual es lo que dedicará para las tareas en el router virtual.

2.4 CONFIGURACIÓN DE CLIENTE TELNET

Dynagen incluye una consola de comandos que permite conectarse a una consola virtual del router es decir se enlaza directamente con el CLI –*command line interface*- pero para hacer uso de este, primero se debe configurar el archivo dynagen.ini localizado C:\Program Files\Dynamips, en este archivo se puede realizar cambios de acuerdo a los comentarios que se encuentran en él. Pero realmente el programa funciona muy bien sin realizar dichos cambios.

2.5 ARCHIVOS DE RED

Dynagen usa un solo archivo para almacenar la configuración de todos los Routers, Switches e interconexiones que se realiza en los laboratorios virtuales. Este archivo usa una simple sintaxis, se lo puede abrir con un editor de texto, se encuentra en la carpeta C:\Archivos de programa\Dynamips\sample_labs., el cual posee varios laboratorios y se localiza en el escritorio, el cual se creó por un acceso directo, con la ubicación:

A screenshot of a Notepad window titled 'simple1 - Bloc de notas'. The window contains the following text:

```
# simple lab

[localhost]

[[7200]]
image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image
# On Linux / Unix use forward slashes:
# image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image
npe = npe-400
ram = 160

[[ROUTER R1]]
s1/0 = R2 s1/0

[[router R2]]
# No need to specify an adapter here, it is taken care of
# by the interface specification under Router R1
```

Figura 2.2 Archivo de Configuración Simple1.net

Al igual que en otros lenguajes de programación el # se usa para agregar comentarios.

Simple lab

La primera sección especifica el *host* que está corriendo Dynamips, en este caso ejecutaremos Dyanmips en la misma máquina que Dynagen, por esta razón especificamos el *localhost*. Si Dynamips se ejecutara en otro ordenador deberíamos colocar el hostname o la dirección IP en su lugar.

[localhost]

La siguiente sección especifica la configuración del servidor Dynamips, el doble corchete significa que la sección que viene a continuación esta anidada dentro del *[localhost]*.

[[7200]]

En esta sección se define la ubicación del *IOS* del router que usaremos

```
image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image
# On Linux / Unix use forward slashes:
# image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image
```

NOTA: El archivo IOS usado en las prácticas puede ser usado como se planteo anteriormente, es decir de manera comprimida. *-BIN-* o sin comprimir *-image-*, para ambos casos respectivamente use la siguientes líneas de comando dentro del archivo de red.

Para el router 7200:

Archivo Descomprimido:

```
image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image
```

Archivo Comprimido:

```
image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.BIN
```

Para el router 3620:

Archivo Descomprimido:

```
image = \Archivos de programa\Dynamips\images\c3620-is-mz.122-5.image
```

Archivo Comprimido:

```
image = \Archivos de programa\Dynamips\images\c3620-is-mz.122-5.BIN
```

En las siguientes líneas se especifica el tamaño de memoria RAM que se usa para un router 7200, *NPE-400*⁶.

```
npe = npe-400
```

```
ram = 160
```

A continuación se define el “ROUTER”. La cadena de caracteres que sigue luego, indica el nombre que asignamos al Router en este caso R1. Este nombre es solo usado por Dynamips/Dynagen, el cual no tiene nada que ver con el *hostname* que se asigna al IOS del Router.

```
[[ROUTER R1]]
```

La línea siguiente establece la conexión de la interface serial 1/0 con la interface serial 1/0 de un segundo Router “R2” vía cable serial, Dynagen automáticamente instala un adaptador PA-8T en el puerto 1 para acomodar la conexión en ambos Routers

```
s1/0 = R2 s1/0
```

Luego encontramos la creación de un segundo Router. Este es el mismo router al cual se refiere en la línea anterior, el cual conecta las interfaces seriales R1 con R2

```
[[router R2]]
```

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

```
# by the interface specification under Router R1
```

⁶ NPE: Network Processing Engine: Motor de Procesamiento de Redes. Mantiene y Ejecuta la administración del Sistema de un Router

2.6 EJECUCIÓN DE DYNAMIPS/DYNAGEN

Primero ejecutamos Dynamips Server el cual se encuentra en el *Desktop* escritorio de Windows. Luego ejecutamos el archivo simple1.net el cual inicializa la red creada en Dynagen.

```

Dynamips Server
Cisco Router Simulation Platform (version 0.2.7-x86)
Copyright (c) 2005-2007 Christophe Fillot.
Build date: May 29 2007 09:03:26

ILT: loaded table "mips64j" from cache.
ILT: loaded table "mips64e" from cache.
ILT: loaded table "ppc32j" from cache.
ILT: loaded table "ppc32e" from cache.
Hypervisor TCP control server started (port 7200).
Shutdown in progress...
Shutdown completed.
CPU0: carved JIT exec zone of 16 Mb into 512 pages of 32 Kb.
C7200 instance 'R1' (id 0):
  UM Status   : 0
  RAM size    : 160 Mb
  IOMEM size  : 0 Mb
  NURAM size  : 128 Kb
  NPE model   : npe-400
  Midplane    : vxr
  IOS image   : \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

Loading ELF file '\Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image'...
ELF entry point: 0x80008000

C7200 'R1': starting simulation (CPU0 PC=0xffffffffbfc00000), JIT enabled.
CPU0: carved JIT exec zone of 16 Mb into 512 pages of 32 Kb.
C7200 instance 'R2' (id 1):
  UM Status   : 0
  RAM size    : 160 Mb
  IOMEM size  : 0 Mb
  NURAM size  : 128 Kb
  NPE model   : npe-400
  Midplane    : vxr
  IOS image   : \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

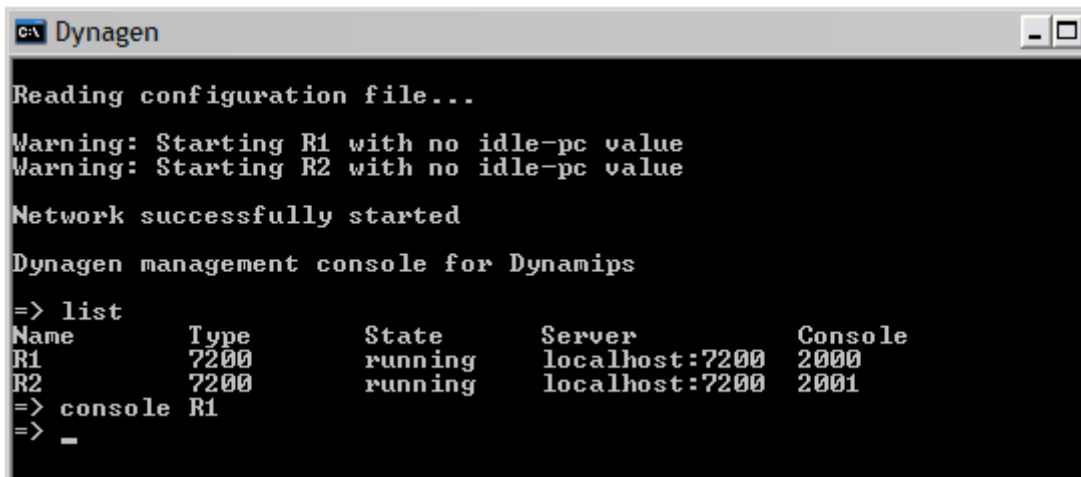
Loading ELF file '\Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image'...
ELF entry point: 0x80008000

C7200 'R2': starting simulation (CPU0 PC=0xffffffffbfc00000), JIT enabled.

```

Figura 2.3 Inicialización de Dynamips Server

Operando Dynagen en la **Figura 2.4** podemos listar los dispositivos en el laboratorio virtual con el comando *list*.



```

C:\> Dynagen

Reading configuration file...

Warning: Starting R1 with no idle-pc value
Warning: Starting R2 with no idle-pc value

Network successfully started

Dynagen management console for Dynamips

=> list
Name      Type      State      Server      Console
R1        7200      running    localhost:7200  2000
R2        7200      running    localhost:7200  2001
=> console R1
=> -

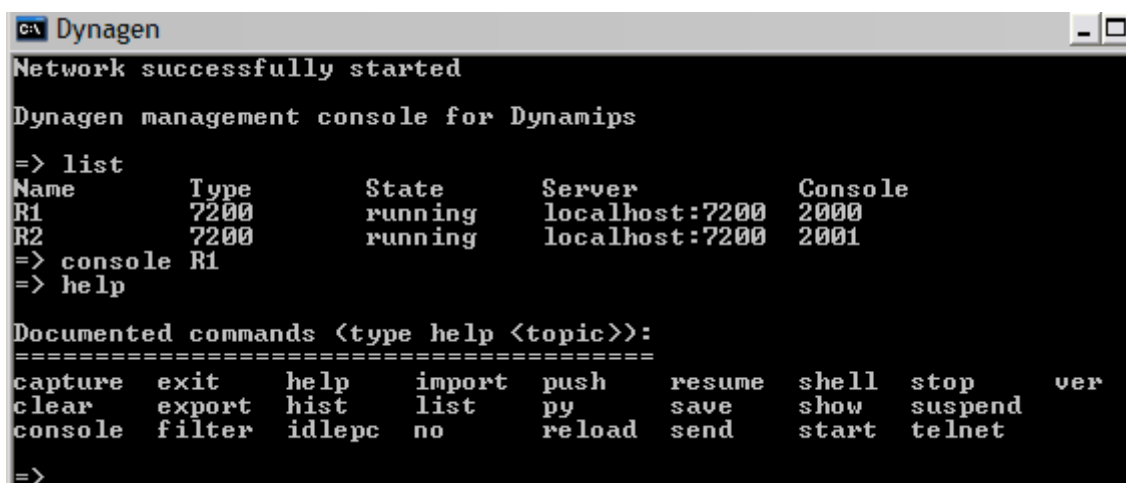
```

Figura 2.4 Dynagen Dispositivos de Red

Debido a la configuración realizada en el archivo `simple1.net`, los dispositivos R1 y R2 se encuentran disponibles, en las siguientes prácticas se usará diferentes topologías de red, con más dispositivos. La pantalla además indica que ambos Routers están ejecutándose en el *localhost* en el puerto de consola de TCP 2000 y 2001 respectivamente.

Se realiza un telnet al puerto para inicializar el router “*console R1*”, también podemos inicializar todos los dispositivos con el comando “*console/all*”.

El comando *help* lista todos los comandos válidos en Dynagen **Figura 2.5**.



```

C:\> Dynagen

Network successfully started

Dynagen management console for Dynamips

=> list
Name      Type      State      Server      Console
R1        7200      running    localhost:7200  2000
R2        7200      running    localhost:7200  2001
=> console R1
=> help

Documented commands (type help <topic>):
=====
capture  exit    help    import  push    resume  shell   stop    ver
clear    export hist    list    py      save    show    suspend
console  filter idlepc  no      reload  send    start   telnet

=> -

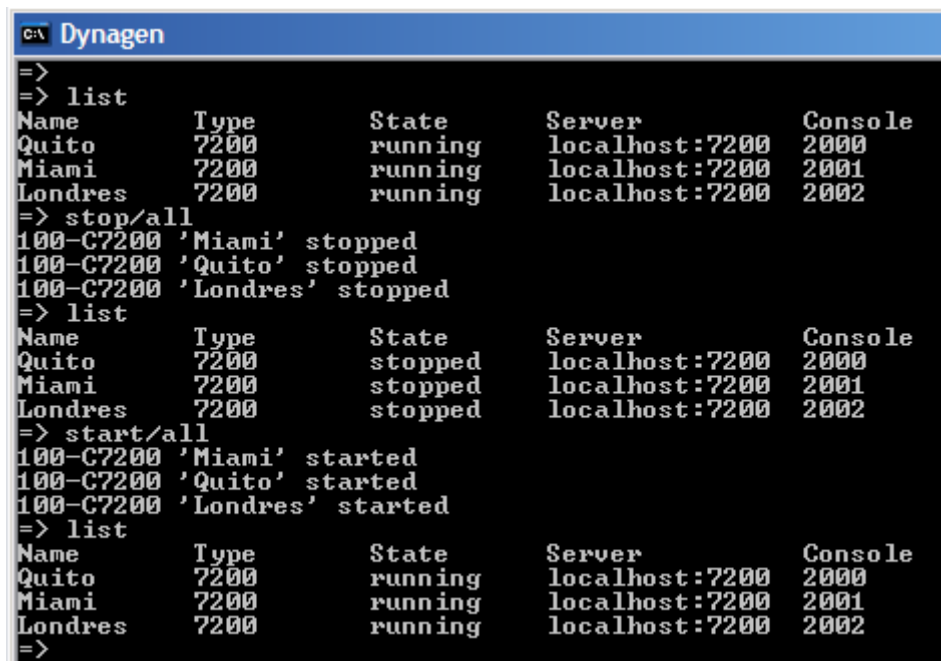
```

Figura 2.5 Comandos de Dynagen

Para obtener ayuda en particular de cualquier comando se usa el comando *help* “+*el comando*”.

Los siguientes comandos sirven para apagar o encender los Routers listados **Figura 2.6.** , en el siguiente listado de router hemos creado un router más y cambiamos sus nombres, esto se logra con el archivo de configuración del laboratorio, que se vio en la sección anterior.

```
stop {/all | router1 [router2] ...}
start {/all | router1 [router2]...}
```



```
C:\> Dynagen
=>
=> list
Name      Type      State      Server      Console
Quito     7200      running    localhost:7200  2000
Miami     7200      running    localhost:7200  2001
Londres   7200      running    localhost:7200  2002
=> stop/all
100-C7200 'Miami'  stopped
100-C7200 'Quito'  stopped
100-C7200 'Londres' stopped
=> list
Name      Type      State      Server      Console
Quito     7200      stopped    localhost:7200  2000
Miami     7200      stopped    localhost:7200  2001
Londres   7200      stopped    localhost:7200  2002
=> start/all
100-C7200 'Miami'  started
100-C7200 'Quito'  started
100-C7200 'Londres' started
=> list
Name      Type      State      Server      Console
Quito     7200      running    localhost:7200  2000
Miami     7200      running    localhost:7200  2001
Londres   7200      running    localhost:7200  2002
=>
```

Figura 2.6 Apagado y Encendido de Routers en Dynagen

2.7 CÁLCULO DE VALORES Idle⁷-PC

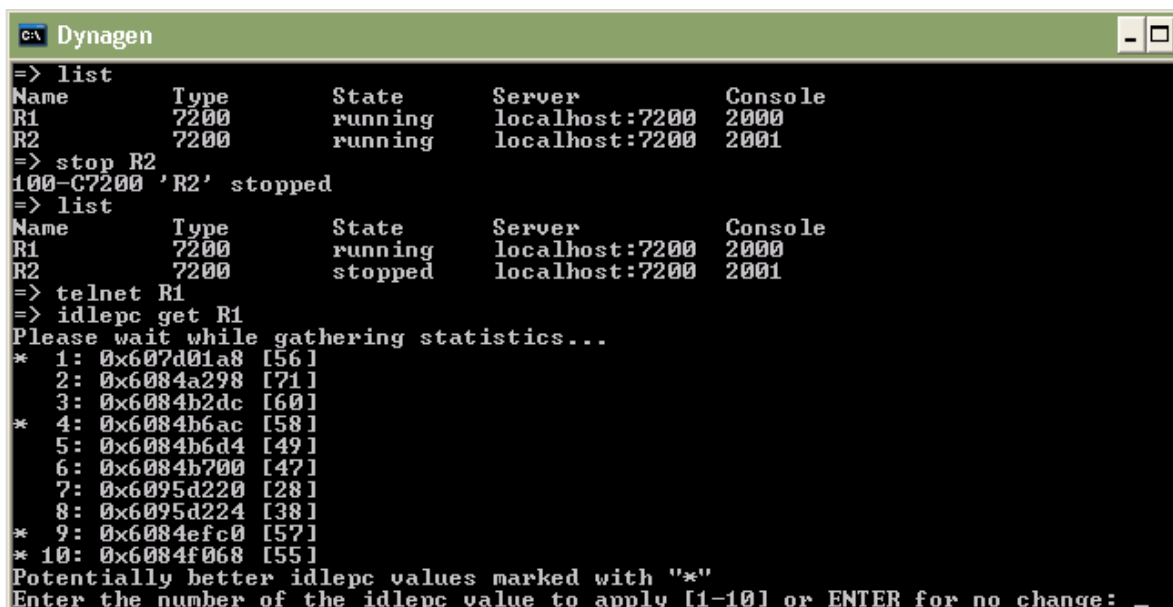
En el anterior laboratorio se habrá notado que el uso del CPU aumentó al 100% esto es debido a que Dynamips no reconoce cuando los Routers virtuales están o no en uso.

Es decir se encuentran inoperantes *-idle-* . El comando “idlepc” realiza un análisis de la imagen que se está usando, para pensar cuanta memoria debe disponer de la aplicación de esta manera disminuye el consumo del procesador.

⁷ Idle: Palabra en ingles que significa.- Inoperante

Para hacer que Dynagen reconozca la cantidad de memoria destinada, se realiza el siguiente procedimiento:

- Primero ejecutamos un laboratorio “simple1.net” y nos aseguramos que un solo router este corriendo, -parando los demás Routers si es necesario-
- Luego abrimos el router con el comando “*Console routername*” de esta forma se accede a la configuración del router.
- Después nos dirigimos a la ventana del Dynagen y usamos el comando “*idlepc get routername*”. Entonces aparecerá una lista con estadísticas, luego de pocos segundos la lista se completará y se deberá escoger una opción, la opción marcada con un “*” es la más idónea **Figura 2.7**.
- La utilización del procesador caerá entonces dramáticamente, esto significa que el procedimiento se lo realizó satisfactoriamente, para no realizar este proceso cada vez que inicia el programa, se usa el comando “*idlepc save routername*” el cual graba estos cambios en nuestro archivo de red⁸. **Figura 2.8 y Figura 2.9**.



```

C:\ Dynagen
=> list
Name      Type      State      Server      Console
R1        7200      running    localhost:7200  2000
R2        7200      running    localhost:7200  2001
=> stop R2
100-C7200 'R2' stopped
=> list
Name      Type      State      Server      Console
R1        7200      running    localhost:7200  2000
R2        7200      stopped    localhost:7200  2001
=> telnet R1
=> idlepc get R1
Please wait while gathering statistics...
* 1: 0x607d01a8 [56]
  2: 0x6084a298 [71]
  3: 0x6084b2dc [60]
* 4: 0x6084b6ac [58]
  5: 0x6084b6d4 [49]
  6: 0x6084b700 [47]
  7: 0x6095d220 [28]
  8: 0x6095d224 [38]
* 9: 0x6084efc0 [57]
* 10: 0x6084f068 [55]
Potentially better idlepc values marked with "*"
Enter the number of the idlepc value to apply [1-10] or ENTER for no change:

```

Figura 2.7 Comando Idlepc, Estadísticas del PC

⁸ NOTA: Los valores de IDLE estadísticos no siempre son los mismos, estos cambian dependiendo de la imagen IOS que se esté usando.

```

c:\ Dynagen
8: 0x6095d224 [38]
* 9: 0x6084efc0 [57]
* 10: 0x6084f068 [55]
Potentially better idlepc values marked with "*"
Enter the number of the idlepc value to apply [1-10] or ENTER for no change: 1
Applied idlepc value 0x607d01a8 to R1

=> idlepc show R1
* 1: 0x607d01a8 [56]
  2: 0x6084a298 [71]
  3: 0x6084b2dc [60]
* 4: 0x6084b6ac [58]
  5: 0x6084b6d4 [49]
  6: 0x6084b700 [47]
  7: 0x6095d220 [28]
  8: 0x6095d224 [38]
* 9: 0x6084efc0 [57]
* 10: 0x6084f068 [55]
Potentially better idlepc values marked with "*"
Enter the number of the idlepc value to apply [1-10] or ENTER for no change: 10
Applied idlepc value 0x6084f068 to R1

=> idlepc save R1 db
idlepc value for image "c7200-jk9o3s-mz.124-7a.image" written to the database
=>
    
```

Figura 2.8 Procedimiento para elección del valor de Idlepc

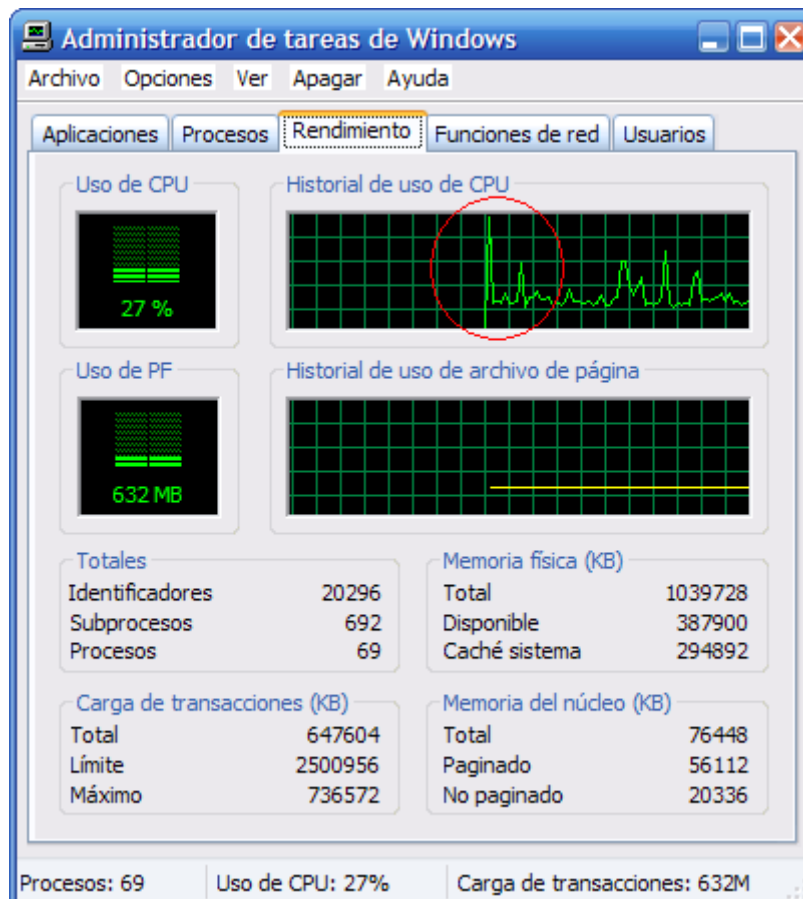


Figura 2.9 Caída del Uso del CPU

Es posible que Dynamips no encuentre un valor de idle-pc para una determinada imagen, o que el valor encontrado no trabaje apropiadamente, en este caso si ocurriese, repita el proceso hasta que aparezcan valores adecuados.

2.8 FRAME RELAY

Dynamips junto a Dynagen proveen soporte para switches integrados Frame-Relay. Si observamos en la carpeta de laboratorios de ejemplo -Sample_Labs -, encontraremos un ejercicio con conectividad hacia una nube Frame-Relay.

```
[[ROUTER R1]]
s1/0 = F1 1

[[ROUTER R2]]
s1/0 = F1 2

[[ROUTER R3]]
s1/0 = F1 3
```

Las interfaces seriales de los router son conectadas hacia los puertos 1,2, y 3, respectivamente de un switch Frame Relay.

```
[[FRSW F1]]
1:102 = 2:201
1:103 = 3:301
2:203 = 3:302
```

Con el siguiente comando FRSW se define el switch que se usa, el formato de cada conexión es el que sigue a continuación:

```
Port:dlci = port:dlci
```

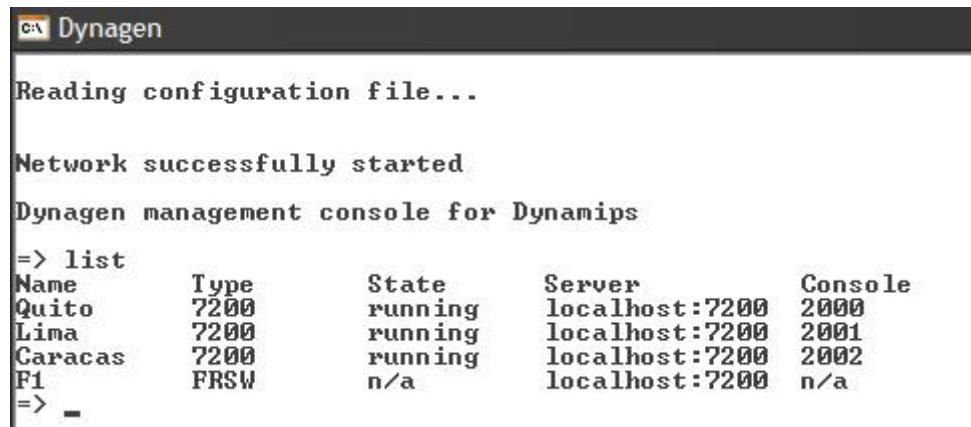
Esto quiere decir que el DLCI⁹ 102 en el puerto 1, está conectado virtualmente con el DLCI 201 del puerto 2 y así sucesivamente.

NOTA: Algo muy importante y que tendrá connotación en posteriores laboratorios, radica en que Dynamips emula un Frame-Relay switch con un LMI¹⁰ tipo ANSI, no

⁹ DLCI: Data Link Circuit Identifier: Identificador de circuitos de enlace de datos.

¹⁰ LMI: Local Management interface: Administrador Local de Interface

Cisco, es por esta razón que hay que especificarlo en la configuración de los Routers, si esto no se realiza no habrá conectividad.



```

C:\> Dynagen
Reading configuration file...

Network successfully started

Dynagen management console for Dynamips

=> list
Name      Type      State      Server      Console
Quito     7200      running    localhost:7200  2000
Lima      7200      running    localhost:7200  2001
Caracas   7200      running    localhost:7200  2002
F1        FRSW      n/a        localhost:7200  n/a
=> -

```

Figura 2.10 Consola de Administrador Dynagen Frame Relay Switch

2.9 CAPTURA DE PAQUETES.

Dynamips/Dynagen puede capturar paquetes de interfaces seriales virtuales o de ethernet, escribiendo su salida en un archivo de captura, el cual puede ser abierto en aplicaciones como Wireshark¹¹, o cualquier otra aplicación que pueda leer formatos de archivo libpcap¹².

Para capturar paquetes escribimos en la ventana de Dynagen el siguiente comando:

```
capture r1 f0/0 r1.cap
```

Este comando especifica que se archive los paquetes enviados o recibidos de la interfaz fastethernet “f0/0” del router “Quito” en un archivo “r1.cap”, el cual se guardará en la carpeta donde se encuentra el archivo de red que se usa en la práctica de Dynagen.

Para poder ver el tráfico de paquetes en tiempo real, se abre el archivo desde la aplicación Wireshark, Dynagen continuamente sigue escribiendo en el archivo de análisis de paquetes, es decir podemos recargar el archivo para seguir viendo los cambios que se

¹¹ Wireshark: Analizador de paquetes de Red

¹² Libpcap: librerías que permiten capturar y transmitir paquetes.

realizaron luego, en el ícono “reload this capture file” en la barra de herramientas de Wireshark.



Figura 2.11 Ícono de Recarga del archivo de captura

Para detener la captura de paquetes usamos el comando:

```
no capture r1 f0/0
```

Dynamips puede capturar paquetes en las interfaces seriales, solo tenemos que especificar el tipo de encapsulación que se está usando es decir, FR frame Relay, HDLC, PPP. En la **Figura 2.11** se ha analizado un paquete, en la fastethernet 0/0 de nuestro router Quito, el cual está usando un protocolo de enrutamiento RIP.

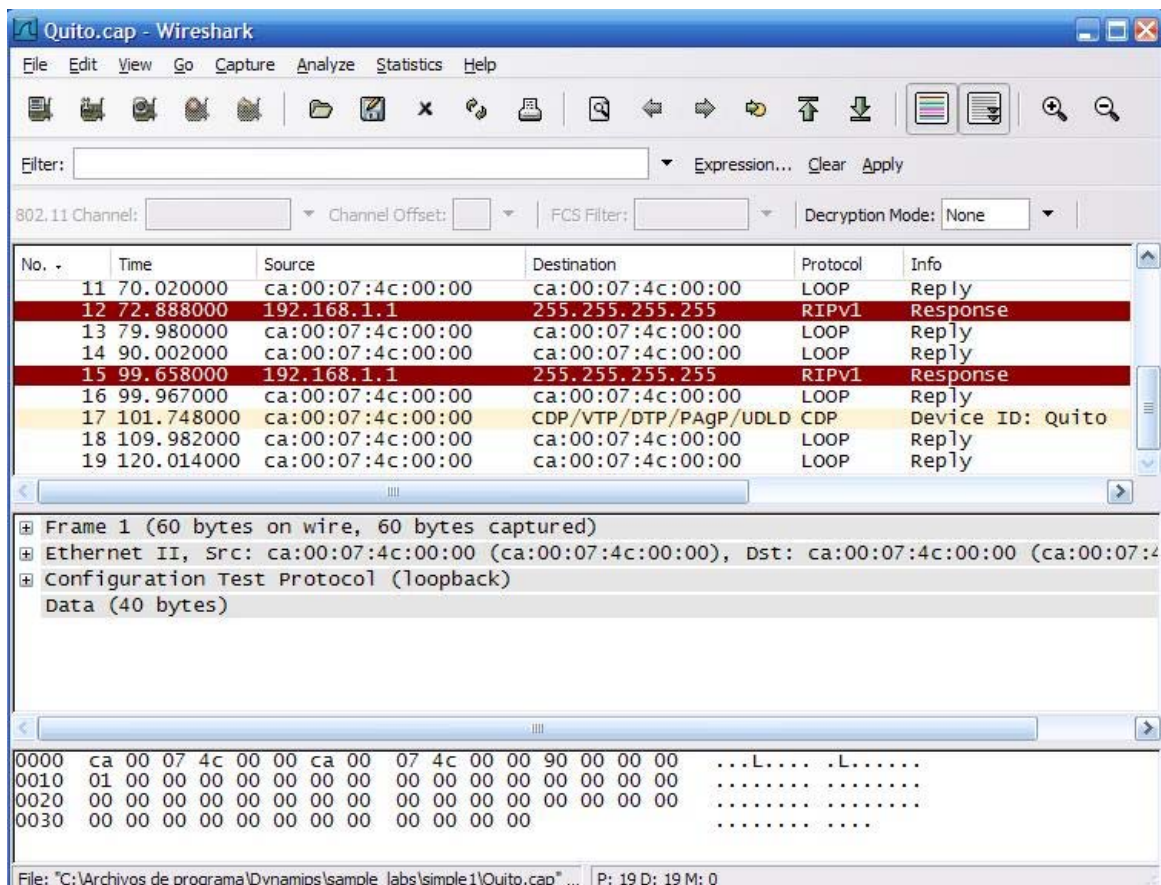


Figura 2.12 Analizador de Paquetes Wireshark

El capturador de paquetes nos permitirá poder ver el dialogo del protocolo, es decir el intercambio de paquetes que se realiza dependiendo del protocolo de enrutamiento implementado, es una herramienta muy poderosa para comprender mejor el funcionamiento de la comunicación entre routers. En la **Figura 2.12** ya podemos observar la difusión de broadcast con RIPv1, protocolo que analizaremos con más detenimiento.

CAPÍTULO 3

PRÁCTICAS DE PROTOCOLOS DE ENRUTAMIENTO

En este capítulo se detalla la configuración de protocolos de enrutamiento en cinco prácticas pasando por enrutamiento estático, enrutamientos dinámicos como, RIP, OSPF, EIGRP, y el protocolo de enrutamiento exterior BGP.

Después de revisar estos conceptos en el capítulo I, a continuación configuraremos los protocolos de enrutamiento interior y exterior. En cada práctica encontraremos base teórica para resolución de cada uno de los laboratorios.

Los esquemas de red usados en esta tesis son básicamente para efectos de entrenamiento, a continuación se presenta un esquema mas general de lo que usualmente se encuentra implementado en las redes mundiales.

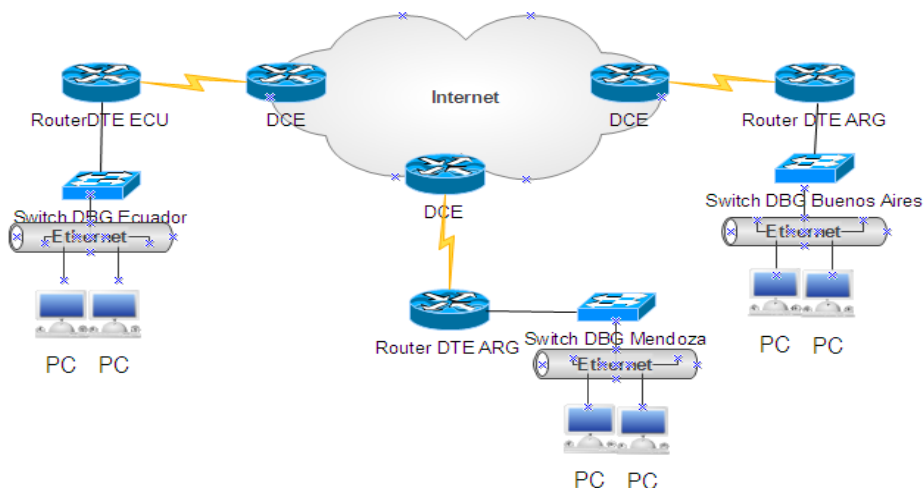


Figura Red de Área Extendida WAN

3.5 PRÁCTICA 1:

Tema: CONFIGURACIÓN DE RUTAS ESTÁTICAS

3.5.1 OBJETIVOS:

- ✓ Configurar el protocolo de enrutamiento estático.
- ✓ Configurar el protocolo de enrutamiento estático por defecto
- ✓ Analizar el intercambio de paquetes en una de sus interfaces
- ✓ Verificar el correcto funcionamiento de la red
- ✓ Detectar posibles fallas con los comandos de verificación.
- ✓ Reconocer las principales características del enrutamiento estático

3.5.2 MARCO TEÓRICO.

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

Rutas Estáticas. Utiliza una ruta programada que el administrador de la red introduce en el router.

Rutas Dinámicas. Utiliza una ruta que un protocolo de enrutamiento ajusta automáticamente ante los cambios de la red.

Para la configuración de rutas estáticas el administrador debe introducir el comando `ip route` seguido de la dirección a la red a la cual se quiere alcanzar junto a su máscara de red, y luego la dirección del siguiente salto –next hop- Ej:

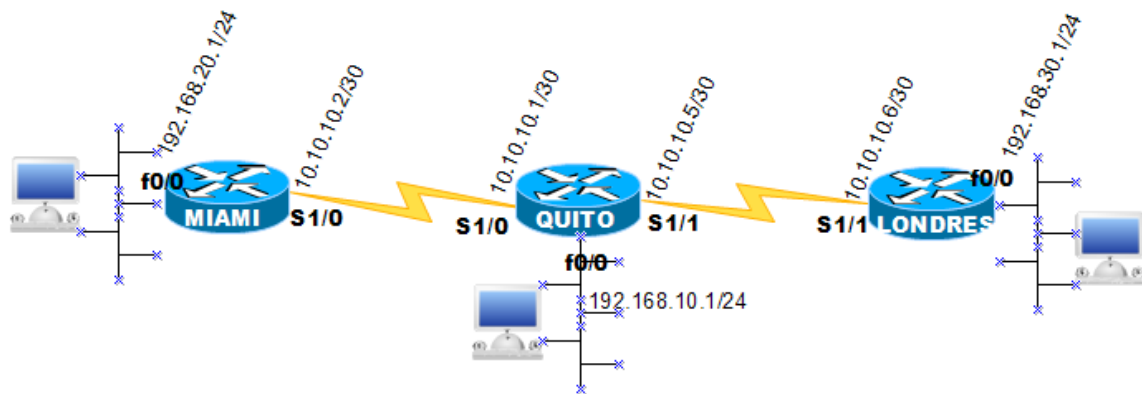


Figura 3.1 Ejemplo para uso de Enrutamiento Estático

Suponiendo que el administrador del router Quito necesita configurar las rutas estáticas para alcanzar las redes 192.168.20.0/24 y 192.168.30.0/24. El administrador debe ejecutar los siguientes comandos.

```

Quito(config)#ip route 192.168.20.0 255.255.255.0 10.10.10.2
                    comando red destino máscara de subred next hop –gateway-
Quito(config)#ip route 192.168.30.0 255.255.255.0 10.10.10.6
                    comando red destino máscara de subred next hop –gateway-

```

Configuración de Rutas Estáticas por defecto.

Las rutas por defecto se usan para enviar paquetes a destinos que no coinciden con los de ninguna de las otras rutas en la tabla de enrutamiento. Generalmente, los routers están configurados con una ruta por defecto para el tráfico que se dirige a la Internet, ya que a menudo resulta poco práctico e innecesario mantener rutas hacia todas las redes de la Internet. En realidad, una ruta por defecto es una ruta estática especial que utiliza este formato (2):

```
ip route 0.0.0.0 0.0.0.0 [ dirección-del-siguiente-salto | interfaz de salida]
```

Para la topología de la **Figura 3.1**, se aplicaría la siguiente configuración para que el router Londres aprenda la red que se encuentra en el router de Quito.

Londres(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.5

3.5.3 ESQUEMA DE LA RED

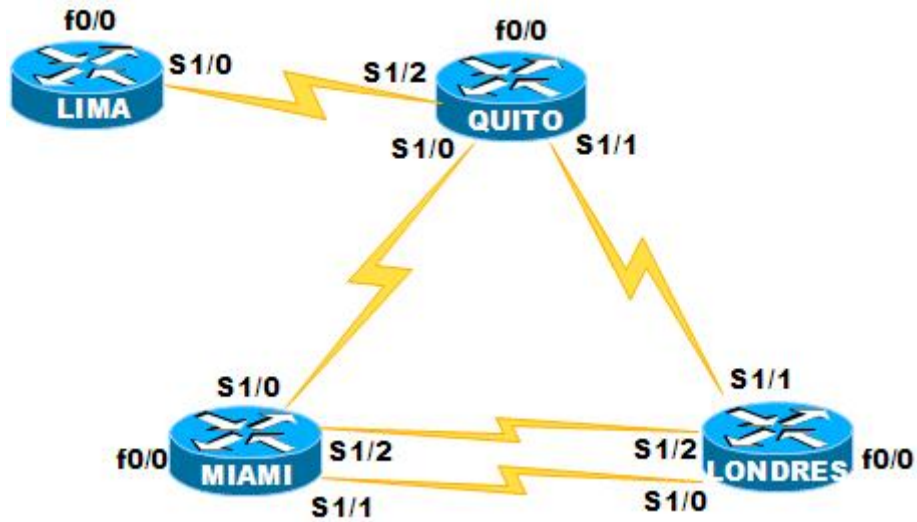


Figura 3.2 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface
Lima	DTE	10.10.10.13	255.255.255.252	S1/0
		192.168.40.1	255.255.255.0	f0/0
Quito	DCE	10.10.10.1	255.255.255.252	S1/0
		10.10.10.5	255.255.255.252	S1/1
		10.10.10.14	255.255.255.252	S1/2
Miami	DTE	192.168.10.1	255.255.255.0	f0/0
		10.10.10.2	255.255.255.252	S1/0
		10.10.10.10	255.255.255.252	S1/1
Londres	DCE	10.10.10.17	255.255.255.252	S1/2
		192.168.20.1	255.255.255.0	f0/0
		10.10.10.6	255.255.255.252	S1/1
Londres	DTE	10.10.10.9	255.255.255.252	S1/0
		10.10.10.18	255.255.255.252	S1/2
		192.168.30.1	255.255.255.0	f0/0

Tabla 3.1 Datos de la Red WAN

3.5.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

Se establece un nombre para el Router, luego la configuración de la clave de consola del Router, y clave de la terminal virtual, con lo cual se restringe el acceso al router, y el acceso remoto hacia este.

```
Router>enable
Router#configure terminal
Router(config)#hostname Quito
Quito(config)#line console 0
Quito(config-line)#password espe
Quito(config-line)#login
Quito(config-line)#exit
Quito(config)#line vty 0 4
Quito(config-line)#password espe
Quito(config-line)#login
Quito(config-line)#exit
Quito(config)#enable password espe
Quito(config)#exit
Quito#disable
Quito>enable
Password: espe
Quito#configure terminal
Quito(config)#enable secret electronica
Quito(config)#exit
Quito#disable
Quito>enable
Password: electrónica
```

Esta operación realizamos en cada uno de los Routers para identificarlo en la red. A continuación asignamos IP del enlace WAN y LAN. Fijando la velocidad de sincronización para el cable DCE, así controlamos la comunicación.

Quito#**configure terminal**

Quito(config)#**interface serial 1/0**

Quito(config-if)#**ip address 10.10.10.1 255.255.255.252**

Quito(config-if)#**clock rate 56000**

Quito(config-if)#**no shutdown**

Quito(config-if)#**exit**

Quito(config)#**interface serial 1/1**

Quito(config-if)#**ip address 10.10.10.5 255.255.255.252**

Quito(config-if)#**clock rate 56000**

Quito(config-if)#**no shutdown**

Quito(config-if)#**exit**

Quito(config)#**interface serial 1/2**

Quito(config-if)#**ip address 10.10.10.14 255.255.255.252**

Quito(config-if)#**clock rate 56000**

Quito(config-if)#**no shutdown**

Quito(config-if)#**exit**

Quito(config)#**interface fastethernet 0/0**

Quito(config-if)#**ip address 192.168.10.1 255.255.255.0**

Quito(config-if)#**no shutdown**

Quito(config if)#**exit**

Miami#**configure terminal**

Miami(config)#**interface serial 1/0**

Miami(config-if)#**ip address 10.10.10.2 255.255.255.252**

Miami(config-if)#**no shutdown**

Miami(config-if)#**exit**

Miami(config)#**interface serial 1/1**

Miami(config-if)#**ip address 10.10.10.10 255.255.255.252**

Miami(config-if)#**clock rate 56000**

Miami(config-if)#**no shutdown**

Miami(config-if)#**exit**

Miami(config)#**interface fastethernet 0/0**

Miami(config-if)#**ip address 192.168.20.1 255.255.255.0**

Miami(config-if)#**no shutdown**

Miami(config if)#**exit**

Londres#**configure terminal**

Londres(config)#**interface serial 1/1**

Londres(config-if)#**ip address 10.10.10.6 255.255.255.252**

Londres(config-if)#**no shutdown**

Londres(config-if)#**exit**

Londres(config)#**interface serial 1/0**

Londres(config-if)#**ip address 10.10.10.9 255.255.255.252**

Londres(config-if)#**no shutdown**

Londres(config-if)#**exit**

Londres(config)#**interface fastethernet 0/0**

Londres(config-if)#**ip address 192.168.30.1 255.255.255.0**

Londres(config-if)#**no shutdown**

Londres(config if)#**exit**

Lima#**configure terminal**

Lima(config)#**interface serial 1/0**

Lima(config-if)#**ip address 10.10.10.13 255.255.255.252**

Lima(config-if)#**no shutdown**

Lima(config-if)#**exit**

Lima(config-if)#**exit**

Lima(config)#**interface fastethernet 0/0**

Lima(config-if)#**ip address 192.168.40.1 255.255.255.0**

Lima(config-if)#**no shutdown**

Lima(config if)#**exit**

NOTA: La configuración de claves de consola, nombres y direcciones, se realizarán sólo en esta práctica, debido a que es un procedimiento general para el acceso de las redes, a partir de la siguiente práctica se entiende que este procedimiento ya fue realizado dependiendo del esquema de la red

Luego de la asignación de direcciones, se configura las rutas estáticas, las cuales deberán enlazar toda la red del esquema, es decir todas las redes tendrán conexión.

Quito#**config ter**

Quito(config)#**ip route 192.168.30.0 255.255.255.0 10.10.10.6**

Quito(config)#**ip route 192.168.20.0 255.255.255.0 10.10.10.2**

Miami#**config ter**

Miami(config)#**ip route 192.168.10.0 255.255.255.0 10.10.10.1**

Miami(config)#**ip route 192.168.30.0 255.255.255.0 10.10.10.9**

Miami(config)#**ip route 192.168.30.0 255.255.255.0 10.10.10.18**

Londres#**config ter**

Londres(config)#**ip route 192.168.10.0 255.255.255.0 10.10.10.5**

Londres(config)#**ip route 192.168.20.0 255.255.255.0 10.10.10.17**

Londres(config)#**ip route 192.168.20.0 255.255.255.0 10.10.10.10**

A continuación configuramos al router Lima para que reconozca cualquier ruta que no esté conectada directamente en el router Quito, es decir aplicamos la ruta por defecto hacia este.

Lima#**config ter**

Lima(config)#**ip route 0.0.0.0 0.0.0.0 10.10.10.14**

3.5.5 VERIFICACIÓN DE CONFIGURACIÓN

Luego de la configuración existen ciertos comandos que se deben usar para verificar que la red este funcionando plenamente. Se realiza un ping a todas las redes que se desea alcanzar fijándose en la tasa de porcentaje de alcance mostrado en la **Figura 3.3**

```

Telnet localhost
Quito#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
Quito#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/61/128 ms
Quito#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/85/160 ms
Quito#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Quito#

```

Figura 3.3 Prueba de Conectividad Ping

En la **Figura 3.3** se realiza un ping desde el router Quito la señalización roja indica la conectividad con la red del Router Miami debido a que se asignó una ruta estática hacia esta red, en el caso contrario un ping hacia la red Lima –señalización verde- indica que no existe conectividad esto es debido a que no se asignó una ruta estática. Las rutas estáticas y protocolos de enrutamiento configurados en un router son posibles ver con los comandos **show run** y **show ip route**, estos comandos usados en el modo de configuración de terminal nos indican la configuración activa es decir interfaces y configuración de rutas y protocolos para el primero, y las tablas de enrutamiento para el segundo comando, a continuación en la **Figura 3.4** se presenta la visualización de los comandos desde el router Miami.

```

Miami#show run
Building configuration...

Current configuration : 1378 bytes
?
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
?
hostname Miami
?
boot-start-marker
boot-end-marker
?
enable secret 5 $1$n5s/$43HvZet10U036UIZ1xJWU1
enable password espe
?

```

Figura 3.4 Comprobación de configuración comando Show Run

En esta primera parte el comando despliega el nombre del Host y las claves asignadas, para protección del router.

```
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex half
?
interface Serial1/0
 ip address 10.10.10.2 255.255.255.252
 serial restart-delay 0
?
interface Serial1/1
 ip address 10.10.10.10 255.255.255.252
 serial restart-delay 0
 clock rate 56000
?
interface Serial1/2
 ip address 10.10.10.17 255.255.255.252
 serial restart-delay 0
 clock rate 56000
?
```

Figura 3.5 Comprobación de configuración comando Show Run

Luego encontramos todas las interfaces que posee un router cisco 7200 en este caso el router tiene siete interfaces seriales y una interfaz fastethernet, este comando nos indica el número ip asignado a cada interfaz con su respectivo reloj si este se encuentra activo, indicando si el cable es DCE. En el router Miami el cual se cita en el ejemplo posee una interfaz fastethernet y tres enlaces WAN –seriales- un camino redundante hacia el router Londres **Figura 3.5**.

A continuación aparece las rutas estáticas asignadas en este caso dos rutas estáticas asignadas hacia el router Londres desde Miami como medida de seguridad esto es muy usual en ciertos enlaces en los cuales no se puede dar el lujo de perder conectividad **Figura 3.6**.

```
ip route 192.168.10.0 255.255.255.0 10.10.10.1
ip route 192.168.30.0 255.255.255.0 10.10.10.9
ip route 192.168.30.0 255.255.255.0 10.10.10.18
?
```

Figura 3.6 Comprobación de configuración comando Show Run

```
line con 0
 password espe
 login
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password espe
 login
?
```

Figura 3.7 Comprobación de configuración comando Show Run

Las siguientes líneas que muestra el comando indica las claves asignadas para la consola y para accesos virtuales es decir la activación del router vía remota, el cual se complementa con las claves secretas encriptadas como medio de seguridad configurado por el administrador.

El comando **show ip route** nos ayuda a desplegar las tablas de enrutamiento esta nos indican todas las redes conectadas hacia el router directa o indirectamente, también presenta el tipo de protocolo configurado en cada interfaz sea este rutas estáticas, RIP, IGRP, EIGRP entre otros también despliega la distancia administrativa y la métrica, **Figura 3.8.**

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

Gateway of last resort is not set

S    192.168.30.0/24 [1/0] via 10.10.10.18
      [1/0] via 10.10.10.9
S    192.168.10.0/24 [1/0] via 10.10.10.1
C    192.168.20.0/24 is directly connected, FastEthernet0/0
      10.0.0.0/30 is subnetted, 3 subnets
C      10.10.10.8 is directly connected, Serial1/1
C      10.10.10.0 is directly connected, Serial1/0
C      10.10.10.16 is directly connected, Serial1/2
Miami#_
```

Figura 3.8 Comprobación de configuración comando Show Ip Route

En el cuadro verde se encuentran las dos vías por donde podría alcanzar la red 192.168.30.0, esto es debido a las rutas estáticas ingresadas en el Router Miami, el cuadro rojo indica la *distancia administrativa* el cual es un método de medida usado por los protocolos de enrutamiento IP, los valores menores son preferidos, junto a este valor se encuentra la métrica que es una medida para escoger la mejor ruta, este valor es una composición del número de saltos, costo (*ancho de banda*), y otros factores, siempre se escogen valores menores, en estos dos indicadores.

3.5.5.1 Verificación de Paquetes

Con el capturador de Paquetes Wireshark podemos observar el intercambio de paquetes entre Routers, en la práctica usaremos la interfaz del router Miami s1/0

Desde la consola de comandos Dynagen, capturamos los paquetes desde la interface s1/0 del router Miami para observar cual camino toma el paquete desde Londres hacia la red 192.168.10.0.

=> **capture Miami s1/0 miami.cap HDLC**

A continuación, abrimos el archivo Miami.cap este nos ayuda a analizar la manera por la cual se comunican estos dispositivos, ya en las siguientes prácticas se usarán protocolos de enrutamiento dinámico, con los cuales se pueden analizar de mejor manera los paquetes de diálogo para notificación de rutas.

Time	Source	Destination	Protocol	Device ID: Quito	Port
140.468000	N/A	N/A	CDP		
141.301000	10.10.10.2	192.168.10.1	ICMP	Echo (ping) request	
141.370000	192.168.10.1	10.10.10.2	ICMP	Echo (ping) reply	
141.441000	10.10.10.2	192.168.10.1	ICMP	Echo (ping) request	
141.481000	192.168.10.1	10.10.10.2	ICMP	Echo (ping) reply	
141.498000	10.10.10.2	192.168.10.1	ICMP	Echo (ping) request	
141.513000	192.168.10.1	10.10.10.2	ICMP	Echo (ping) reply	
141.519000	10.10.10.2	192.168.10.1	ICMP	Echo (ping) request	
141.535000	192.168.10.1	10.10.10.2	ICMP	Echo (ping) reply	
141.541000	10.10.10.2	192.168.10.1	ICMP	Echo (ping) request	
141.590000	192.168.10.1	10.10.10.2	ICMP	Echo (ping) reply	

Figura 3.9 Verificación de Paquetes

En la **Figura 3.9** podemos ver el proceso del comando Ping desde el router Miami hacia la red 192.168.10.1 del router Quito, cada columna indica de forma respectiva el intervalo de tiempo, la dirección origen, la dirección destino, el protocolo en este caso CDP e ICMP y su información.

Resumen de comandos usados en la práctica:

Comando	Descripción
show interface	Presenta la configuración de cada interface
show ip route	Presenta la tabla de enrutamiento
show run	Presenta la configuración actual del router
ping	Prueba de conectividad para capa de enlace
ip route	Establece una ruta estática o por defecto

Tabla 3.2 Lista de Comandos

3.6 PRÁCTICA 2

Tema: CONFIGURACIÓN DE RIP -ROUTING INFORMATION PROTOCOL-

3.6.1 OBJETIVOS:

- ✓ Establecer un ancho de banda menor para la interface serial 1\2 en el router Miami.
- ✓ Configurar el protocolo de enrutamiento dinámico RIP en la topología.
- ✓ Verificar que el protocolo este en correcto funcionamiento
- ✓ Detectar posibles fallas con los comandos de verificación.
- ✓ Reconocer las principales características de RIP y su comportamiento con rutas de diferente ancho de banda

3.6.1 MARCO TEÓRICO.

El Protocolo de información de enrutamiento (RIP) fue descrito originalmente en el RFC 1058. Sus características principales son las siguientes:

- ✓ Es un protocolo de enrutamiento por *vector-distancia*.
- ✓ Utiliza el *número de saltos como métrica* para la selección de rutas.
- ✓ Si el número de saltos es superior a 15, el paquete es desechado.
- ✓ Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

Para configurar RIP en el siguiente ejemplo se aplican los siguientes comandos para las redes conectadas directamente en cada router:

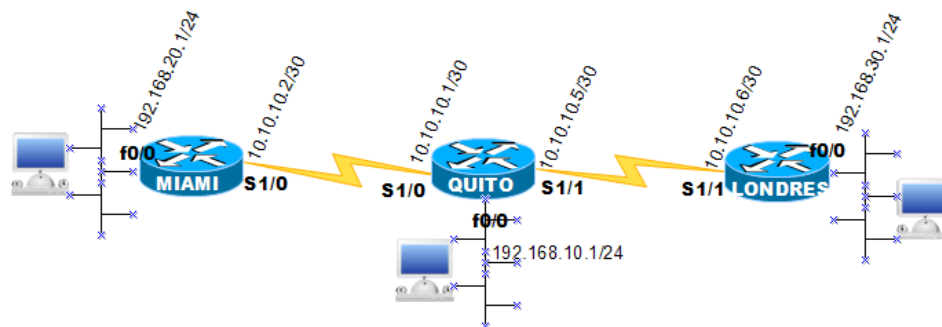


Figura 3.10 Ejemplo RIP Diagrama de Red

Si se desea que toda la red converja, cada router debe informar a los demás que sus interfaces están configuradas con un protocolo de enrutamiento en este caso RIP, a continuación se encuentra la configuración de la red de la **Figura 3.10**

```
Miami(config)#router rip
```

```
Miami(config-router)#network 10.10.10.0
```

```
Miami(config-router)#network 192.168.20.0
```

```
Quito(config)#router rip
```

```
Quito(config-router)#network 10.10.10.0
```

```
Quito(config-router)#network 10.10.10.4
```

```
Quito(config-router)#network 192.168.10.0
```

```
Londres(config)#router rip
```

```
Londres(config-router)#network 10.10.10.4
```

```
Londres(config-router)#network 192.168.30.0
```

Nota: *RIP al igual que IGRP es un protocolo de enrutamiento Classful es decir que, en sus actualizaciones no se incluyen las máscaras de subred de sus vecinos. Como resultado la información de cada subred es resumida –sumarizada- en una red mayor.*

RIP es usualmente configurado en redes TCP/IP pequeñas y medianas, usa el *hop count*¹ como métrica, RIP no considera el ancho de banda para decidir qué camino es el mejor.

Distancia Administrativa

En la práctica anterior ya se habló un poco de la distancia administrativa, el cual es un mecanismo para escoger la mejor ruta de entre múltiples caminos que se podrían dar en una topología. El valor de la distancia administrativa por defecto ha sido asignado con una

¹ Hop Count: Numero de Saltos usado en Routers como métrica, esta numeración tiene un número máximo antes de desechar el paquete

preferencia por las entradas manuales sobre las automáticas, y los protocolos de enrutamiento con métricas sofisticadas sobre protocolos de enrutamiento con métricas simples. Una comparación de las distancias administrativas se citan en la siguiente tabla.

Enrutamiento	Distancia administrativa por defecto
Interface Conectada	0
Ruta Estatica	0
Ruta Estatica al siguiente salto	1
EIGRP ruta sumaria	5
BGP Externo	20
EIGRP Interno	90
IGRP	100
OSPF	110
RIP (v1 y v2)	120
EGP	140
EIGRP Externo	170
BGP Interno	200
Desconocido (Unkonown)	255

Tabla 3.3 Valores de Distancia Administrativas

3.6.3 ESQUEMA DE LA RED

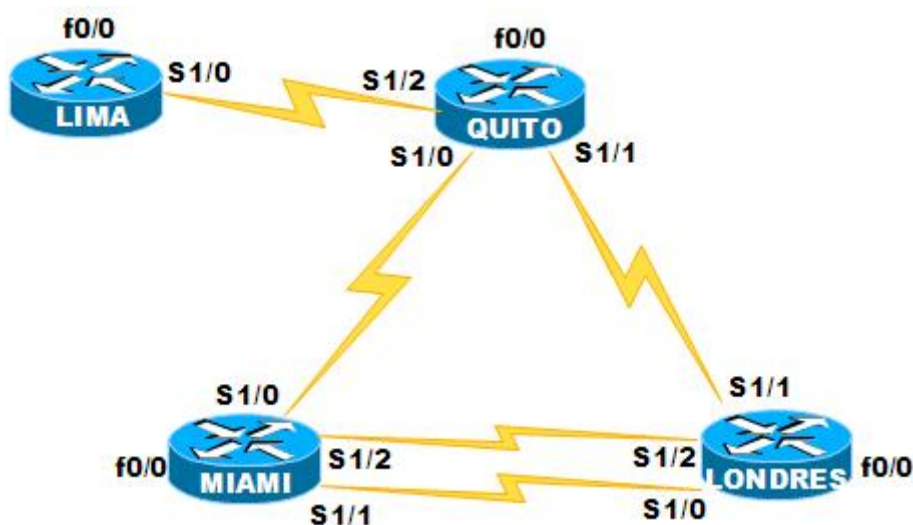


Figura 3.11 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface
Lima	DTE	10.10.10.13	255.255.255.252	S1/0
		192.168.40.1	255.255.255.0	f0/0
Quito	DCE	10.10.10.1	255.255.255.252	S1/0
	DCE	10.10.10.5	255.255.255.252	S1/1
	DCE	10.10.10.14	255.255.255.252	S1/2
		192.168.10.1	255.255.255.0	f0/0
Miami	DTE	10.10.10.2	255.255.255.252	S1/0
	DCE	10.10.10.10	255.255.255.252	S1/1
	DCE	10.10.10.17	255.255.255.252	S1/2
		192.168.20.1	255.255.255.0	f0/0
Londres	DTE	10.10.10.6	255.255.255.252	S1/1
	DTE	10.10.10.9	255.255.255.252	S1/0
	DTE	10.10.10.18	255.255.255.252	S1/2
		192.168.30.1	255.255.255.0	f0/0

Tabla 3.4 Datos de la Red WAN RIP

3.6.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

Configuración del protocolo de enrutamiento RIP, se aplica el protocolo en cada dirección de red IP a las cuales se requiere tener conexión. Debido a que RIP usa sumarización a la red classful, asumirá el protocolo en todas las subredes sin tomar en cuenta su máscara de subred. Es decir sería suficiente con establecer el protocolo para la red 10.0.0.0 ya que acogería todas las subredes pertenecientes, en la configuración siguiente se realiza la inclusión de cada red classles.

Quito#router rip

Quito(config-router)#**network 192.168.10.0**

Quito(config-router)#**network 10.10.10.0**

Quito(config-router)#**network 10.10.10.4**

Quito(config-router)#**network 10.10.10.12**

Quito(config-router)#**exit**

Miami#router rip

Miami(config-router)#**network 192.168.20.0**

Miami(config-router)#**network 10.10.10.0**

Miami(config-router)#**network 10.10.10.8**

```
Miami(config-router)#network 10.10.10.16
```

```
Miami(config-router)#exit
```

```
Londres#router rip
```

```
Londres(config-router)#network 192.168.30.0
```

```
Londres(config-router)#network 10.10.10.4
```

```
Londres(config-router)#network 10.10.10.8
```

```
Londres(config-router)#network 10.10.10.16
```

```
Londres(config-router)#exit
```

```
Lima#router rip
```

```
Lima(config-router)#network 192.168.40.0
```

```
Lima(config-router)#network 10.10.10.12
```

```
Lima(config-router)#exit
```

Para establecer un valor de ancho de banda *bandwidth*, se usa el comando *bandwidth* en el modo de configuración de interface, seguido luego por el valor en kilobits. En este caso la interface usa 1544Kbits que es un T1, la norma usual en USA. A continuación reduciremos a la mitad este ancho de banda para ver su comportamiento.

```
Miami# interface serial 1/2
```

```
Miami(config-if)#bandwidth 772
```

```
Miami(config-if)#exit
```

3.6.5 VERIFICACIÓN DE CONFIGURACIÓN –RIP-

Además de realizar una comprobación de capa de enlace de datos, en esta práctica estableceremos una sesión telnet la cual trabaja hasta capa de aplicación del modelo OSI. De esta forma podemos acceder de un router a otro cuando la red converge; y así, es más fácil detectar fallas. **Figura 3.12.** y **Figura 3.13**

```
Quito#ping 10.10.10.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.13, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/110/196 ms
Quito#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/96/144 ms
Quito#ping 10.10.10.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/74/156 ms
Quito#ping 10.10.10.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.9, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/99/268 ms
```

Figura 3.12 Prueba de conectividad capa dos OSI

```
Quito#telnet 10.10.10.6
Trying 10.10.10.6 ... Open

User Access Verification

Password:
Londres>
Londres>enable
Password:
Londres#
```

Figura 3.13 Prueba de conectividad capa siete OSI comando Telnet

El comando **show ip protocols** muestra cuáles son los protocolos que transportan tráfico IP en el router. Este resultado puede utilizarse para verificar la mayor parte, si no toda, la configuración del protocolo RIP.

Algunos de los aspectos de la configuración más comunes que deben ser verificados son, el tipo de protocolo de enrutamiento, las interfaces activas con el envío y recepción de paquetes, y si el router publica las redes correctas(2)

```

Londres>
Londres>enable
Password:
Londres#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 27 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 1, receive any version
  Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0    1     1 2
  Serial1/0          1     1 2
  Serial1/1          1     1 2
  Serial1/2          1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.30.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.10.10     120          00:00:20
    10.10.10.5      120          00:00:11
    10.10.10.17     120          00:00:24
  Distance: <default is 120>
Londres#_

```

Figura 3.14 Prueba de conectividad capa dos OSI

En la **Figura 3.14** se visualiza los protocolos que se están usando en el router Londres, el cual es RIP, con este comando se despliega una gran cantidad de información: como el tiempo de actualización de las tablas de enrutamiento, la distancia administrativa, las interfaces, y el resumen *-sumarization-* a redes classful activas en el protocolo.

Otro aspecto importante que se debe tomar en cuenta es que RIP no diferencia la mejor ruta en base al ancho de banda, si no simplemente establece como métrica el conteo de saltos *hop count* por esta razón, si se usa una interface de fibra óptica FDDI, la cual es vertiginosamente más rápido versus un cable serial, RIP coloca a los dos caminos como iguales.

Con el comando *show interface* podemos observar las características de cada interface, en la **Figura 3.15** y **Figura 3.16**, se puede realizar una comparación de ancho de banda. Y claramente observar el desbalance, es decir el camino más corto y rápido sería la interfaz serial 1/1 ya que esta posee un ancho de banda más grande.

```

Serial1/1 is up, line protocol is up
Hardware is M81-X.21
Internet address is 10.10.10.10/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:06, output 00:00:09, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 37 packets input, 3384 bytes, 0 no buffer
Received 37 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
44 packets output, 4462 bytes, 0 underruns
 0 output errors, 0 collisions, 2 interface resets
 0 output buffer failures, 0 output buffers swapped out
3 carrier transitions      DCD=up DSR=up DTR=up RTS=up CTS=up

```

Figura 3.15 Prueba de conectividad comando Show interface –RIP-

```

Serial1/2 is up, line protocol is up
Hardware is M81-X.21
Internet address is 10.10.10.17/30
MTU 1500 bytes, BW 772 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:01, output 00:00:04, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 579 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 43 packets input, 3908 bytes, 0 no buffer
Received 43 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
47 packets output, 4666 bytes, 0 underruns
 0 output errors, 0 collisions, 2 interface resets
 0 output buffer failures, 0 output buffers swapped out
3 carrier transitions      DCD=up DSR=up DTR=up RTS=up CTS=up

```

Figura 3.16 Prueba de conectividad comando Show interface -RIP-

Usando el comando *show ip route*, podemos ver los caminos que usaría el Router Miami para llegar a la red 192.168.30.0 –recuadro verde- en este caso existen tres caminos: uno por la interfaz del router Quito 10.10.10.1 y los otros por las interfaces 10.10.10.18 y 10.10.10.9, así RIP no diferencia el ancho de banda, como otros protocolos que veremos en siguientes prácticas


```

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

Gateway of last resort is not set

R    192.168.30.0/24 [120/1] via 10.10.10.18, 00:00:25, Serial1/2
      [120/1] via 10.10.10.9, 00:00:19, Serial1/1
      [120/1] via 10.10.10.1, 00:00:01, Serial1/0
R    192.168.10.0/24 [120/1] via 10.10.10.1, 00:00:01, Serial1/0
R    192.168.40.0/24 [120/1] via 10.10.10.1, 00:00:01, Serial1/0
C    192.168.20.0/24 is directly connected, FastEthernet0/0
      10.0.0.0/30 is subnetted, 5 subnets
C      10.10.10.8 is directly connected, Serial1/1
R      10.10.10.12 [120/1] via 10.10.10.1, 00:00:01, Serial1/0
C      10.10.10.0 is directly connected, Serial1/0
R      10.10.10.4 [120/1] via 10.10.10.18, 00:00:26, Serial1/2
      [120/1] via 10.10.10.9, 00:00:19, Serial1/1
      [120/1] via 10.10.10.1, 00:00:01, Serial1/0
C      10.10.10.16 is directly connected, Serial1/2

```

Figura 3.17 Prueba de conectividad comando Show ip route –RIP-

En la **Figura 3.18**, el administrador se traslado al router Lima, haciendo uso de telnet para realizar pruebas con el comando show ip route, los círculos indican la distancia administrativa y la métrica para alcanzar las redes 10.10.10.8 y 10.10.10.16, aquí se comprueba que la métrica es simplemente el número de saltos hacia la red.

```

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

Gateway of last resort is not set

R    192.168.30.0/24 [120/1] via 10.10.10.14, 00:00:24, Serial1/0
R    192.168.10.0/24 [120/1] via 10.10.10.14, 00:00:25, Serial1/0
C    192.168.40.0/24 is directly connected, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 10.10.10.14, 00:00:25, Serial1/0
      10.0.0.0/30 is subnetted, 5 subnets
R      10.10.10.8 [120/2] via 10.10.10.14, 00:00:25, Serial1/0
C      10.10.10.12 is directly connected, Serial1/0
R      10.10.10.0 [120/1] via 10.10.10.14, 00:00:25, Serial1/0
R      10.10.10.4 [120/1] via 10.10.10.14, 00:00:25, Serial1/0
R      10.10.10.16 [120/2] via 10.10.10.14, 00:00:25, Serial1/0
Lima#_

```

Figura 3.18 Prueba de conectividad comando Show ip route –RIP-

NOTA: Para esta práctica se usó la implementación de RIP v1, el cual no envía la máscara de subred en sus actualización de enrutamiento. Sí se usa un criterio de subneteo variable, la versión más reciente de RIP es decir la versión 2, soporta el envío de la máscara de subred esto aclara el reconocimiento de redes específicas que usan VLSM. El

cambio a RIPv2 es bastante sencillo simplemente se aumenta el siguiente comando en la configuración del router.

```
Quito#config ter  
Quito(config)#router rip  
Quito(config-router)#version 2  
Quito(config-router)#end
```

El objetivo del documento no contempla el estudio de VLSM, pero se recuerda que VLSM se utiliza para crear esquemas de direccionamiento eficientes y escalables debido al crecimiento físico de las redes. En todas las prácticas se hace uso de este direccionamiento IP con la meta de no desperdiciar direcciones en enlaces punto a punto.

3.6.5.1 Verificación de Paquetes

Para la siguiente verificación se procederá a apagar la interface s1/1 del router Quito.

```
Quito#config ter  
Quito(config)#int s1/1  
Quito(config-int)#shutdown
```

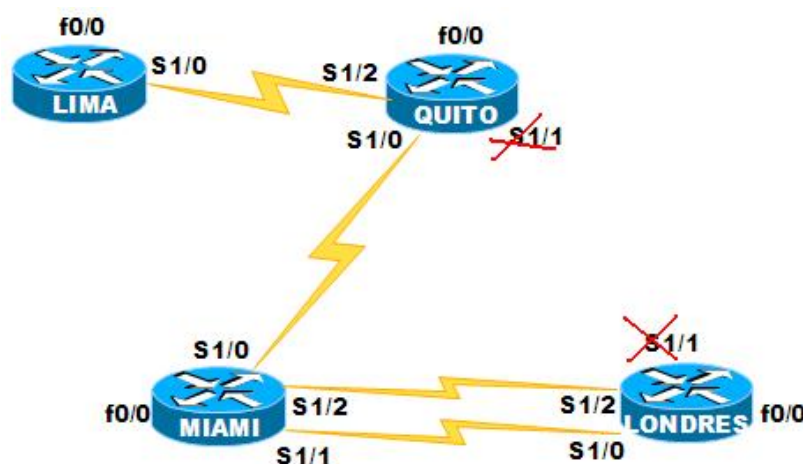


Figura 3.19 Esquema para comprobación de ruta

Desde la consola de comandos Dynagen, capturamos los paquetes desde la interface s1/0 del router Miami para observar cuál camino toma el paquete desde Londres hacia la red 192.168.10.0.

=> **capture Miami s1/0 miami.cap HDLC**

Note que siempre para interface seriales punto a punto se utiliza al final del comando el tipo de encapsulación usado, en este caso por defecto cisco usa HDLC del cual es propietario.

A continuación, abrimos el archivo Miami.cap el cual indica los procesos sucitados en la interface s1/0 del router Miami. RIP simplemente toma las dos rutas como válidas, sin importar como ya se mencionó el ancho de banda.

82	169.282000	N/A	N/A	CDP	Device ID: Miami Port ID
83	170.135000	N/A	N/A	SLARP	Line keepalive, outgoing
84	173.025000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
85	173.064000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
86	173.115000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
87	173.125000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
88	173.185000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
89	173.233000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
90	173.280000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
91	173.297000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
92	173.325000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
93	173.338000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
94	175.249000	N/A	N/A	SLARP	Line keepalive, outgoing

Figura 3.20 Prueba de conectividad Wireshark Miami.cap

Ahora procedemos a apagar la interface s1/0 del router Londres, para observar el proceso de elección de ruta y actualizamos el capturador de paquetes Wireshark.

126	275.337000	N/A	N/A	SLARP	Line keepalive, outgoing
127	275.376000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
128	275.439000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
129	275.626000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
130	275.676000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
131	275.767000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
132	275.787000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
133	275.787000	10.10.10.1	255.255.255.255	RIPv1	Response
134	275.873000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
135	275.900000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
136	275.927000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
137	275.974000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
138	279.996000	N/A	N/A	SLARP	Line keepalive, outgoing

Figura 3.21 Prueba de conectividad Wireshark Miami.cap

Ahora de manera reiterativa procedemos a prender la interface s1/0 del Router Londres para observar el proceso de elección de ruta.

179	360.001000	N/A	N/A	SLARP	Line keepalive, outgoing
180	364.297000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
181	364.346000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
182	364.403000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
183	364.451000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
184	364.481000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
185	364.488000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
186	364.503000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
187	364.518000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
188	364.540000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
189	364.551000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
190	365.267000	N/A	N/A	SLARP	Line keepalive, outgoing

Figura 3.22 Prueba de conectividad Wireshark Miami.cap

RIP hace uso de su tabla de enrutamiento es decir, que la última ruta actualizada es la más idónea para enviar los paquetes sin importar congestión o ancho de banda.

En la **Figura 3.22a** se actualizó la versión de RIP v1, a RIP v2, podemos ver el intercambio de paquetes con la etiqueta RIP v2, la cual hará que las actualizaciones de la tabla de enrutamiento no tengan ningún problema con la aplicación de subneteo variable, es decir sin el resumen de direcciones classless a redes mayores classful.

50.303000	10.10.10.1	224.0.0.9	RIPv2	Request
50.303000	10.10.10.1	224.0.0.9	RIPv2	Request
50.366000	10.10.10.1	224.0.0.9	RIPv2	Request
50.710000	10.10.10.2	10.10.10.1	RIPv2	Response
50.757000	10.10.10.2	10.10.10.1	RIPv2	Response
50.757000	10.10.10.2	10.10.10.1	RIPv2	Response
52.108000	10.10.10.1	224.0.0.9	RIPv2	Response

Figura 3.22a Captura de paquetes IP, RIPv2

3.7 PRÁCTICA 3

Tema: CONFIGURACIÓN DE OSPF -OPEN SHORT PATH FIRST-

3.7.1 OBJETIVOS

- ✓ Configurar el protocolo de enrutamiento dinámico OSPF en la topología.
- ✓ Observar el proceso de elección de DR-designated router- y BDR -backup designated router-
- ✓ Detectar posibles fallas con los comandos de configuración.
- ✓ Verificar que la red cumpla con todas las pruebas de conexión.
- ✓ Entender el comportamiento jerárquico que posee el protocolo de enrutamiento OSPF.
- ✓ Reconocer las principales características del enrutamiento dinámico OSPF

3.7.2 MARCO TEÓRICO.

El protocolo público conocido como "Primero la ruta más corta" (OSPF) es un protocolo de enrutamiento de estado del enlace no patentado. Las características clave del OSPF son las siguientes:

- ✓ Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- ✓ Envían actualizaciones desencadenadas sólo cuando se haya producido un cambio de red
- ✓ Cada router envía un *LSP -Link State Packet-*, *LSA -Link State Advertisement-* que contiene información de sus vecinos y los costos del enlace.
- ✓ Usan un mecanismo "*hello*" para determinar la posibilidad de comunicarse con los vecinos
- ✓ Cada router tiene un mapa completo de la red gracias a los *LSP's* y puede calcular la ruta más corta usando el algoritmo Dijkstra.

Todos los primeros protocolos de enrutamiento como RIP v1 eran protocolos de vector-distancia. En la actualidad, se usan muchos protocolos de enrutamiento por vector-distancia, como por ejemplo RIP v2, IGRP y el protocolo de enrutamiento híbrido EIGRP.

Comparison of Cisco's IP Distance Vector Routing Protocols

Characteristic	RIPv1	RIPv2	IGRP	EIGRP
Count to infinity	X	X	X	
Split horizon	X	X	X	X
Holddown timer	X	X	X	
Triggered updates with route poisoning	X	X	X	X
Load balancing—equal paths	X	X	X	X
Load balancing—unequal paths			X	X
VLSM support		X		X
Routing algorithm	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL
Metric	Hops	Hops	Composite	Composite
Hop count limit	15	15	100	100
Scalability	Small	Small	Medium	Large

Figura 3.23 Comparación de protocolos de Vector Distancia

Los protocolos de enrutamiento del estado de enlace difieren de los protocolos de vector-distancia. Los protocolos del estado de enlace generan una inundación de información de ruta, que da a cada router una visión completa de la topología de red. El método de actualización desencadenada por eventos permite el uso eficiente del ancho de banda y una convergencia más rápida. Los cambios en el estado de un enlace se envían a todos los Routers en la red tan pronto como se produce el cambio (2).

Los protocolos de enrutamiento del estado de enlace reúnen la información de ruta de todos los demás Routers de la red o dentro de un área definida de la red. Una vez que se haya reunido toda la información, cada router calcula las mejores rutas hacia todos los destinos de la red. Dado que cada router mantiene su propia visión de la red, es menos probable que se propague información incorrecta de parte de cualquiera de los Routers vecinos (7).

OSPF reconoce tres tipos de redes:

- ✓ Redes Punto a Punto
- ✓ Multi-access o Broadcast
- ✓ NBMA non broadcast multi-access Ej: Frame Relay

NOTA: En este capítulo y práctica se analizará el comportamiento de OSPF en redes Punto a Punto y Broadcast, en el capítulo V referente a Frame Relay trataremos más a fondo su configuración y comportamiento.

Descripción y Conceptos de OSPF

OSPF es un protocolo de estándares abiertos, entre los diferentes protocolos es el más usado debido a su versatilidad y escalabilidad. OSPF se lo puede usar y configurar en una sola área en las redes pequeñas, y en redes grandes se lo puede configurar con un diseño jerárquico. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red en un área y mejora el rendimiento.

Cada router mantiene una lista de vecinos adyacentes, que se conoce como base de datos de adyacencia. La base de datos de adyacencia es una lista de todos los Routers vecinos con los que un router ha establecido comunicación bidireccional. Esto es exclusivo de cada router.

Para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los Routers OSPF seleccionan un router designado (DR) y un router designado de respaldo (BDR) que sirven como puntos de enfoque para el intercambio de información de enrutamiento (2).

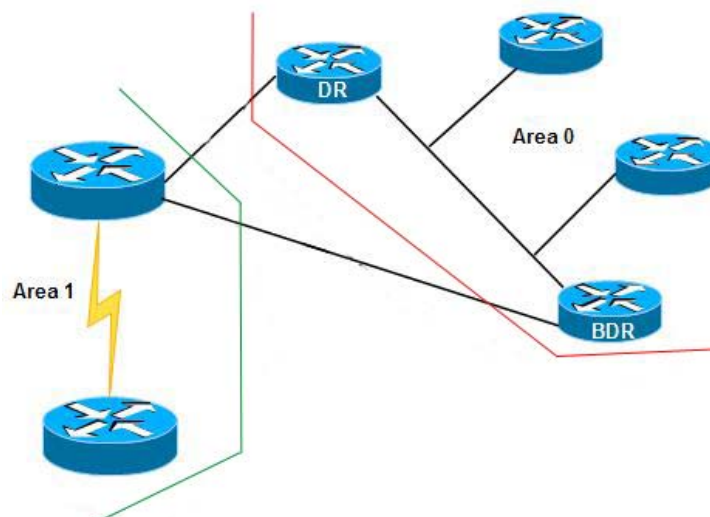


Figura 3.24 Diseño Jerárquico de Red OSPF

El valor asignado a un enlace se lo denomina “Costo”, este costo al igual que RIP es una manera para establecer la mejor ruta, en el caso de OSPF este costo es basado en el ancho de banda o la velocidad de transmisión.

Router Designado y Router Designado por Respaldo

Los Routers en un ambiente multiacceso como Ethernet, deben elegir un DR y un BDR que los represente en la red. El BDR no realiza ninguna función cuando el DR está funcionando. Esto quiere decir que simplemente recibe toda la información pero permite que el DR realice todas las tareas de sincronización y emisión. OSPF usa los siguientes criterios para establecer el DR y el BDR.

- ✓ El router con la prioridad más alta es DR.
- ✓ El router con la segunda prioridad más alta es BDR.
- ✓ Por defecto la prioridad es uno en la interfaces OSPF. En caso de un empate se usa el ID, el ID es el numero de IP en este caso también el más alto es elegido DR y el siguiente BDR.
- ✓ Un router con prioridad 0 nunca será elegido DR o BDR, este es luego llamado “Drother”
- ✓ Si un router con mayor prioridad ingresa en la red, el DR y el BDR no cambian a menos que estos fallen.

OSPF Múltiples Áreas.

Como se hablo anteriormente OSPF designa Routers fronterizos para reducir el intercambio de información entre múltiples áreas, este concepto es muy importante ya que este protocolo de enrutamiento tiene un diseño jerárquico.

Características de la aplicación de múltiples áreas:

- Cada área es responsable de su operabilidad.
- Routers pertenecientes a otras áreas no necesitan continuamente correr el algoritmo SPF, ya que los problemas son aislados por área.
- Reduce los LSAs propagados entre áreas.
- Se puede controlar los tipos de información de rutas que se permite dentro y fuera de un área.

Tipos de Routers para la interconexión de Múltiples Áreas.

- ✓ Router Internos.- Estos Routers se caracterizan por que tienen todas sus interfaces dentro de un área.
- ✓ Routers de Backbone.- Routers que tienen por lo menos una interface conectada al área 0.
- ✓ Router Fronterizo de Área. -*Area Border Router*-. Router que poseen interfaces pertenecientes a múltiples áreas.
- ✓ Router Fronterizo de Sistema Autónomo. *Autonomous System Boundery Router*. – Si poseen una interface dentro de una interconexión externa.

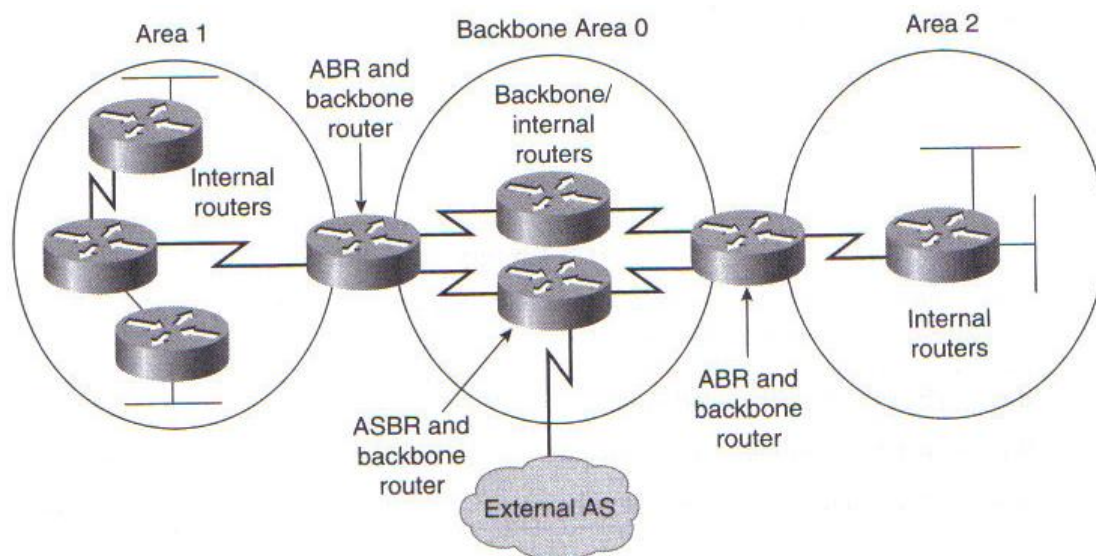


Figura 3.25 Diseño Jerárquico de Red OSPF –Tipos de Routers-

Tipos de Áreas

- ✓ Área Estándar.- Esta área acepta actualización de enlaces internos, sumarización de rutas entre áreas, y rutas externas.
- ✓ Área Backbone.- Todas las demás áreas se conectan a esta área para intercambio de información.
- ✓ Stub Área.- Esta área no acepta información de rutas externas a un sistema autónomo.
- ✓ *Totally Stubby Área*.- Esta área no acepta rutas de sistemas autónomos externos, o rutas sumarizadas de otras rutas internas. Si el Router necesita enviar un paquete hacia una red externa este puede hacer uso de una ruta configurada por defecto.
- ✓ *Not-so-stubby-área*.- Esta área importa un limitado número de rutas externas

Configuración de OSPF

El enrutamiento OSPF utiliza el concepto de áreas. Cada router contiene una base de datos completa de los estados de enlace de un área específica. A un área de la red OSPF se le puede asignar cualquier número de 0 a 65.535. En las redes OSPF con varias áreas, se requiere que todas las áreas se conecten al área 0. El área 0 también se denomina el área backbone (2).

La configuración de OSPF requiere que el proceso de enrutamiento OSPF esté activo en el router con las direcciones de red y la información de área especificadas. Las direcciones de red se configuran con una máscara wildcard y no con una máscara de subred. La máscara wildcard representa las direcciones de enlaces o de host que pueden estar presentes en este segmento. Los ID de área se pueden escribir como número entero o con la notación decimal punteada

```
Router(config)#router ospf process-id
```

En la línea de comando encontramos el número de *process id*, este número puede tener cualquier valor entre 1 y 65535. La mayoría de los administradores de red utilizan el mismo número para cada sistema autónomo.

```
Router(config-router)#network address wildcard-mask area area-id
```

La máscara wildcard representa el conjunto de direcciones de host que admite el segmento. Esto es distinto de lo que ocurre con una máscara de subred que se utiliza al configurar las direcciones IP en las interfaces.

3.7.3 ESQUEMA DE LA RED

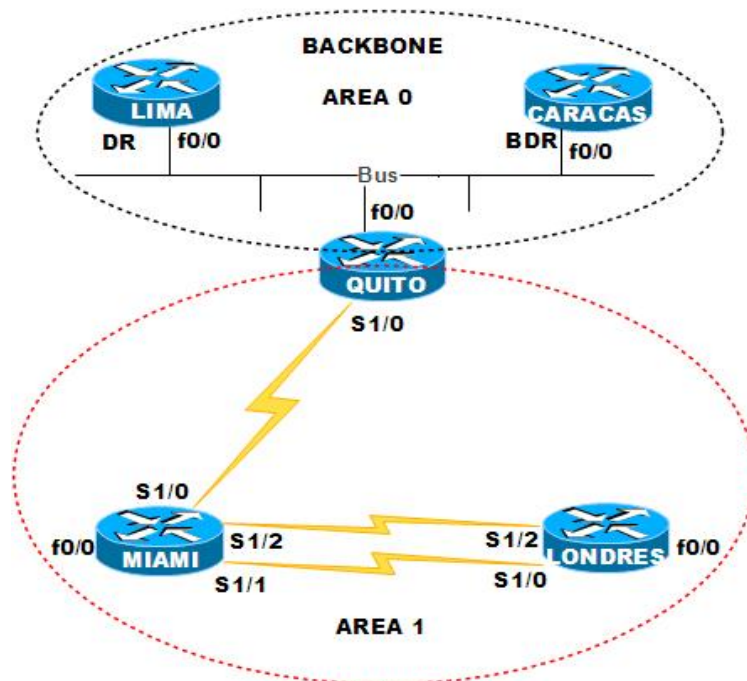


Figura 3.26 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface
Lima		192.168.10.3	255.255.255.240	f0/0
Quito		192.168.10.1	255.255.255.240	f0/0
	DCE	10.10.10.1	255.255.255.252	S1/0
Miami	DTE	10.10.10.2	255.255.255.252	S1/0
	DCE	10.10.10.10	255.255.255.252	S1/1
	DCE	10.10.10.17	255.255.255.252	S1/2
		192.168.20.1	255.255.255.0	f0/0
Londres	DTE	10.10.10.9	255.255.255.252	S1/0
	DTE	10.10.10.18	255.255.255.252	S1/2
		192.168.30.1	255.255.255.0	f0/0
Caracas		192.168.10.2	255.255.255.240	f0/0

Tabla 3.5 Datos de la Red WAN –OSPF múltiples áreas-

3.7.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

Primero se procede configurar en cada router, los nombres de host, consola, terminal virtual y activación de claves como se realizó ya en las primeras prácticas usando la **Tabla 3.5** como guía para establecer el esquema de la red.

A continuación se configura el protocolo de enrutamiento OSPF en el “area 0” y luego el “area 1”.

```
Lima# router ospf 1
```

```
Lima(config-router)#network 192.168.10.0 0.0.0.15 area 0
```

```
Lima(config-router)#end
```

```
Quito# router ospf 1
```

```
Quito(config-router)#network 192.168.10.0 0.0.0.15 area 0
```

```
Quito(config-router)#network 10.10.10.0 0.0.0.3 area 1
```

```
Quito(config-router)#end
```

```
Caracas# router ospf 1
```

```
Caracas(config-router)#network 192.168.10.0 0.0.0.15 area 0
```

```
Caracas(config-router)#end
```

```
Miami#router ospf 1
```

```
Miami(config-router)#network 192.168.20.0 0.0.0.255 area 1
```

```
Miami(config-router)#network 10.10.10.0 0.0.0.3 area 1
```

```
Miami(config-router)#network 10.10.10.16 0.0.0.3 area1
```

```
Miami(config-router)#network 10.10.10.8 0.0.0.3 area 1
```

```
Miami(config-router)#end
```

```
Londres#router ospf 1
```

```
Londres(config-router)#network 192.168.30.0 0.0.0.255 area 1
```

```
Londres(config-router)#network 10.10.10.0 0.0.0.3 area 1
```

```
Londres(config-router)#end
```

3.7.5 VERIFICACIÓN DE OSPF MULTIAREA.

Primero realizamos una prueba de conectividad con el comando ping o telnet ya que se encuentra levantado el protocolo de enrutamiento para las distintas redes del esquema **Figura 3.27**.

```

Quito#
Quito#ping 192.168.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/76/140 ms
Quito#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/79/92 ms
Quito#ping 10.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/128/336 ms
Quito#ping 10.10.10.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.18, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/128/184 ms
Quito#ping 10.10.10.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.9, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/197/324 ms

```

Figura 3.27 Verificación de Conectividad

Para desplegar la información de los Routers vecinos que usan el protocolo de enrutamiento OSPF, se usa el comando *show ip ospf neighbor*, el cual en la **Figura 3.28**, nos muestra en el router Miami, las IDs de los Routers exclusivamente del área donde se encuentran, en este caso el Área 1, además presenta la prioridad de cada router y su estado, en el caso de redes multiacceso, también muestra las interfaces por las cuales se comunica.

```

Miami#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address          Interface
192.168.30.1     0     FULL/ -         00:00:36   10.10.10.18     Serial1/2
192.168.30.1     0     FULL/ -         00:00:36   10.10.10.9      Serial1/1
192.168.10.1     0     FULL/ -         00:00:33   10.10.10.1      Serial1/0

```

Figura 3.28 Show IP OSPF neighbor router Miami

En el router Quito usamos este mismo criterio. Debido al diseño de la red, el área 0, o backbone, es una red multiacceso, en la cual existe la elección de un router DR y BDR, en la pantalla encontramos esta elección. OSPF elige como DR al router con el ID más alto y luego el que sigue en jerarquía como el BDR.

```
Quito#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
192.168.10.2    1     FULL/BDR        00:00:36   192.168.10.2 FastEthernet0/
0
192.168.10.3    1     FULL/DR         00:00:38   192.168.10.3 FastEthernet0/
0
192.168.20.1    0     FULL/-          00:00:34   10.10.10.2   Serial1/0
Quito#
```

Figura 3.29 Show IP OSPF neighbor router Quito

El comando *show ip ospf interface* presenta información específica de las interfaces que usan este protocolo, en la **Figura 3.30** entre lo más importante encontramos el ID de proceso, el ID del router, y el tipo de red que está conectado con su respectivo costo, el cual es 1 por defecto, ver Anexo pagina. A9.

```
Quito#show ip ospf interface
FastEthernet0/0 is up, line protocol is up
Internet Address 192.168.10.1/28, Area 0
Process ID 1, Router ID 192.168.10.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 192.168.10.3, Interface address 192.168.10.3
Backup Designated router (ID) 192.168.10.2, Interface address 192.168.10.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Index 1/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.10.2 (Backup Designated Router)
  Adjacent with neighbor 192.168.10.3 (Designated Router)
Suppress hello for 0 neighbor(s)
```

Figura 3.30 Show IP OSPF interface router Quito

Si siguiendo con la secuencia de pantallas se encuentra la información de la siguiente interface en la **Figura 3.31**, esta interface es un enlace serial en el router Quito, en este se despliega el tipo de red que a diferencia de la anterior interface es Punto a Punto con una asignación distinta de costo 64, este comando también presenta el intercambio de paquetes *hello* que son un mecanismo de estado de enlace para mantener convergencia en toda la red o área, en este caso.

```

Serial1/0 is up, line protocol is up
Internet Address 10.10.10.1/30, Area 1
Process ID 1, Router ID 192.168.10.1, Network Type POINT TO POINT, Cost: 64
Transmit Delay is 1 sec, State POINT TO POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 4 msec, maximum is 4 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.20.1
Suppress hello for 0 neighbor(s)

```

Figura 3.31 Show IP OSPF interface router Quito

Aplicamos el comando anterior en el Router Miami, aquí podemos observar e identificar ciertas características que debe tener nuestro router. Algo que se ha hecho énfasis en esta práctica es el uso del camino redundante, ya que OSPF si hace uso del ancho de banda para establecer el costo del enlace, además podemos ver un costo más grande que el que posee una conexión T1 común y corriente debido al cambio de ancho de banda que se realizó en su configuración **Figura 3.32 y 3.33**

```

Serial1/2 is up, line protocol is up
Internet Address 10.10.10.17/30, Area 1
Process ID 1, Router ID 192.168.20.1, Network Type POINT TO POINT, Cost: 129
Transmit Delay is 1 sec, State POINT TO POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.30.1
Suppress hello for 0 neighbor(s)

```

Figura 3.32 Show IP OSPF interface router Miami

```

Serial1/1 is up, line protocol is up
Internet Address 10.10.10.10/30, Area 1
Process ID 1, Router ID 192.168.20.1, Network Type POINT TO POINT, Cost: 64
Transmit Delay is 1 sec, State POINT TO POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 192.168.30.1
Suppress hello for 0 neighbor(s)

```

Figura 3.33 Show IP OSPF interface router Miami

Show ip route, nos muestra los caminos más cortos por donde se enviarán los paquetes hacia las diferentes redes; desde el router Miami usamos este comando, podemos

observar entonces el protocolo de enrutamiento usado en las interfaces y las redes conocidas, que pueden ser conectadas directa e indirectamente, en la **Figura 3.34** encontramos en los recuadros verdes las redes hacia el router Londres y el router Quito, respectivamente, con su distancia administrativa y costo, fíjese que no existe otro camino debido a que éste es el camino más corto por el cual puede llegar, si apagamos esta interface s1/1 luego aparecería como la mejor ruta la interface s1/2 el cual posee la mitad de ancho de banda que el anterior.

Otro aspecto importante que observar es la distinción entre áreas usada para cada red, en el segundo recuadro verde encontramos las sigla IA para la red 192.168.10.1 el cual indica que esta red pertenece a otra área en particular.

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

Gateway of last resort is not set

O 192.168.30.0/24 [110/65] via 10.10.10.9, 00:17:14, Serial1/1
  192.168.10.0/28 is subnetted, 1 subnets
O IA 192.168.10.0 [110/65] via 10.10.10.1, 00:17:14, Serial1/0
C 192.168.20.0/24 is directly connected, FastEthernet0/0
  10.0.0.0/30 is subnetted, 3 subnets
C 10.10.10.8 is directly connected, Serial1/1
C 10.10.10.0 is directly connected, Serial1/0
C 10.10.10.16 is directly connected, Serial1/2
```

Figura 3.34 Show IP route desde el router Miami

3.7.5.1 Verificación de Paquetes

Para la siguiente verificación se procederá a apagar la interface s1/0 del router Londres.

```
Londres#config ter
Londres(config)#int s1/0
Londres(config-int)#shutdown
```

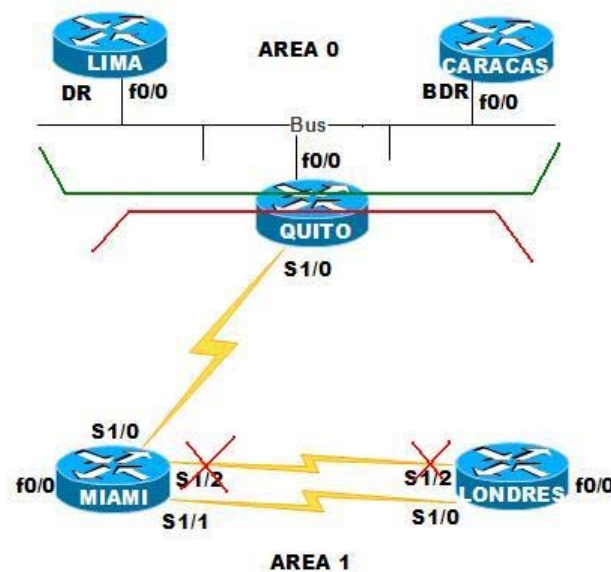


Figura 3.35 Esquema para comprobación de ruta

Desde la consola de comandos Dynagen, capturamos los paquetes desde la interface s1/0 del router Miami para observar cual camino toma el paquete desde Londres hacia la red 192.168.10.1.

=> **capture Miami s1/0 miami.cap HDLC**

A continuación, abrimos el archivo Miami.cap el cual indica los procesos en la interface s1/0 del router Miami. OSPF usa una métrica compuesta por el ancho de banda de cada enlace en este caso la interface s1/0 es la ruta más corta debido a su bajo costo asignado **Figura 3.36**.

27	56.476000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
28	56.558000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
29	56.667000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
30	56.694000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
31	56.775000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
32	56.787000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
33	56.874000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
34	56.903000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply
35	56.972000	10.10.10.9	192.168.10.1	ICMP	Echo (ping) request
36	56.992000	192.168.10.1	10.10.10.9	ICMP	Echo (ping) reply

Figura 3.36 Prueba de conectividad Wireshark Miami.cap

Ahora procedemos a apagar la interface s1/0 del router Londres, para observar el proceso de elección de ruta y actualizamos el capturador de paquetes Wireshark. Además podemos ver el envío de paquetes de estado de enlace LS, los cuales avisan del cambio que se produjo en la red, en este caso el DR se encarga de enviar un *LS update* hacia todos los demás Routers para que conozcan del cambio por medio de la dirección 224.0.0.5

64	121.759000	10.10.10.2	224.0.0.5	OSPF	Hello Packet
65	122.136000	10.10.10.1	224.0.0.5	OSPF	Hello Packet
66	123.649000	10.10.10.2	224.0.0.5	OSPF	LS Update
67	123.689000	N/A	N/A	CDP	Device ID: Miami Port ID: Serial1/0
68	123.962000	N/A	N/A	SLARP	Line keepalive, outgoing sequence 60,
69	126.214000	10.10.10.1	224.0.0.5	OSPF	LS Acknowledge
70	129.994000	N/A	N/A	SLARP	Line keepalive, outgoing sequence 62,
71	131.721000	10.10.10.2	224.0.0.5	OSPF	Hello Packet
72	132.155000	10.10.10.1	224.0.0.5	OSPF	Hello Packet

88	162.757000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
89	162.853000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
90	163.005000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
91	163.027000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
92	163.080000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
93	163.108000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
94	163.208000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
95	163.245000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
96	163.325000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
97	163.387000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
98	163.928000	N/A	N/A	SLARP	Line keepalive, out

Figura 3.37 Prueba de conectividad Wireshark Miami.cap

Ahora nuevamente procedemos a prender la interface s1/0 del Router Londres para observar el proceso de elección de ruta.

87	162.158000	10.10.10.1	224.0.0.5	OSPF	Hello Packet
88	162.757000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
89	162.853000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
90	163.005000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
91	163.027000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
92	163.080000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
93	163.108000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
94	163.208000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
95	163.245000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply
96	163.325000	10.10.10.18	192.168.10.1	ICMP	Echo (ping) request
97	163.387000	192.168.10.1	10.10.10.18	ICMP	Echo (ping) reply

Figura 3.38 Prueba de conectividad Wireshark Miami.cap

En los Routers Cisco, si una ruta ya existe, la tabla de enrutamiento es usada al mismo tiempo que el cálculo de la ruta más corta SPF, Si SPF está calculando una nueva ruta, el uso de la tabla de enrutamiento ocurrirá sólo después de que se haya completado el cálculo de SPF

3.8 PRÁCTICA 4

Tema: CONFIGURACIÓN DE EIGRP –ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL-

3.8.1 OBJETIVOS

- ✓ Configurar el protocolo de enrutamiento dinámico EIGRP en la topología.
- ✓ Detectar posibles fallas con los comandos de verificación.
- ✓ Verificar el correcto funcionamiento de la red y el protocolo.
- ✓ Analizar el intercambio de paquetes en EIGRP.
- ✓ Reconocer las principales características del enrutamiento EIGRP y su comportamiento para escoger la mejor ruta entre caminos de distinto ancho de banda.
- ✓ Comprender el cálculo compuesto de su métrica.

3.8.2 MARCO TEÓRICO.

El EIGRP es un protocolo mejorado de enrutamiento por vector-distancia, patentado por Cisco. Las características más importantes de EIGRP son las siguientes:

- ✓ Es un protocolo mejorado de enrutamiento por vector-distancia.
- ✓ Utiliza balanceo de carga asimétrico.
- ✓ Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace.
- ✓ Utiliza el Algoritmo de Actualización Difusa (DUAL) para el cálculo de la ruta más corta.
- ✓ Las actualizaciones son mensajes de multicast a la dirección 224.0.0.10 generadas por cambios en la topología.

Los Routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

EIGRP guarda las rutas que se aprenden de manera específicas. Las rutas reciben un estado específico y se pueden rotular para proporcionar información adicional de utilidad.

EIGRP mantiene las siguientes tablas:

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

Tabla de vecinos.- Cada router EIGRP mantiene una tabla de vecinos que enumera a los Routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

Al conocer nuevos vecinos, se registran la dirección y la interfaz del vecino. Cuando un vecino envía un paquete *hello*, publica un tiempo de espera². Si un paquete *hello* no se recibe dentro del tiempo de espera, entonces se informa al Algoritmo de Actualización Difusa (DUAL) que el router no es alcanzable y este necesitará hacer el cambio en la topología para hacer conocer a los demás.

Tabla de topología.- Esta se compone de todas las tablas de enrutamiento EIGRP en el sistema autónomo.

DUAL toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino. EIGRP rastrea esta información para que los Routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de DUAL se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los Routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red. La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica (2).

² Tiempo de espera: Es la cantidad de tiempo durante el cual un router considera que un vecino se puede alcanzar

Campos que conforman la tabla de enrutamiento:

- ✓ **Distancia Factible (FD) –*Feasible distance*–:** Ésta es la métrica calculada más baja hacia cada destino.
- ✓ **Origen de la ruta:** Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el enrutamiento basado en políticas.
- ✓ **Distancia informada (AD) –*advertised distance*– :** La distancia informada (AD) de la ruta es la distancia informada por un vecino adyacente hacia un destino específico.
- ✓ **Información de interfaz:** La interfaz a través de la cual se puede alcanzar el destino.
- ✓ **Estado de ruta:** El estado de una ruta. Una ruta se puede identificar como *pasiva*, lo que significa que la ruta es estable y está lista para usar, o *activa*, lo que significa que la ruta se encuentra en el proceso de recálculo por parte de DUAL.

Tabla de enrutamiento.- EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología. Los Routers EIGRP mantienen una tabla de enrutamiento por cada protocolo de red. Un sucesor es una ruta seleccionada como ruta principal para alcanzar un destino. DUAL identifica esta ruta en base a la información que contienen las tablas de vecinos y de topología y la coloca en la tabla de enrutamiento. Puede haber hasta cuatro rutas de sucesor para cada destino en particular. Éstas pueden ser de costo igual o desigual y se identifican como las mejores rutas sin bucles hacia un destino determinado (2).

Un sucesor factible (FS) –*feasible sucesor*– es una ruta de respaldo. Estas rutas se identifican al mismo tiempo que los sucesores, pero sólo se mantienen en la tabla de topología. Los múltiples sucesores factibles para un destino se pueden mantener en la tabla de topología, aunque no es obligatorio (2).

Un router visualiza los sucesores factibles como vecinos corriente abajo, o más cerca del destino que él. El costo del sucesor factible se calcula a base del costo publicado del router vecino hacia el destino. Si una ruta del sucesor colapsa, el router busca un sucesor factible identificado. Esta ruta se promoverá al estado de sucesor. Un sucesor factible debe tener un costo publicado menor que el costo del sucesor actual hacia el destino. Si es imposible identificar un sucesor factible en base a la información actual, el router coloca un estado activo en una ruta y envía paquetes de consulta a todos los vecinos para re calcular la topología actual. El router puede identificar cualquier nuevo sucesor o sucesor factible a partir de los nuevos datos recibidos de los paquetes de respuesta que responden a los pedidos de consulta. Entonces, el router establecerá el estado de la ruta en pasivo.

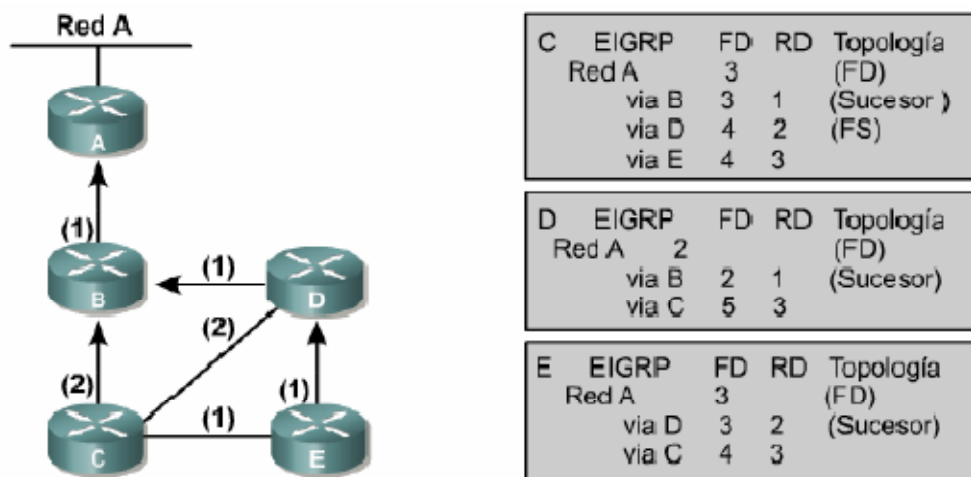


Figura 3.39 Ejemplo del Algoritmo DUAL de EIGRP

Es posible registrar información adicional acerca de cada ruta en la tabla de topología. EIGRP clasifica a las rutas como internas o externas. EIGRP agrega un rótulo de ruta a cada ruta para identificar esta clasificación.

Las rutas internas se originan dentro del AS EIGRP

Las rutas externas se originan fuera del AS EIGRP.

Las rutas aprendidas o redistribuidas desde otros protocolos de enrutamiento como RIP, OSPF e IGRP son externas. Las rutas estáticas que se originan fuera del AS EIGRP son externas. El rótulo puede establecerse en un número entre 0-255 para adaptar el rótulo.

Ventajas de EIGRP sobre los protocolos de vector-distancia simples:

- ✓ Convergencia rápida
- ✓ Uso eficiente del ancho de banda
- ✓ Compatibilidad con VLSM y CIDR
- ✓ Compatibilidad con capas de varias redes
- ✓ Independencia de los protocolos enrutados

EIGRP envía actualizaciones parciales y limitadas, y hace un uso eficiente del ancho de banda. EIGRP usa un ancho de banda mínimo cuando la red es estable.

Los Routers EIGRP no envían las tablas en su totalidad, sino que envían actualizaciones parciales e incrementales.

Esto es parecido a la operación de OSPF, salvo que los Routers EIGRP envían estas actualizaciones parciales sólo a los Routers que necesitan la información, no a todos los Routers del área. Por este motivo, se denominan actualizaciones limitadas. En vez de enviar actualizaciones de enrutamiento temporizadas, los Routers EIGRP usan pequeños paquetes **hello** para mantener la comunicación entre sí. Aunque se intercambian con regularidad, los paquetes **hello** no usan una cantidad significativa de ancho de banda.

EIGRP admite IP, IPX y AppleTalk mediante los PDM³. EIGRP puede redistribuir información de IPX, RIP y SAP para mejorar el desempeño general.

EIGRP usa una métrica compuesta configurable para determinar la mejor ruta.

Tecnologías EIGRP

³ PDM: Módulos dependientes de Protocolo

Cada nueva tecnología representa una mejora con respecto a la eficiencia en la operación de EIGRP, la velocidad de convergencia o la funcionalidad con respecto a IGRP y otros protocolos de enrutamiento. Estas tecnologías pertenecen a una de las siguientes cuatro categorías:

- ✓ Detección y recuperación de vecinos
- ✓ Protocolo de transporte confiable
- ✓ Algoritmo de máquina de estado finito DUAL
- ✓ Módulos dependientes de protocolo

Un router EIGRP supone que, siempre y cuando reciba paquetes *hello* de los vecinos conocidos, estos vecinos y sus rutas seguirán siendo viables o pasivos. Lo siguiente puede ocurrir cuando los Routers EIGRP forman adyacencias: Aprender de forma dinámica las nuevas rutas que se unen a la red

- ✓ Identificar los Routers que llegan a ser inalcanzables o inoperables
- ✓ Redetectar los Routers que habían estado inalcanzables anteriormente

El (RTP)⁴ es un protocolo de capa de transporte que garantiza la entrega ordenada de paquetes EIGRP a todos los vecinos.

En una red IP, los hosts usan TCP para secuenciar los paquetes y asegurarse de que se entreguen de manera oportuna. Sin embargo, EIGRP es independiente de los protocolos.

Esto significa que *no se basa en TCP/IP* para intercambiar información de enrutamiento de la forma en que lo hacen RIP, IGRP y OSPF. Para mantenerse independiente de IP, EIGRP usa RTP como su protocolo de capa de transporte propietario para garantizar la entrega de información de enrutamiento (2).

EIGRP puede hacer una llamada a RTP para que proporcione un servicio confiable o no confiable, según lo requiera la situación. Por ejemplo, los paquetes *hello* no requieren

⁴ RTP: Protocolo de Transporte Confiable

el gasto de la entrega confiable porque se envían con frecuencia y se deben mantener pequeños. La entrega confiable de otra información de enrutamiento puede realmente acelerar la convergencia porque entonces los routers EIGRP no tienen que esperar a que un temporizador expire antes de retransmitir. (7)

Con RTP, EIGRP puede realizar envíos en multicast y en unicast a diferentes pares de forma simultánea. Esto maximiza la eficiencia.

Una de las mejores características de EIGRP es su diseño modular. Se ha demostrado que los diseños modulares o en capas son los más escalables y adaptables. EIGRP logra la compatibilidad con los protocolos enrutados, como IP, IPX y AppleTalk, mediante los PDM. En teoría, EIGRP puede agregar PDM para adaptarse fácilmente a los protocolos enrutados nuevos o revisados como IPv6.

Cada PDM es responsable de todas las funciones relacionadas con su protocolo enrutado específico. El módulo IP-EIGRP es responsable de las siguientes funciones:

- ✓ Enviar y recibir paquetes EIGRP que contengan datos IP
- ✓ Avisar a DUAL una vez que se recibe la nueva información de enrutamiento IP
- ✓ Mantener los resultados de las decisiones de enrutamiento DUAL en la tabla de enrutamiento IP
- ✓ Redistribuir la información de enrutamiento que se aprendió de otros protocolos de enrutamiento capacitados para IP

Paquetes de datos EIGRP

Al igual que OSPF, EIGRP depende de diferentes tipos de paquetes para mantener sus tablas y establecer relaciones con los Routers vecinos. Esta sección describirá estos tipos de paquetes.

Paquetes EIGRP:

- ✓ Hello

- ✓ Acuse de recibo
- ✓ Actualización
- ✓ Consulta
- ✓ Respuesta

EIGRP depende de los paquetes *hello* para detectar, verificar y volver a detectar los Routers vecinos. La segunda detección se produce si los Routers EIGRP no intercambian *hellos* durante un intervalo de tiempo de espera pero después vuelven a establecer la comunicación.

El intervalo hello por defecto depende del ancho de banda de la interfaz. En las redes IP, los Routers EIGRP envían hellos a la dirección IP multicast 224.0.0.10.

Los routers EIGRP almacenan la información sobre los vecinos en la tabla de vecinos. La tabla de vecinos incluye el campo de Número de Secuencia (Seq No) para registrar el número del último paquete EIGRP recibido que fue enviado por cada vecino.

La tabla de vecinos también incluye un campo de Tiempo de Espera que registra el momento en que se **recibió** el último paquete. Los paquetes deben recibirse dentro del período correspondiente al intervalo de Tiempo de Espera para mantenerse en el estado Pasivo. *El estado Pasivo significa un estado alcanzable y operacional.*

Si EIGRP no recibe un paquete de un vecino dentro del tiempo de espera, EIGRP supone que el vecino no está disponible. En ese momento, interviene DUAL para reevaluar la tabla de enrutamiento. Por defecto, el tiempo de espera es equivalente al triple del intervalo hello, pero un administrador puede configurar ambos temporizadores según lo desee.

Los Routers EIGRP usan paquetes de acuse de recibo para indicar la recepción de cualquier paquete EIGRP durante un intercambio confiable. RTP proporciona comunicación confiable entre hosts EIGRP. El receptor debe enviar acuse de recibo de un mensaje recibido para que sea confiable. Los paquetes de acuse de recibo, que son paquetes hello sin datos, se usan con este fin. Al contrario de los hellos multicast, los

paquetes de acuse de recibo se envían en unicast. Los acuses de recibo pueden adjuntarse a otros tipos de paquetes EIGRP, como los **paquetes de respuesta**.

Los **paquetes de actualización** se utilizan cuando un router detecta un nuevo vecino o un cambio de topología. Los Routers EIGRP envían paquetes de actualización en unicast a ese nuevo vecino para que pueda aumentar su tabla de topología o en el caso de cambio de topología envían un multicast a todos los vecinos, avisando el cambio. Es posible que se necesite más de un paquete de actualización para transmitir toda la información de topología al vecino recientemente detectado (8).

Si un router EIGRP pierde su sucesor y no puede encontrar un sucesor factible para una ruta, DUAL coloca la ruta en el estado Activo. Entonces se envía una consulta en multicast a todos los vecinos con el fin de ubicar un sucesor para la red destino. Los vecinos deben enviar respuestas que suministren información sobre sucesores o indiquen que no hay información disponible. Las consultas se pueden enviar en multicast o en unicast, mientras que las respuestas siempre se envían en unicast. Ambos tipos de paquetes se envían de forma confiable (2).

Algoritmo DUAL usado en EIGRP

Para comprender mejor la convergencia con DUAL, vea el ejemplo en la **Figura 3.40**. Cada router ha construido una tabla de topología que contiene información acerca de la manera de enrutar al destino Red A (2).

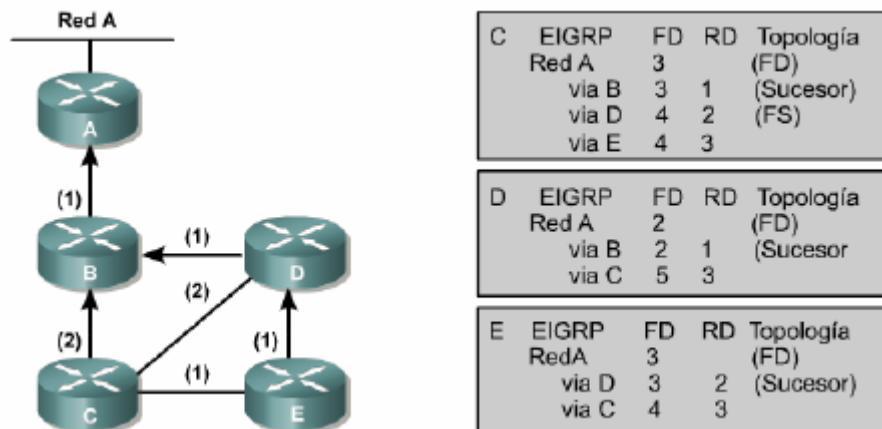


Figura 3.40 Ejemplo de elección de Ruta DUAL EIGRP

- ✓ Cada tabla de topología identifica la siguiente información: El protocolo de enrutamiento EIGRP
- ✓ El costo más bajo de la ruta, denominado distancia factible (FD)
- ✓ El costo de la ruta, según lo publica el router vecino, denominado distancia informada (RD)
- ✓ La columna de Topología identifica la ruta principal denominada ruta del sucesor (sucesor), y, cuando se identifica, la ruta de respaldo denominada sucesor factible (FS).

3.8.3 ESQUEMA DE LA RED

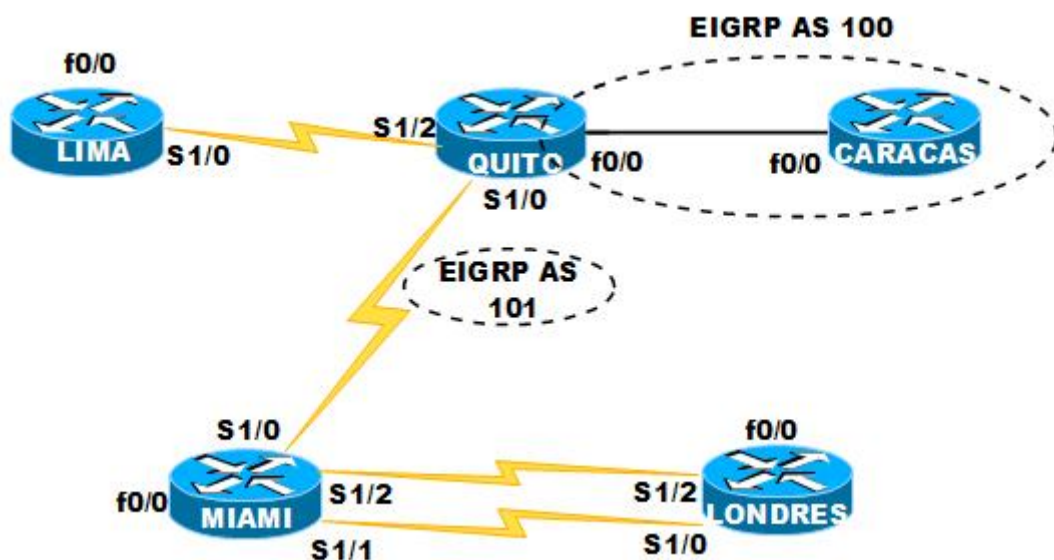


Figura 3.41 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface	AS
Lima	DTE	10.10.10.13	255.255.255.252	S1/0	101
		192.168.40.1	255.255.255.0	f0/0	101
Quito	DCE	10.10.10.1	255.255.255.252	S1/0	101
		10.10.10.14	255.255.255.252	S1/2	101
		192.168.10.1	255.255.255.240	f0/0	100
Miami	DTE	10.10.10.2	255.255.255.252	S1/0	101
		10.10.10.10	255.255.255.252	S1/1	101
	DCE	10.10.10.17	255.255.255.252	S1/2	101
		192.168.20.1	255.255.255.0	f0/0	101
Londres	DTE	10.10.10.9	255.255.255.252	S1/0	101
		10.10.10.18	255.255.255.252	S1/2	101
		192.168.30.1	255.255.255.0	f0/0	101
Caracas		192.168.10.2	255.255.255.240	f0/0	100

Tabla 3.6 Datos de la Red WAN

3.8.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

De igual manera que en anteriores practicas configuramos cada router con sus respectivas IPs, los nombres de host, consola, terminal virtual y activación de claves, para estableces el esquemas de la red.

A continuación se configura el protocolo de enrutamiento EIGRP teniendo en cuenta el valor para los sistemas autónomos, EIGRP es muy fácil de implementar usa el mismo método de configuración que IGRP y RIP especificando el número de sistemas autónomo y la red que se pretende usar.

Lima#config ter

Lima(config)#router eigrp 101

Lima(config-router)#network 192.168.40.0

Lima(config-router)#network 10.0.0.0

Lima(config-router)#exit

Quito#config ter

Quito(config)#router eigrp 101

Quito(config-router)#network 10.0.0.0

```
Quito(config-router)#exit
Quito(config)#router eigrp 100
Quito(config-router)#network 192.168.10.0
Quito(config-router)#exit
```

```
Miami#config ter
Miami(config)#router eigrp 101
Miami(config-router)#network 192.168.20.0
Miami(config-router)#network 10.0.0.0
Miami(config-router)#exit
```

```
Londres#config ter
Londres(config)#router eigrp 101
Londres(config-router)#network 192.168.30.0
Londres(config-router)#network 10.0.0.0
Londres(config-router)#exit
```

```
Caracas#config ter
Caracas(config)#router eigrp 100
Caracas(config-router)#network 192.168.10.0
Caracas(config-router)#exit
```

3.8.5 VERIFICACIÓN DE EIGRP

Después de activar el protocolo de enrutamiento EIGRP procedemos a realizar las pruebas de conectividad desde el router Quito usando el comando Ping y telnet para asegurar que existe conectividad en las demás capas del modelo OSI.

```

Quito#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/57/128 ms
Quito#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/68/136 ms
Quito#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/161/568 ms
Quito#telnet 192.168.30.1
Trying 192.168.30.1 ... Open

User Access Verification

Password:
Londres>enable
Password:
Londres#

```

Figura 3.42 Pruebas de conectividad Ping y Telnet EIGRP

Con el comando *show ip route* examinamos las tablas de enrutamiento de los Routers Quito, Miami, Caracas **Figura 3.43, 3.44 y 3.45**.

En la **Figura 3.43** podemos ver todas las rutas que posee el router Quito hacia las distintas redes conectadas directa e indirectamente, EIGRP usa un cálculo de métrica compuesta, y su distancia administrativa por defecto es 90 véase **Tabla 3.3**.

```

Londres#exit
[Connection to 192.168.30.1 closed by foreign host]
Quito#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D 192.168.30.0/24 [90/2684416] via 10.10.10.2, 01:08:11, Serial1/0
  192.168.10.0/28 is subnetted, 1 subnets
C 192.168.10.0 is directly connected, FastEthernet0/0
D 192.168.40.0/24 [90/2172416] via 10.10.10.13, 01:08:11, Serial1/2
D 192.168.20.0/24 [90/2172416] via 10.10.10.2, 01:08:11, Serial1/0
  10.0.0.0/30 is subnetted, 4 subnets
D 10.10.10.8 [90/2681856] via 10.10.10.2, 01:08:11, Serial1/0
C 10.10.10.12 is directly connected, Serial1/2
C 10.10.10.0 is directly connected, Serial1/0
D 10.10.10.16 [90/4339968] via 10.10.10.2, 01:08:11, Serial1/0
Quito#_

```

Figura 3.43 Tablas de enrutamiento router Quito

De acuerdo con la topología existen dos caminos hacia la red 192.168.30.0 pero EIGRP escoge la ruta más corta por la interfaz 10.10.10.9 ya que este posee un ancho de banda mayor que la de la interfaz 10.10.10.18 **Figura 3.44**.

Con el comando *show ip route* mas la *ip* a la cual se quiere alcanzar podemos ver información más detallada sobre la interfaz. En la **Figura 3.45** podemos ver la comparación entre las métricas de ambas rutas.

```

Quito# show ip route 10.10.10.9
Routing entry for 10.10.10.8/30
  Known via "eigrp 101", distance 90, metric 2681856, type internal
  Redistributing via eigrp 101
  Last update from 10.10.10.2 on Serial1/0, 00:18:35 ago
  Routing Descriptor Blocks:
  * 10.10.10.2, from 10.10.10.2, 00:18:35 ago, via Serial1/0
    Route metric is 2681856, traffic share count is 1
    Total delay is 40000 microseconds, minimum bandwidth is 1544 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1

```

Figura 3.44 Tablas de enrutamiento router Quito para alcanzar la int s1/2 en el router Londres

```

Quito# show ip route 10.10.10.18
Routing entry for 10.10.10.16/30
  Known via "eigrp 101", distance 90, metric 4339968, type internal
  Redistributing via eigrp 101
  Last update from 10.10.10.2 on Serial1/0, 00:18:42 ago
  Routing Descriptor Blocks:
  * 10.10.10.2, from 10.10.10.2, 00:18:42 ago, via Serial1/0
    Route metric is 4339968, traffic share count is 1
    Total delay is 40000 microseconds, minimum bandwidth is 772 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1

```

Figura 3.45 Tabla de enrutamiento router Quito para alcanzar la int s1/0 en el router Londres

Desde el router Miami también podemos ver el camino más corto en el despliegue de rutas de su tabla de enrutamiento **Figura 3.46**.

```

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

Gateway of last resort is not set

D 192.168.30.0/24 [90/2172416] via 10.10.10.9, 01:18:46, Serial1/1
D 192.168.40.0/24 [90/2684416] via 10.10.10.1, 01:17:06, Serial1/0
C 192.168.20.0/24 is directly connected, FastEthernet0/0
  10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C   10.10.10.8/30 is directly connected, Serial1/1
D   10.10.10.12/30 [90/2681856] via 10.10.10.1, 01:17:07, Serial1/0
C   10.10.10.0/30 is directly connected, Serial1/0
D   10.0.0.0/8 is a summary, 01:18:52, Null0
C   10.10.10.16/30 is directly connected, Serial1/2
Miami#

```

Figura 3.46 Tabla de enrutamiento router Miami

Cálculo de la Métrica para EIGRP

EIGRP calcula su métrica agregando un valor a las diferentes características del enlace. Primero se debe buscar estas características en la interface con el comando show interface. En este ejemplo se calculara como EIGRP da el valor de 2172416 para establecerla como métrica hacia la red 192.168.30.0 desde el router Miami hacia el router Londres.

```

Serial1/1 is up, line protocol is up
Hardware is M8T-X.21
Internet address is 10.10.10.10/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:04, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec

```

Figura 3.47 Información de la interface s1/1Comando show interface

En la **Figura 3.47** se despliega la información de la interface del router Miami específicamente en la serial 1/1. Se ha marcado con rojo la información más importante para el cálculo de la métrica. EIGRP usa la siguiente fórmula para el cálculo:

$$\text{Bandwidth} = 10000000 \div \text{BW}_{\text{mínimo disponible}}$$

$$\text{Ancho de banda} = 10000000 \div 1158 = 8635.57$$

$$\text{Delay} = \text{DLY} \div 10$$

$$\text{Retraso} = 20000 \div 10 = 2000$$

$$\text{Metrica} = (\text{Ancho de Banda} + \text{Retraso}) \times 256 = 2170031$$

El valor calculado es aproximado ya que el ancho de banda no es el que se muestra en el comando show interface, pero para el ejemplo es válido, el ancho de banda mínimo se lo puede obtener dentro de los paquetes hello, el cual puede ser desglosado con el capturador de paquetes. **Figura 3.48**

```

EIGRP Parameters
  Type = 0x0001 (EIGRP Parameters)
  Size = 12 bytes
  K1 = 1
  K2 = 0
  K3 = 1
  K4 = 0
  K5 = 0

```

Figura 3.48 Wireshark desglose de un Paquete Hello

El proceso de selección de ruta de EIGRP es diferente a cualquier otro protocolo de enrutamiento, este usa las siguientes características:

Ancho de Banda BW (K1). El más pequeño ancho de banda entre el origen y el destino.

Retraso (K3). El retraso acumulado a lo largo de la ruta.

Confiabilidad (K4). Este valor está basado en los *keepalives* entre el origen y el destino, es escogido el peor

Carga K2. Este valor viene en bits por segundo y es escogido el peor, entre el origen y el destino.

Unidad de Transmisión Máxima MTU. El valor más pequeño en la ruta

La siguiente fórmula es usada si todos estos valores son encontrados apropiadamente:

$$\text{Métrica} = (K1 \times \text{bandwidth}) + [(K2 \times \text{bandwidth}) \div (256 \times \text{load})] + K3 \times \text{delay}$$

En la siguiente figura realizamos un test de conectividad en el router Caracas hacia las demás redes, el cual falla al intentar un ping, esto es debido a que el router Caracas se encuentra en un distinto sistema autónomo, este cambio se ha realizado para distinguir entre protocolos de enrutamiento interior RIP, OSPF, EIGRP entre otros, y protocolos de enrutamiento exterior como BGP, en la próxima práctica se hablará más al respecto.

```
Caracas>enable
Password:
Caracas#ping 192.168.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Caracas#ping 10.10.10.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Caracas#_
```

Figura 3.49 Prueba de conectividad desde router Caracas

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

Gateway of last resort is not set

192.168.10.0/28 is subnetted, 1 subnets
C    192.168.10.0 is directly connected, FastEthernet0/0
Caracas#_
```

Figura 3.50 Tablas de enrutamiento router Caracas

EIGRP hace uso de comandos para poder mostrar sus tablas de vecinos y tabla de topología, con los comandos show ip eigrp neighbors y show ip eigrp topology respectivamente **Figura 3.51** y **Figura 3.52**.

```
Quito#show ip eigrp neighbors
IP-EIGRP neighbors for process 101
H   Address                Interface      Hold Uptime    SRTT  RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
1   10.10.10.13              Se1/2         12 00:49:33    291 1746 0   7
0   10.10.10.2               Se1/0         14 00:49:33    244 1464 0  13
IP-EIGRP neighbors for process 100
```

Figura 3.51 Tablas de vecinos router Quito

En la tabla de topología encontramos los dos sistemas autónomos que reconoce el Router Quito, cada uno con su respectiva información de rutas. **Figura 3.52** También encontramos los códigos para los distintos estados por los que puede pasar una ruta dependiendo si hubiese cambio en la topología.

```

Quito#show ip eigrp topology
IP-EIGRP Topology Table for AS(101)/ID(192.168.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.8/30, 1 successors, FD is 2681856
   via 10.10.10.2 (2681856/2169856), Serial1/0
P 10.10.10.12/30, 1 successors, FD is 2169856
   via Connected, Serial1/2
P 10.10.10.0/30, 1 successors, FD is 2169856
   via Connected, Serial1/0
P 10.10.10.16/30, 1 successors, FD is 4339968
   via 10.10.10.2 (4339968/3827968), Serial1/0
P 192.168.40.0/24, 1 successors, FD is 2172416
   via 10.10.10.13 (2172416/28160), Serial1/2
P 192.168.30.0/24, 1 successors, FD is 2684416
   via 10.10.10.2 (2684416/2172416), Serial1/0
P 192.168.20.0/24, 1 successors, FD is 2172416
   via 10.10.10.2 (2172416/28160), Serial1/0
IP-EIGRP Topology Table for AS(100)/ID(192.168.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/28, 1 successors, FD is 28160
   via Connected, FastEthernet0/0

```

Figura 3.52 Tablas de topología router Quito

Existe un comando muy útil para ver los procesos en un router, además sirve para diagnosticar problemas, en las anteriores prácticas no se usó este comando ya que este puede ser reemplazado por el capturador de paquetes Wireshark que es mucho más detallado.

Para activar todo el sistema de diagnóstico se usa **debug all** y para desactivarlo **no debug all**, en esta práctica para ser más específico se usará **debug eigrp packets**, este comando desplegará el intercambio de paquetes. En la **Figura 3.53** remarcado en rojo se encuentra el intervalo de paquetes *hello* para la interface serial 1/2, se puede apreciar el envío del paquete cada cinco segundos el cual es configurado por defecto en EIGRP.

```

15:51:59.915: EIGRP: Sending HELLO on Serial1/2
15:51:59.915: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
15:52:02.055: EIGRP: Sending HELLO on FastEthernet0/0
15:52:02.059: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
15:52:02.371: EIGRP: Sending HELLO on Serial1/0
15:52:02.375: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
15:52:03.027: EIGRP: Received HELLO on Serial1/0 nbr 10.10.10.2
15:52:03.027: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
15:52:03.423: EIGRP: ddb not configured on FastEthernet0/0
15:52:04.039: EIGRP: Received HELLO on Serial1/2 nbr 10.10.10.13
15:52:04.039: AS 101, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
15:52:04.651: EIGRP: Sending HELLO on Serial1/2

```

Figura 3.53 Comando Debug router Quito

3.8.5.1 Verificación de Paquetes

Observaremos a continuación el comportamiento de EIGRP cuando la interface serial 1/0 del router Londres es apagada **Figura 3.54**.

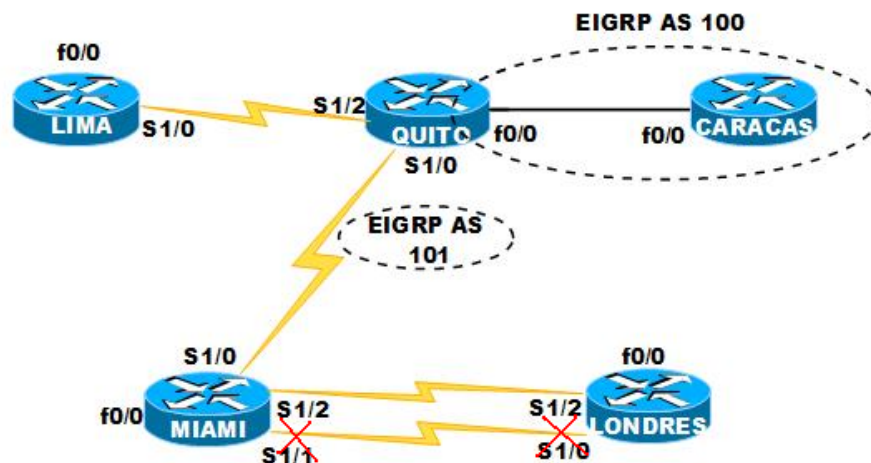


Figura 3.54 Esquema para comprobación de ruta y resolución de Dual

Antes de apagar la interface desde la consola de comandos Dynagen, capturamos los paquetes desde la interface s1/0 del router Miami para observar cual camino toma el paquete desde Londres hacia la red 10.10.10.1

=> **capture Miami s1/0 miami.cap HDLC**

A continuación, abrimos el archivo Miami.cap el cual indica los procesos en la interface s1/0 del router Miami. **Figura 3.55**.

En la **Figura 3.55** del capturador podemos ver el envío de los paquetes desde el Router Londres hacia la interface 10.10.10.1 por la interfaz 10.10.10.9, debido a que esta posee una métrica menor que su ruta hermana 10.10.10.18 en la int s1/2.

32.557000	10.10.10.1	224.0.0.10	EIGRP	Hello
34.361000	N/A	N/A	SLARP	Line keepalive, out
34.649000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
34.705000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
34.785000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
34.846000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
34.927000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
34.939000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
34.964000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
34.982000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
35.001000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
35.066000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
35.343000	10.10.10.2	224.0.0.10	EIGRP	Hello

Figura 3.55 Verificación Ping desde Router Londres a Router Quito

Después de haber realizado esto, se procede a apagar la interface s1/0 del router Londres, en la **Figura 3.56** podemos examinar el proceso que realiza EIGRP para recalcular las rutas usando los paquetes de operación EIGRP.

```
Londres#config ter
Londres(config)#int s1/0
Londres(config-int)#shutdown
```

74.564000	10.10.10.1	224.0.0.10	EIGRP	Hello
76.450000	10.10.10.2	10.10.10.1	EIGRP	Update
76.680000	10.10.10.1	10.10.10.2	EIGRP	Acknowledge
76.778000	10.10.10.1	10.10.10.2	EIGRP	query
76.860000	10.10.10.2	10.10.10.1	EIGRP	Acknowledge
76.971000	10.10.10.2	10.10.10.1	EIGRP	Reply
77.055000	10.10.10.1	10.10.10.2	EIGRP	Acknowledge
77.534000	10.10.10.2	224.0.0.10	EIGRP	Hello
78.964000	N/A	N/A	SLARP	Line keepal

Figura 3.56 Esquema para comprobación de ruta y resolución de Dual

Seguimiento del proceso

75.45 Desde la interfaz 10.10.10.2 se envía un Update unicast, para avisar que ha habido un cambio en la topología.

76.68 Desde la interfaz 10.10.10.1 se envía un acknowledge que son una especie de paquetes Hello para dar a conocer que han llegado paquetes updates, queries y replies.

76.77 Desde 10.10.10.1 se envía un Querie el cual indica que se esta haciendo un cálculo de ruta y que no se puede encontrar un sucesor factible, este paquete se envía a sus vecinos preguntando si estos poseen un sucesor factible hacia ese destino. Los Queries son siempre multicast.

76.97 Desde 10.10.10.2 se envía un Replie que indica que ha llegado un paquete Querie. Estos son enviados en unicast hacia la fuente original del paquete Querie.

Luego de este proceso la nueva ruta es tomada como factible, y realizamos un ping en la **Figura 3.57** encontramos el envío del paquete por la otra ruta 10.10.10.18 la cual posee una métrica más grande pero se encuentra activa.

130.323000	10.10.10.1	224.0.0.10	EIGRP	Hello
131.919000	10.10.10.18	10.10.10.1	ICMP	Echo (ping) request
132.013000	10.10.10.1	10.10.10.18	ICMP	Echo (ping) reply
132.113000	10.10.10.18	10.10.10.1	ICMP	Echo (ping) request
132.138000	10.10.10.1	10.10.10.18	ICMP	Echo (ping) reply
132.174000	10.10.10.18	10.10.10.1	ICMP	Echo (ping) request
132.205000	10.10.10.1	10.10.10.18	ICMP	Echo (ping) reply
132.345000	10.10.10.18	10.10.10.1	ICMP	Echo (ping) request
132.376000	10.10.10.1	10.10.10.18	ICMP	Echo (ping) reply
132.487000	10.10.10.18	10.10.10.1	ICMP	Echo (ping) request
132.552000	10.10.10.1	10.10.10.18	ICMP	Echo (ping) reply

Figura 3.57 Esquema para comprobación de ruta y resolución de Dual

Ya en la **Figura 3.58** volvemos a activar la interfaz del router Londres, otra vez se envían updates para hacer conocer a sus vecinos y DUAL aplica su algoritmo, como resultado la ruta con la métrica menor es tomada para enviar los paquetes mientras que la otra ruta queda de respaldo.

355.169000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
355.216000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
355.359000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
355.401000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
355.503000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
355.529000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
355.599000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
355.609000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
355.726000	10.10.10.9	10.10.10.1	ICMP	Echo (ping) request
355.732000	10.10.10.1	10.10.10.9	ICMP	Echo (ping) reply
357.921000	10.10.10.2	224.0.0.10	EIGRP	Hello

Figura 3.58 Esquema para comprobación de ruta y resolución de Dual

3.9 PRÁCTICA 5

Tema: CONFIGURACIÓN DE BGP -BORDER GATEWAY PROTOCOL-

3.9.1 OBJETIVOS

- ✓ Configurar el protocolo de enrutamiento BGP en la topología, usando EBGp entre sistemas autónomos e IBGP *full mesh* dentro de cada sistema autónomo.
- ✓ Verificar conectividad entre los dispositivos.
- ✓ Analizar los paquetes BGP con el capturador
- ✓ Reconocer las principales características del enrutamiento dinámico BGP.
- ✓ Comprender las distintas formas por las cuales BGP atribuye la elección de mejor ruta.

3.9.2 MARCO TEÓRICO.

Los protocolos de enrutamiento externo son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de enrutamiento interno la prioridad era buscar rutas óptimas atendiendo únicamente al criterio de minimizar la ‘distancia’ medida en términos de la métrica elegida para la red.

La selección de rutas entre sistemas autónomos plantea un problema diferente, ya que la cuestión no se reduce a la selección de la ruta óptima sino que se debe atender a criterios externos de tipo político, económico, administrativo, etc...

EBGP y IBGP

Si un AS *-Autonomous System-* tiene múltiples routers BGP, podrían ser usados para ofrecer un servicio de tránsito para otros AS. Cuando BGP está funcionando entre dos o más AS lo llamamos exterior BGP (EBGP). Cuando BGP está funcionando en el mismo AS lo llamamos IBGP.

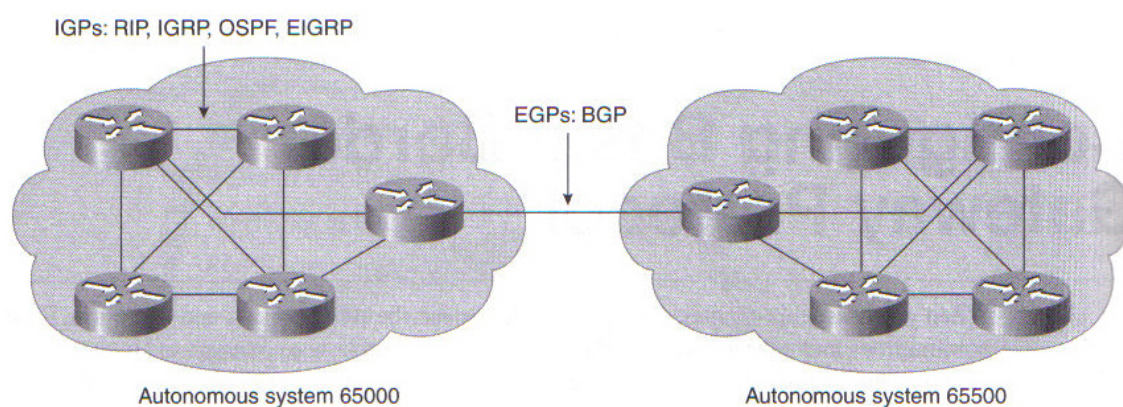


Figura 3.59 Esquema de red con dos sistemas autónomos

FUNCIONES DE BGP.

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de enrutamiento, llamados pasarelas, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando TCP.:

- ✓ OPEN
- ✓ UPDATE
- ✓ KEEPALIVE
- ✓ NOTIFICATION

BGP supone tres procedimientos funcionales:

- ✓ Adquisición de vecino.
- ✓ Detección de vecino alcanzable.
- ✓ Detección de red alcanzable.

OPERACIÓN DE BGP

Dos dispositivos de encaminamiento se considera que son vecinos si están en la misma subred. Si los dos dispositivos de encaminamiento están en distintos sistemas autónomos, podrían desear intercambiar información. Para este cometido es necesario

realizar primero el proceso de adquisición de vecino. Se requiere un mecanismo formal de encaminamiento ya que alguno de los dos vecinos podría no querer participar. Existirán situaciones en las que un vecino no desee intercambiar información esto se puede deber a múltiples factores como por ejemplo que este sobresaturado y entonces no quiere ser responsable del tráfico que llega desde fuera del sistema.

En el protocolo de **adquisición de vecino**, un dispositivo envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no indica cómo puede saber un dispositivo la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones se tratan en el momento de establecer la configuración del sistema o por una intervención activa del gestor de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo envía al otro un mensaje OPEN. Si el otro dispositivo acepta la relación, envía un mensaje de KEEPALIVE.

Una vez establecida la relación de vecino, se utiliza el procedimiento de **detección de vecino alcanzable** para mantener la relación. Este procedimiento consiste en enviarse entre los dos vecinos periódicamente mensajes de KEEPALIVE para asegurarse de que la relación sigue establecida.

El último procedimiento especificado por BGP es la detección de red alcanzable. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para llegar hasta esa red. Siempre que se realiza un cambio en esa base de datos, el dispositivo de almacenamiento envía un mensaje de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.

MENSAJES BGP.

Los mensajes BGP tienen una cabecera común de 19 octetos que contiene los siguientes tres campos:

- ✓ *Marcador*: reservado para autenticación. El emisor puede insertar un valor en este campo para permitir al receptor comprobar la veracidad del emisor.
- ✓ *Longitud*: longitud del mensaje en octetos.

✓ *Tipo*: tipo de mensaje: OPEN, UPDATE, NOTIFICATION, KEEPALIVE.

MENSAJE OPEN.

Para adquirir un vecino, el router abre primero una conexión TCP con el dispositivo vecino y después envía un mensaje OPEN. Este mensaje identifica al AS al que pertenece el emisor y suministra la dirección IP del dispositivo de encaminamiento.

En la siguiente figura se muestra el formato del mensaje OPEN:

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Version	1
AS	2
Tiempo permanencia	2
Id de BGP	4
Long Opciones	1
Opciones	Variable

Tabla 3.7 Mensaje OPEN

Versión: Indica la versión del protocolo del mensaje. La versión actual es 4.

AS: Identifica al sistema autónomo del emisor del mensaje.

Tiempo de permanencia: Indica el tiempo de que propone el emisor como Hold Time.

Identificador de BGP: Identifica al BGP emisor.

MENSAJE KEEPALIVE.

El mensaje KEEPALIVE consta solo de la cabecera. Cada dispositivo de mantenimiento envía regularmente estos mensajes para evitar que expire el temporizador mantenimiento.

MENSAJE UPDATE.

Un mensaje UPDATE puede contener uno o dos tipos de información. Consideremos primero la información sobre una ruta particular a través de la red, esto implica tres campos, campo de información sobre la capacidad de alcanzar la capa de red (NLRI), campo de longitud de los atributos del camino total, y el campo de los atributos de camino. El campo NLRI contiene una lista de identificadores de redes que se pueden alcanzar por esta ruta. Cada red se identifica por su dirección IP, que es en realidad una parte de la dirección IP completa.

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Long. Rutas no factibles	2
Rutas Retiradas	Variable
Long Total atributos de camino	2
Atributos de camino	Variable
Inf de accesibilidad de la capa de red	Variable

Tabla 3.8 Mensaje Update

El campo llamado “atributos de camino” contiene una lista de atributos que se aplican a esta ruta particular. Los atributos definidos son los siguientes:

Origin: Indica si la información fue generada por un protocolo de dispositivo de encaminamiento interior IBGP o exterior EBGP.

Path AS: Una lista de los AS que son atravesados por la ruta.

Next hop: Dirección IP del dispositivo de encaminamiento frontera que se debe usar como siguiente salto para alcanzar los destinos indicados.

Local Preference: Usado por un dispositivo de encaminamiento para informar a otros dispositivos de encaminamiento dentro del mismo AS de su grado de preferencia para salir hacia una ruta particular, siempre se escoge el mayor valor, el valor por default en Routers Cisco es 100

MED Multi exit discriminator: También llamada métrica, a diferencia de *local preference attribute* se usa para comunicar información sobre las

rutas hacia otros AS. Un menor valor siempre es escogido como el mejor, el valor por default en Routers Cisco es 100

Agregado_atómico, Agente_unión: Estos dos campos implementan el concepto de unión de rutas. En esencia, un conjunto de redes y su espacio de direcciones correspondiente se pueden organizar jerárquicamente, o como un árbol. En este caso las direcciones de las redes se estructuran en dos o más partes. Todas las redes de un subárbol comparten una dirección internet parcial común. Usando esta dirección parcial común, la cantidad de información que se debe comunicar en NLRI se puede reducir significativamente.

MENSAJE NOTIFICATION.

Se envían cuando se detecta algún tipo de error. En la siguiente figura se muestra el formato del mensaje NOTIFICATION:

Campo	Long (bytes)
Marcador	16
Longitud	2
Tipo	1
Codigo de Error	1
Subcodigo Error	1
Datos	Variable

Tabla 3.9 Mensaje de Notificación

El subcódigo de error nos da más información sobre el error, los posibles códigos son los siguientes:

Message Header Error subcodes:
1 - Connection Not Synchronized.
2 - Bad Message Length.
3 - Bad Message Type.

Tabla 3.10 Subcódigos de Error

Open Message Error subcodes
1 - Unsupported Version Number.
2 - Bad Peer AS.
3 - Bad BGP Identifier.
4 - Unsupported Authentication Code.
5 - Authentication Failure.
6 - Unacceptable Hold Time.

Tabla 3.11 Subcódigos de Error

UPDATE Message Error subcodes:	
1	Malformed Attribute List.
2	Unrecognized Well-known Attribute.
3	Missing Well-known Attribute.
4	Attribute Flags Error.
5	Attribute Length Error.
6	Invalid ORIGIN Attribute
7	AS Routing Loop.
8	Invalid NEXT_HOP
9	Optional Attribute Error.
10	Invalid Network Field.
11	Malformed AS_PATH.

Tabla 3.12 Subcódigos de Error

3.9.3 ESQUEMA DE LA RED

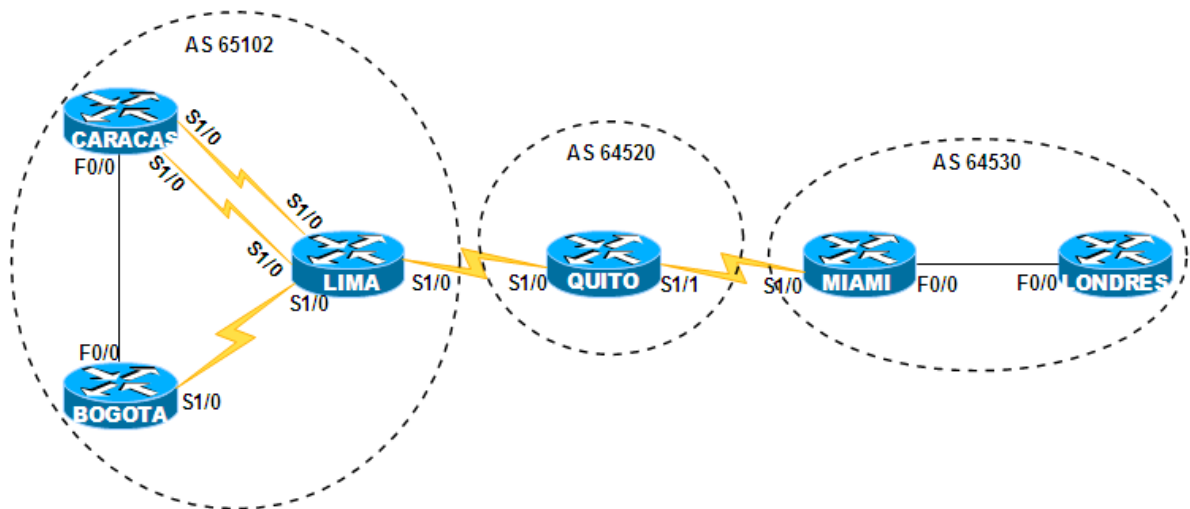


Figura 3.60 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface	BGP Tipo
Quito	DTE	10.2.1.2	255.255.255.0	S1/0	EBGP
	DTE	10.1.1.2	255.255.255.0	S1/1	EBGP
		192.168.3.1	255.255.255.0	f0/0	EBGP
Lima	DCE	10.2.1.1	255.255.255.0	S1/0	EBGP
	DCE	192.168.1.17	255.255.255.240	S1/1	IBGP
	DCE	192.168.1.33	255.255.255.240	S1/2	IBGP
	DCE	192.168.1.49	255.255.255.240	S1/3	IBGP
Caracas	DTE	192.168.1.18	255.255.255.240	S1/0	IBGP
	DTE	192.168.1.34	255.255.255.240	S1/1	IBGP
		192.168.1.65	255.255.255.240	f0/0	IBGP
Bogota	DTE	192.168.1.50	255.255.255.240	S1/0	IBGP
		192.168.1.66	255.255.255.240	f0/0	IBGP
Miami	DCE	10.1.1.1	255.255.255.0	S1/0	EBGP
		192.168.2.49	255.255.255.240	f0/0	IBGP
Londres		192.168.2.50	255.255.255.240	f0/0	IBGP

Tabla 3.13 Datos de la Red WAN

3.9.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

PRIMERA PARTE: CONFIGURACIÓN EBGP

Los comandos a continuación presentan la configuración de EBGP entre sistemas autónomos, en este caso, al router Quito se le da a conocer de sus vecinos y su identificación de sistema autónomo, y así respectivamente en los Routers Lima y Miami.

Quito#**config ter**

Quito(config)#**router bgp 64520**

Quito(config-router)#**neighbor 10.2.1.1 remote-as 65102**

Quito(config-router)#**neighbor 10.1.1.1 remote-as 64530**

El siguiente comando da a conocer a sus vecinos de la existencia de una red con su respectiva máscara.

Quito(config-router)#**network 192.168.3.0 mask 255.255.255.0**

Quito(config-router)#**exit**

Lima#**config ter**

Lima (config)#**router bgp 65102**

Lima (config-router)#**neighbor 10.2.1.2 remote-as 64520**

Lima (config-router)#**network 192.168.1.0 mask 255.255.255.0**

Lima (config-router)#**exit**

Miami#**config ter**

Miami(config)#**router bgp 64530**

Miami(config-router)#**neighbor 10.1.1.2 remote-as 64520**

Miami(config-router)#**network 192.168.2.0 mask 255.255.255.0**

Miami(config-router)#**exit**

SEGUNDA PARTE: CONFIGURACIÓN IBGP

Caracas#**config ter**

Caracas(config)#**router bgp 65102**

Caracas(config-router)#**neighbor 192.168.1.17 remote-as 65102**

Caracas(config-router)#**neighbor 192.168.1.33 remote-as 65102**

Caracas(config-router)#**neighbor 192.168.1.66 remote-as 65102**

Caracas(config-router)#**network 192.168.1.0 mask 255.255.255.0**

Caracas(config-router)#**exit**

Bogota#**config ter**

Bogota (config)#**router bgp 65102**

Bogota (config-router)#**neighbor 192.168.1.49 remote-as 65102**

Bogota (config-router)#**neighbor 192.168.1.65 remote-as 65102**

Bogota (config-router)#**network 192.168.1.0 mask 255.255.255.0**

Bogota (config-router)#**exit**

Lima#**config ter**

```
Lima(config)#router bgp 65102
Lima (config-router)#neighbor 192.168.1.18 remote-as 65102
Lima (config-router)#neighbor 192.168.1.34 remote-as 65102
Lima (config-router)#neighbor 192.168.1.50 remote-as 65102
Lima (config-router)#network 192.168.1.0 mask 255.255.255.0
Lima (config-router)#exit
```

```
Londres#config ter
Londres (config)#router bgp 64530
Londres (config-router)#neighbor 192.168.2.49 remote-as 65102
Londres (config-router)#network 192.168.2.0 mask 255.255.255.0
Londres (config-router)#exit
```

```
Miami#config ter
Miami(config)#router bgp 64530
Miami(config-router)#neighbor 192.168.2.50 remote-as 64530
Miami(config-router)#network 192.168.2.0 mask 255.255.255.0
Miami(config-router)#exit
```

3.9.5 VERIFICACIÓN DE BGP

Desde el router Lima realizamos pruebas de conectividad ping hacia las redes dentro del sistema autónomo. **Figura 3.61**

```
Lima#ping 192.168.1.65
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.65, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/118/184 ms
Lima#ping 192.168.1.66
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/200/300 ms
```

Figura 3.61 Prueba de Conectividad Ping

De nuevo desde el router Lima presentamos su tabla de enrutamiento **Figura 3.62**, la rutas BGP se muestran con la letra B, dependiendo de su distancia administrativa

podemos saber si es BGP interno o externo respectivamente, en la pantalla encontramos la red Ethernet que une el router Caracas con el router Bogotá, las cuales son alcanzables por la vía 192.168.1.18 en este caso BGP interno, para las redes Ethernet del Router Quito y Miami su distancia administrativa es de veinte esto indica BGP externo

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

Gateway of last resort is not set

10.0.0.0/16 is subnetted, 1 subnets
C 10.2.0.0 is directly connected, Serial1/0
192.168.1.0/24 is variably subnetted, 5 subnets, 2 masks
B 192.168.1.64/28 [200/0] via 192.168.1.18, 00:01:09
C 192.168.1.32/28 is directly connected, Serial1/2
C 192.168.1.48/28 is directly connected, Serial1/3
B 192.168.1.0/24 [200/0] via 0.0.0.0, 00:01:09, Null0
C 192.168.1.16/28 is directly connected, Serial1/1
B 192.168.2.0/24 [20/0] via 10.2.1.2, 00:01:04
B 192.168.3.0/24 [20/0] via 10.2.1.2, 00:01:30
```

Figura 3.62 Tabla de enrutamiento router Lima

El comando *show ip bgp summary* nos ayuda a verificar la relación entre vecinos usando BGP, en la siguiente pantalla y desde el router Lima encontramos información como el número de sistema autónomo al cual pertenece el router, el ID del router y las redes vecinas, en este caso las tres redes hacia los Routers Caracas y Bogotá y una hacia otro Sistema Autónomo en el router Quito.

```
Lima#show ip bgp summary
BGP router identifier 192.168.1.49, local AS number 65102
BGP table version is 6, main routing table version 6
4 network entries using 468 bytes of memory
6 path entries using 312 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1448 total bytes of memory
BGP activity 4/0 prefixes, 6/0 paths, scan interval 60 secs

Neighbor      U      AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.2.1.2      4  64520      8         6         6    0    0  00:02:13      2
192.168.1.18  4  65102      6         8         6    0    0  00:02:04      1
192.168.1.34  4  65102      6         8         6    0    0  00:02:01      1
192.168.1.50  4  65102      6         8         6    0    0  00:02:22      1
```

Figura 3.63 Entradas en el router Lima

Otro comando muy importante usado para el análisis en BGP es *show ip bgp*, este desplega información de todas las redes a las que se puede alcanzar con su respectivo

siguiente salto. En la **Figura 3.64** se aplica el comando desde el router Caracas, fíjese en las redes y su respectivo siguiente salto por el cual puede llegar.

En el recuadro rojo encontramos la red 192.168.3.0 la cual es alcanzable por la vía 10.2.1.2, esta información es errónea, esta es una de las características en el comportamiento de BGP, cuando el router Quito notifica de su red, envía su interface como siguiente salto y al pasar por el router Lima ésta la envía con la misma información, dejando conocer al router Caracas que el siguiente salto sigue siendo el de Quito, para corregir este problema es necesario configurar al router Lima notificar que la red es alcanzable con su propio siguiente salto o interface.

```
Caracas#show
*Feb 6 10:59:30.663: %SYS-5-CONFIG_I: Configured from console by consoleip bgp
BGP table version is 5, local router ID is 192.168.1.65
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
* i192.168.1.0      192.168.1.33      0      100      0 i
*>i                192.168.1.17      0      100      0 i
* i192.168.1.64/28  192.168.1.66      0      100      0 i
*>                0.0.0.0           0              32768 i
* i192.168.2.0     10.2.1.2          0      100      0 64520 64530 i
* i                10.2.1.2          0      100      0 64520 64530 i
* i192.168.3.0     10.2.1.2          0      100      0 64520 i
* i                10.2.1.2          0      100      0 64520 i
```

Figura 3.64 Redes router Caracas

Lima#**config ter**

Lima(config)#**router bgp 65102**

Lima(config-router)# **neighbor 192.168.1.18 next-hope-self**

```
Caracas#show ip bgp
BGP table version is 13, local router ID is 192.168.1.65
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
* i192.168.1.0      192.168.1.33      0      100      0 i
*>i                192.168.1.17      0      100      0 i
* i192.168.1.64/28  192.168.1.66      0      100      0 i
*>                0.0.0.0           0              32768 i
* i192.168.2.0     192.168.1.33      0      100      0 64520 64530 i
*>i                192.168.1.17      0      100      0 64520 64530 i
* i192.168.3.0     192.168.1.33      0      100      0 64520 i
*>i                192.168.1.17      0      100      0 64520 i
```

Figura 3.65 Redes actualización Router Caracas

En la **Figura 3.65**, ya se ha actualizado la tabla de enrutamiento y encontramos las rutas adecuadas para llegar hacia la red en el router Quito, este comportamiento es general en BGP, esta pequeña configuración se debe realizar para que exista conectividad entre redes de este tipo de esquema de red, no así en redes tipo Ethernet ya que en estas sí se notifica con el salto correspondiente.

Desde el router Miami aplicamos también esta configuración ya que esta posee el mismo problema se puede realizar pruebas ping detectar estos errores o simplemente presentando la tabla de enrutamiento

```
Miami#config ter
```

```
Miami(config)#router bgp 64530
```

```
Miami(config-router)# neighbor 192.168.2.50 next-hop-self
```

Para desplegar información de vecinos BGP se usa el comando `show ip bgp neighbor`, en la **Figura 3.66** encontramos incluso información de los mensajes enviados y recibidos por el protocolo de enrutamiento y sus notificaciones, también número de AS y más información sobre los paquetes.

```
Quito#show ip bgp neighbor
BGP neighbor is 10.1.1.1, remote AS 64530, external link
BGP version 4, remote router ID 192.168.2.49
BGP state = Established, up for 00:48:29
Last read 00:00:58, last write 00:00:30, hold time is 180, keepalive interval
is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received<old & new>
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

```

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	3	1
Keepalives:	50	51
Route Refresh:	0	0
Total:	54	53

```
Default minimum time between advertisement runs is 30 seconds
```

Figura 3.66 Presentación de Vecinos Router Quito

3.9.5.1 Verificación de Paquetes

Desde la interface s1/1 del router Lima se capturará paquetes para ver el funcionamiento de BGP y sus distintos mensajes y paquetes de notificación de rutas y redes, para mayor estudio se pueden producir fallas en la red, de igual forma para observar el comportamiento del protocolo.

>capture Lima s1/1 lima.cap HDLC

192.168.1.17	192.168.1.18	TCP	25579 > bgp [SYN] Seq=0 Len=0 MSS=14
192.168.1.18	192.168.1.17	TCP	bgp > 25579 [SYN, ACK] Seq=0 Ack=1 w
192.168.1.17	192.168.1.18	TCP	25579 > bgp [ACK] Seq=1 Ack=1 win=16
192.168.1.17	192.168.1.18	BGP	OPEN Message
192.168.1.18	192.168.1.17	BGP	OPEN Message, KEEPALIVE Message
192.168.1.17	192.168.1.18	BGP	KEEPALIVE Message
192.168.1.18	192.168.1.17	TCP	bgp > 25579 [ACK] Seq=65 Ack=65 win=
N/A	N/A	SLARP	Line keepalive, outgoing sequence 2,
N/A	N/A	CDP	Device ID: Lima Port ID: Serial1/1
N/A	N/A	CDP	Device ID: Lima Port ID: Serial1/1
N/A	N/A	SLARP	Line keepalive, outgoing sequence 6,
N/A	N/A	SLARP	Line keepalive, outgoing sequence 3,
N/A	N/A	SLARP	Line keepalive, outgoing sequence 7,
N/A	N/A	SLARP	Line keepalive, outgoing sequence 4,
N/A	N/A	SLARP	Line keepalive, outgoing sequence 8,
192.168.1.17	192.168.1.18	BGP	KEEPALIVE Message
192.168.1.18	192.168.1.17	BGP	KEEPALIVE Message
192.168.1.17	192.168.1.18	BGP	UPDATE Message, UPDATE Message

Figura 3.67 Presentación de Paquetes Lima

En la **Figura 3.67** se realiza el dialogo entre las interfaces del router Caracas y el router Lima, con los distintos paquetes que usa BGP, el cual usa TCP como su protocolo de transporte el cual provee conexión orientada hacia la confiabilidad de entrega.

Después que TCP es establecido, el primer mensaje enviado por cada lado es el Open message, si este mensaje es aceptado se envía un Keepalive confirmando el regreso del Open anterior. Luego de esta confirmación se envían Updates y Keepalives de intercambio. En un inicio BGP intercambia su entera tabla de enrutamiento y luego poco a poco envía actualizaciones incrementales para hacer cambios en las tablas de enrutamiento. Los Keepalives son enviados para asegurar que la conexión existe entre pares BGP.

Los mensajes de notificación se envían solo cuando existen errores o en condiciones especiales. También los mensajes de actualización -updates- contienen

información de un solo camino, múltiples caminos requerirán múltiples mensajes, con sus respectivos atributos -tipos de mensajes BGP Marco Teórico-

Todos los protocolos de enrutamiento vistos se implementan dentro de varias tecnologías WAN, estas tecnologías han ido evolucionando con el tiempo y existen varias de las cuales hablamos ya en el primer capítulo, HDLC es un entramado que garantiza entrega confiable de datos, en el siguiente capítulo se estudiará los protocolos que hacen posible la conmutación serial para conexiones de este tipo.

CAPÍTULO 4

PRÁCTICAS DE ENCAPSULAMIENTO WAN

En este capítulo se realizara una práctica completa acerca del protocolo que hace posible la transmisión de datos entre nodos punto a punto, HDLC es un grupo de protocolos que trabajan en la capa enlace del modelo OSI el cual hace posible el envío de paquetes, PPP o conocido como Protocolo Punto a Punto es usado como transporte de datagramas sobre enlaces punto a punto. Este protocolo es usado en routers, los cuales lo usan para soporte y generación de tramas de niveles superiores. Este capítulo muestra una práctica con un análisis detallado de este tipo de encapsulación, además se usara el protocolo de enrutamiento EIGRP para el descubrimiento de rutas.

4.1 PRÁCTICA 6

Tema: CONFIGURACIÓN DE PPP

4.1.1 OBJETIVOS

- ✓ Configurar las direcciones IP del esquema de la red.
- ✓ Configurar el protocolo PPP en las interfaces seriales de acuerdo a la Tabla de configuración.

- ✓ Configurar y comprobar el modo de autenticación PPP CHAP en una de las interfaces
- ✓ Comparar el encapsulamiento HDLC y PPP en diferentes interfaces.
- ✓ Verificar conectividad y envío de paquetes.
- ✓ Configurar EIGRP en la red, para analizar su desempeño junto a PPP.

4.1.2 MARCO TEÓRICO.

En el capítulo I se hablo acerca de PPP, la fase de autenticación de una sesión PPP es opcional. Una vez establecido el enlace y seleccionado el protocolo de autenticación, se puede autenticar el dispositivo par. La autenticación, si se utiliza, se lleva a cabo antes de que comience la fase de configuración del protocolo de la capa de red.

Proceso de encapsulamiento y autenticación PPP

Cuando se utiliza el comando **encapsulation ppp**, la autenticación CHAP o PAP se puede agregar de forma optativa. Si no se especifica ninguna clase de autenticación, la sesión PPP comienza de inmediato. Si se requiere de autenticación, el proceso da los siguientes pasos:

- Se determina el método de autenticación.
- Se revisa la base de datos local o el servidor de seguridad, que tiene una base de datos de contraseñas y nombres de usuario, para verificar que el nombre de usuario y la contraseña dados concuerdan con alguna entrada.
- El proceso verifica la respuesta de autenticación que envía la base de datos local. Si la respuesta es positiva, se inicia la sesión PPP. Si es negativa, se termina la sesión.

Las opciones de autenticación requieren que la parte del enlace que realiza la llamada introduzca la información de autenticación. Esto ayuda a garantizar que el usuario tenga el permiso del administrador de la red para efectuar la llamada. Los routers pares intercambian mensajes de autenticación.

Al configurar la autenticación PPP, el administrador de la red puede seleccionar el Protocolo de autenticación de contraseña (PAP) o el Protocolo de autenticación de intercambio de señales (CHAP).

Por lo general, el protocolo de preferencia es CHAP.

Protocolo de autenticación de contraseña (PAP)

PAP ofrece un método sencillo para que un nodo remoto establezca su identidad, mediante el intercambio de señales de dos vías. Una vez que se ha completado la fase de establecimiento del enlace PPP, el nodo remoto envía el conjunto de nombre de usuario/contraseña por el enlace repetidas veces hasta que se acusa recibo de la autenticación o la conexión se termina.

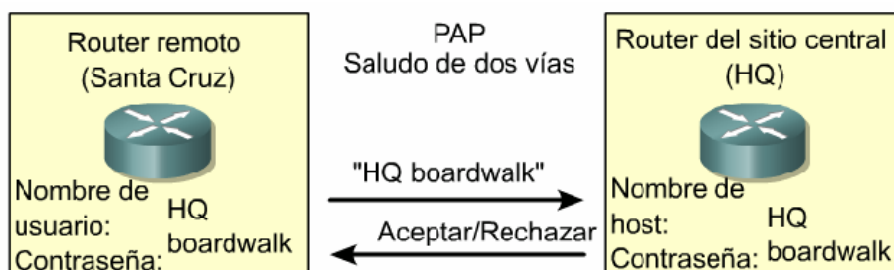


Figura 4.1 Autenticación de dos vías PAP

PAP no es un protocolo de autenticación sólido. Las contraseñas se envían por el enlace en texto no cifrado, y no hay protección contra la reproducción o los intentos de descubrimiento mediante intentos reiterados de ensayo y error. El nodo remoto tiene control de la frecuencia y la temporización de los intentos de conexión.

Protocolo de autenticación de intercambio de señales (CHAP)

CHAP se utiliza al iniciar un enlace y verifica, de forma periódica, la identidad del nodo remoto por medio de un intercambio de señales de tres vías. CHAP se realiza al establecer el enlace inicial y se repite durante el tiempo que dure el enlace.

Después de completar la fase de establecimiento del enlace PPP, el host envía un mensaje de comprobación al nodo remoto. El nodo remoto responde con un valor calculado mediante la función hash de una vía que, en general, es Message Digest 5 (MD5). Esta respuesta se basa en la contraseña y el mensaje de comprobación. El router local verifica la respuesta contra su propio cálculo del valor hash esperado. Si los valores concuerdan, se acusa recibo de la autenticación; de lo contrario, la conexión termina de inmediato.

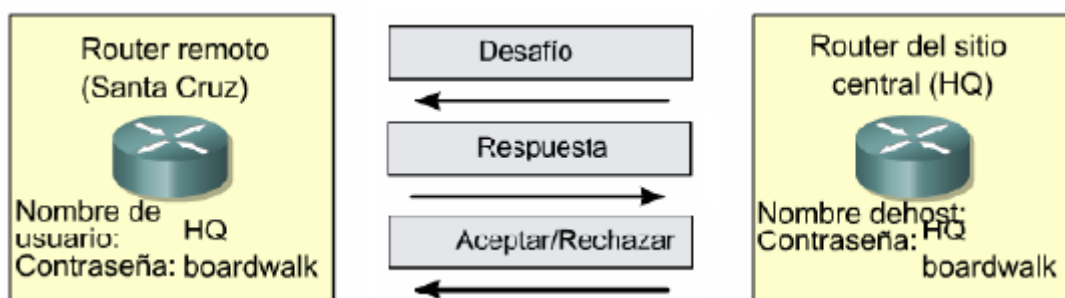


Figura 4.2 Autenticación de tres vías CHAP

CHAP brinda protección contra los intentos de reproducción a través del uso de un valor de comprobación variable que es exclusivo e impredecible. Como la comprobación es única y aleatoria, el valor hash resultante también será único y aleatorio. El uso de comprobaciones reiteradas tiene como fin limitar el tiempo de exposición ante cualquier ataque. El router local o un servidor de autenticación de terceros tiene el control de la frecuencia y la temporización de las comprobaciones.

PPP es muy fácil de configurar solo activamos el encapsulamiento en las interfaces donde se requiera el protocolo.

```
Router#configure terminal
```

```
Router(config)#interface serial 0/0
```

```
Router(config-if)#encapsulation ppp
```

La compresión de software de punto a punto puede configurarse en las interfaces seriales que utilizan encapsulamiento PPP. La compresión se ejecuta en el software y puede afectar el rendimiento del sistema de forma significativa. No se recomienda la compresión si la mayor parte del tráfico está compuesto por archivos comprimidos (2).

Los siguientes comandos sirven para monitorear los datos que se pasan al enlace y para evitar la formación de bucles en las tramas:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp quality percentage
```

Los siguientes comandos ejecutan el equilibrio de las cargas en múltiples enlaces:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink
```

4.1.3 ESQUEMA DE LA RED

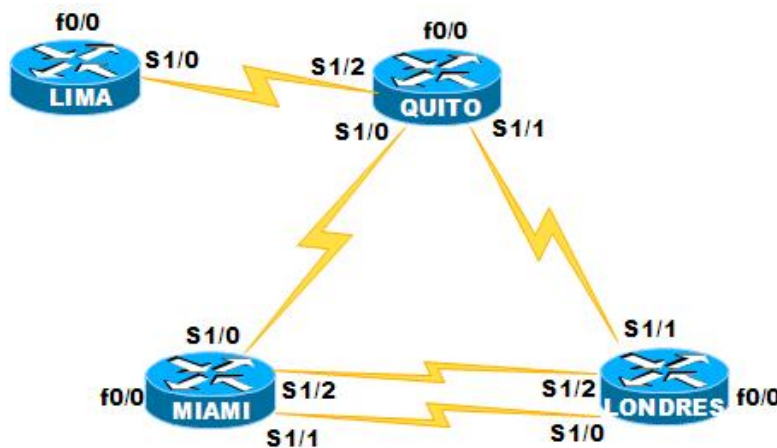


Figura 4.3 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface	Encapsulacion	Autenticacion	Password
Lima	DTE	10.10.10.13	255.255.255.252	S1/0	PPP	-	
		192.168.40.1	255.255.255.0	f0/0	HDLC Ethernet	-	
Quito	DCE	10.10.10.1	255.255.255.252	S1/0	PPP	CHAP	telecomunicaciones
		10.10.10.5	255.255.255.252	S1/1	HDLC	-	
		10.10.10.14	255.255.255.252	S1/2	PPP	-	
Miami	DTE	192.168.10.1	255.255.255.0	f0/0	HDLC Ethernet	-	
		10.10.10.2	255.255.255.252	S1/0	PPP	CHAP	telecomunicaciones
		10.10.10.10	255.255.255.252	S1/1	HDLC	-	
		10.10.10.17	255.255.255.252	S1/2	HDLC	-	
Londres	DTE	192.168.20.1	255.255.255.0	f0/0	HDLC Ethernet	-	
		10.10.10.6	255.255.255.252	S1/1	HDLC	-	
		10.10.10.9	255.255.255.252	S1/0	HDLC	-	
		10.10.10.18	255.255.255.252	S1/2	HDLC	-	
		192.168.30.1	255.255.255.0	f0/0	HDLC Ethernet	-	

Tabla 4.1 Datos de la Red WAN

4.1.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

Después de configurar las IPs del esquema con sus respectivos nombres y claves de consola, configuramos las interfaces con encapsulamiento PPP de acuerdo a la **Tabla 4.2**

```
Lima#config ter  
Lima(config)#int s1/0  
Lima(config-if)#encapsulation ppp  
Lima(config-if)#end
```

```
Quito#config ter  
Quito(config)#int s1/2  
Quito(config-if)#encapsulation ppp  
Quito(config-if)#exit  
Quito(config)#int s1/0  
Quito(config-if)#encapsulation ppp  
Quito(config-if)#end
```

```
Miami#config ter  
Miami(config)#int s1/0  
Miami(config-if)#encapsulation ppp  
Miami(config-if)#end
```

Para la configuración de la autenticación CHAP se debe seguir el siguiente orden de pasos:

Primero se define el nombre de usuario que es el nombre del otro Router con el que se va a establecer comunicación, y la clave debe ser la misma en ambos extremos.

```
Quito#config ter  
Quito(config)#username Quito password telecomunicaciones
```

Luego entramos en la interface serial donde vamos a implementar la autenticación y usamos los siguientes comandos, en este caso implementaremos chap.

```
Quito(config)#int s1/0  
Quito(config-if)#ppp authentication chap
```

Este proceso se realiza en cada interface donde se desea la autenticación, en este laboratorio siguiendo la **Tabla 4.2** el router Quito está usando este método de autenticación con el router Miami,

```
Miami#config ter  
Miami(config)#username Quito password telecomunicaciones  
Miami(config)#int s1/0  
Miami(config-if)#ppp authentication chap
```

Configuración de EIGRP

Configuramos el protocolo de enrutamiento EIGRP para mostrar su desempeño en redes donde PPP es implementado, de manera idéntica se procede con la configuración al igual que cuando el protocolo HDLC está activo.

```
Lima#config ter  
Lima(config)#router eigrp 101  
Lima(config-router)#network 10.0.0.0  
Lima(config-router)#network 192.168.40.0  
Lima(config-router)#end
```

```
Quito#config ter  
Quito(config)#router eigrp 101  
Quito (config-router)#network 10.0.0.0  
Quito (config-router)#network 192.168.10.0  
Quito (config-router)#end
```

```
Miami#config ter
Miami (config)#router eigrp 101
Miami (config-router)#network 10.0.0.0
Miami (config-router)#network 192.168.20.0
Miami (config-router)#end
```

```
Londres#config ter
Londres (config)#router eigrp 101
Londres (config-router)#network 10.0.0.0
Londres (config-router)#network 192.168.30.0
Londres (config-router)#end
```

4.1.5 VERIFICACIÓN DE PPP.

Se comprueba conectividad hacia todas las redes, especialmente en las interfaces donde se aplicó PPP. **Figura 4.4**

```
Quito#ping 10.10.10.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.13, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/60/96 ms
Quito#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/101/268 ms
Quito#ping 10.10.10.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.6, timeout is 2 seconds:
?????
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/72/168 ms
Quito#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 4.4 Prueba de conectividad Ping

El Router Quito, posee dos interfaces con encapsulación ppp, la red 10.10.10.12/30 y la red 10.10.10.0/30, las demás interfaces poseen encapsulamiento HDLC el cual viene por defecto en todas las interfaces seriales de un router cisco, esto podemos comprobar con el comando *show interface*. **Figura 4.5**, **Figura 4.6** y **Figura 4.7**

```
Serial1/0 is up, line protocol is up
Hardware is M8T-X.21
Internet address is 10.10.10.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:55, output 00:00:05, output hang never
Last clearing of "show interface" counters 00:02:12
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
  Conversations 0/1/256 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 36 packets input, 1745 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 37 packets output, 2370 bytes, 0 underruns
  0 output errors, 0 collisions, 2 interface resets
  0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Figura 4.5 Interface serial 1/0 router Quito

```
Serial1/1 is up, line protocol is up
Hardware is M8T-X.21
Internet address is 10.10.10.5/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:08, output 00:00:02, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
```

Figura 4.6 Interface serial 1/1 router Quito


```

Serial1/2 is up, line protocol is up
Hardware is M8T-X.21
Internet address is 10.10.10.14/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, crc 16, loopback not set
Keepalive set (10 sec)
Restart-Delay is 0 secs
Last input 00:00:42, output 00:00:08, output hang never
Last clearing of "show interface" counters 00:04:58
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 76 packets input, 2708 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 76 packets output, 3367 bytes, 0 underruns
 0 output errors, 0 collisions, 2 interface resets
 0 output buffer failures, 0 output buffers swapped out
 2 carrier transitions      DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

```

Figura 4.7 Interface serial 1/2 router Quito

El comando *debug ppp negotiation* permite ver la negociación de ppp en las interfaces activas, también podemos ver esta negociación con el capturador de paquetes.

EIGRP se comporta de la misma forma en interfaces donde PPP es implementado, en la **Figura 4.8**, se presenta la tabla de enrutamiento del router Quito la única diferencia aparente en esta pantalla radica en que a diferencia de HDLC, en su tabla de enrutamiento presenta también la IP de la red que está conectada en la interface a más de la ip propia del enlace, en la pantalla existe una comparación entre los recuadros rojos (PPP) y verde (HDLC).

```

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

Gateway of last resort is not set

D    192.168.30.0/24 [90/2172416] via 10.10.10.6, 00:02:09, Serial1/1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    192.168.40.0/24 [90/2172416] via 10.10.10.13, 00:02:13, Serial1/2
D    192.168.20.0/24 [90/2172416] via 10.10.10.2, 00:02:08, Serial1/0
D    10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
D    10.10.10.8/30 [90/2681856] via 10.10.10.6, 00:02:09, Serial1/1
      [90/2681856] via 10.10.10.2, 00:02:09, Serial1/0
C    10.10.10.12/30 is directly connected, Serial1/2
C    10.10.10.13/32 is directly connected, Serial1/2
C    10.10.10.2/32 is directly connected, Serial1/0
C    10.10.10.0/30 is directly connected, Serial1/0
D    10.0.0.0/8 is a summary, 00:02:21, Null0
C    10.10.10.4/30 is directly connected, Serial1/1
D    10.10.10.16/30 [90/2681856] via 10.10.10.6, 00:02:09, Serial1/1
      [90/2681856] via 10.10.10.2, 00:02:09, Serial1/0

```

Figura 4.8 Tabla de enrutamiento router Quito

EIGRP se comporta de manera similar al igual que HDLC, la red implementada en la práctica tiene ambas encapsulaciones, y no existe ningún problema de convergencia de la red, usando el protocolo de enrutamiento EIGRP, tal vez el único cambio podría ser una pequeña demora en la entrega de paquetes en las interface donde exista autenticación.

```

Quito#show ip eigrp topology
IP-EIGRP Topology Table for AS<101>/ID<192.168.10.1>

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.8/30, 2 successors, FD is 2681856
   via 10.10.10.2 (2681856/2169856), Serial1/0
   via 10.10.10.6 (2681856/2169856), Serial1/1
P 10.10.10.14/32, 0 successors, FD is Inaccessible
   via 10.10.10.13 (2681856/2169856), Serial1/2
P 10.10.10.12/30, 1 successors, FD is 2169856
   via Connected, Serial1/2
P 10.10.10.13/32, 1 successors, FD is 2169856
   via Rconnected (2169856/0)
P 10.10.10.2/32, 1 successors, FD is 2169856
   via Rconnected (2169856/0)
P 10.10.10.0/30, 1 successors, FD is 2169856
   via Connected, Serial1/0
P 10.0.0.0/8, 1 successors, FD is 2169856
   via Summary (2169856/0), Null0
P 10.10.10.1/32, 0 successors, FD is Inaccessible
   via 10.10.10.6 (3193856/2681856), Serial1/1
   via 10.10.10.2 (2681856/2169856), Serial1/0

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.10.10.4/30, 1 successors, FD is 2169856
   via Connected, Serial1/1
P 10.10.10.16/30, 2 successors, FD is 2681856
   via 10.10.10.2 (2681856/2169856), Serial1/0
   via 10.10.10.6 (2681856/2169856), Serial1/1
P 192.168.40.0/24, 1 successors, FD is 2172416
   via 10.10.10.13 (2172416/28160), Serial1/2
P 192.168.10.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 192.168.30.0/24, 1 successors, FD is 2172416
   via 10.10.10.6 (2172416/28160), Serial1/1
P 192.168.20.0/24, 1 successors, FD is 2172416
   via 10.10.10.2 (2172416/28160), Serial1/0

```

Figura 4.9 Tabla de topología router Quito

4.1.5.1 Verificación de Paquetes

En la consola de Dynagen usamos el comando para capturar paquetes, esta vez lo realizaremos en la interfaz activa con PPP.

```
>capture Quito s1/2 quito1.cap PPP
```

Note en el comando para la captura la especificación del protocolo de encapsulación para la interface, si por error se usara HDLC, esta captura de paquetes no presentaría la información deseada, ya que no existe tal encapsulamiento en dicha interface.

En la siguiente pantalla encontramos el intercambio de paquetes que está activo en la interface, en su primera parte encontramos los paquetes HELLO propios de las actualizaciones periódicas de EIGRP, luego se encuentra el intercambio de paquetes PPP del encapsulamiento.

23.062000	10.10.10.14	224.0.0.10	EIGRP	Hello
24.484000	N/A	N/A	PPP LCP	Echo Request
24.500000	N/A	N/A	PPP LCP	Echo Reply
27.031000	N/A	N/A	PPP LCP	Echo Request
27.078000	N/A	N/A	PPP LCP	Echo Reply
27.703000	10.10.10.14	224.0.0.10	EIGRP	Hello
27.781000	10.10.10.13	224.0.0.10	EIGRP	Hello
32.453000	10.10.10.14	192.168.40.1	ICMP	Echo (ping) request
32.562000	192.168.40.1	10.10.10.14	ICMP	Echo (ping) reply
32.609000	10.10.10.13	224.0.0.10	EIGRP	Hello
32.672000	10.10.10.14	192.168.40.1	ICMP	Echo (ping) request
32.672000	10.10.10.14	224.0.0.10	EIGRP	Hello
32.687000	192.168.40.1	10.10.10.14	ICMP	Echo (ping) reply
32.703000	10.10.10.14	192.168.40.1	ICMP	Echo (ping) request
32.703000	192.168.40.1	10.10.10.14	ICMP	Echo (ping) reply
32.734000	10.10.10.14	192.168.40.1	ICMP	Echo (ping) request

Figura 4.10 Intercambio de paquetes PPP y EIGRP router Quito

En la **Figura 4.10** también se realizó un ping desde el router Quito hacia la red del router Lima, este intercambio de paquetes ICMP se lo puede observar claramente.

CAPÍTULO 5

PRÁCTICAS FRAME RELAY

La tecnología Frame Relay se ha convertido en una de las tecnologías WAN más utilizadas. Una de las razones de su popularidad es que resulta atractiva económicamente cuando se la compara con líneas arrendadas. En este capítulo se revisará la tecnología Frame Relay junto a dos prácticas las cuales implementan protocolos de enrutamiento OSPF y EIGRP.

5.1 PRÁCTICA 7

Tema: CONFIGURACIÓN DE FRAME-RELAY CON OSPF

5.1.1 OBJETIVOS

- ✓ Configurar un Switch Frame Relay para trabajar con una topología de estrella
- ✓ Configurar las direcciones IP del esquema de la red con su respectivo PVC y DLCI
- ✓ Configurar encapsulación Frame Relay
- ✓ Configurar el protocolo de enrutamiento dinámico OSPF en la topología.
- ✓ Verificar el correcto funcionamiento del esquema de red, conectividad y envío de paquetes.

- ✓ Reconocer las principales características de Frame Relay junto al protocolo de enrutamiento OSPF.

5.1.2 MARCO TEÓRICO.

En el capítulo I se detalló el funcionamiento de Frame Relay, el establecimiento de circuitos virtuales, PVC, DLCI y la topología que usualmente usa, existe un problema particular en Frame Relay, el cual tiene que ver con sus actualizaciones. Por defecto, una red Frame Relay ofrece conectividad de acceso múltiple sin *broadcast* (NBMA) entre dos sitios remotos. Un entorno NBMA se considera igual a otros entornos de medios de acceso múltiple, por ejemplo Ethernet, en el que todos los routers se encuentran en la misma subred. Sin embargo, para reducir los costos, las nubes NBMA generalmente se construyen siguiendo una topología en estrella. En la topología en estrella, la topología física no provee las funciones de acceso múltiple que sí brinda Ethernet.

La topología física consta de múltiples PVCs.

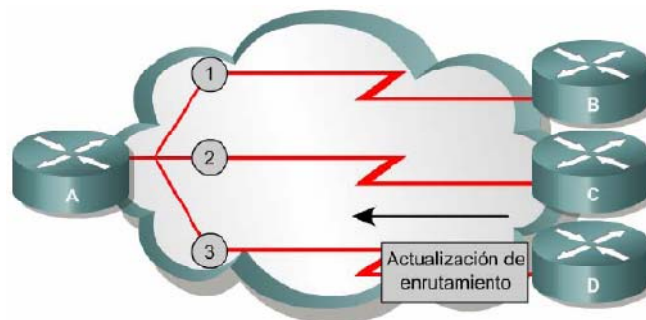


Figura 5.1 Problema de actualización en una Red Frame Relay

La topología NBMA de Frame Relay puede causar dos problemas:

1. Problemas de alcance relativos a las actualizaciones de enrutamiento.
2. La necesidad de replicar los paquetes broadcast en cada uno de los PVCs cuando una interfaz física contiene más de un PVC

La actualización mediante horizonte dividido reduce los loops de enrutamiento al no permitir que una actualización de enrutamiento recibida en una interfaz sea reenviada por la misma interfaz. Si el router B, **Figura 5.1** un router en una punta de la estrella, envía una actualización de enrutamiento broadcast al router A, el router de el nodo central, y el router A tiene varios PVCs en una sola interfaz física, entonces el router A no puede enviar la actualización de enrutamiento a través de la misma interfaz física a otro router en una punta de la estrella. Si el horizonte dividido está inhabilitado, es posible enviar la actualización de enrutamiento a través de la misma interfaz física por la que se recibió. El horizonte dividido no presenta problemas cuando hay un único PVC en la interfaz física.

Esta sería una conexión Frame Relay punto a punto (2).

Los routers que dan soporte a conexiones múltiples a través de una interfaz física tienen varios PVCs que terminan en un único router. Este router debe replicar los paquetes broadcast, por ejemplo: los broadcasts de actualización de enrutamiento, en todos los PVCs y enviarlos a los routers remotos. Los paquetes broadcast replicados pueden consumir ancho de banda y aumentar significativamente la latencia en el tráfico de usuario. Puede parecer lógico apagar el horizonte dividido para resolver los problemas de alcance que origina. Sin embargo, no todos los protocolos de la capa de red permiten inhabilitar el horizonte dividido y el desconectarlo aumenta la probabilidad de que ocurran loops de enrutamiento.

Una forma de resolver los problemas del horizonte dividido es utilizar una topología de malla completa. Sin embargo, esto aumentará el costo porque se requieren más PVCs. La solución de mayor aceptación es el uso de subinterfaces.

Subinterfaces en Frame Relay

Para permitir el envío de las actualizaciones broadcast de enrutamiento en una topología Frame Relay en estrella, se configura el router de la central con interfaces

asignadas lógicamente. Estas interfaces reciben el nombre de subinterfaces. Las subinterfaces son subdivisiones lógicas de una interfaz física.

En entornos de horizonte dividido, es posible reenviar las actualizaciones de enrutamiento recibidas en una subinterfaz a través de otra subinterfaz. En una configuración de subinterfaces, cada circuito virtual puede configurarse como una conexión punto a punto. Esto permite que cada subinterfaz actúe de modo similar a una línea arrendada. Al utilizar una interfaz Frame Relay punto a punto, cada pareja de routers punto a punto se encuentra en su propia subred.

Las subinterfaces Frame Relay pueden configurarse en modo punto a punto y en modo multipunto:

- **Punto a punto:** se utiliza una sola subinterfaz punto a punto para establecer una conexión PVC a otra interfaz física o subinterfaz de un router remoto. En este caso, cada pareja de routers punto a punto está en su propia subred y cada subinterfaz punto a punto tiene un solo DLCI. En un entorno punto a punto, cada subinterfaz actúa como una interfaz punto a punto. Entonces, el tráfico de actualización de enrutamiento no está sujeto a la regla del horizonte dividido.
- **Multipunto:** se utiliza una sola subinterfaz multipunto para establecer múltiples conexiones PVC a múltiples interfaces físicas o subinterfaces en routers remotos. Todas las interfaces involucradas se encuentran en la misma subred. La subinterfaz actúa como una interfaz Frame Relay NBMA de modo que el tráfico de actualización de enrutamiento está sujeto a la regla de horizonte dividido.

El comando **encapsulation frame-relay** está asignado a la interfaz física. Todos los demás aspectos de la configuración, tales como la dirección de capa de red y los DLCI se asignan a cada subinterfaz.

Las configuraciones multipunto pueden utilizarse para ahorrar direcciones, lo que puede ser de utilidad si no se está utilizando una Máscara de subred de longitud variable (VLSM). Sin embargo, las configuraciones multipunto podrían funcionar

inapropiadamente dadas las consideraciones de tráfico de broadcasts y del horizonte dividido. La opción de la subinterfaz punto a punto se creó para evitar esos problemas.

Las redes NBMA son aquellas que soportan muchos routers, pero no tiene disponibilidad de broadcast, cuando una interface se conecta a varios sitios sobre una red NBMA, esta red provoca problemas de alcance sobre los dispositivos.

Una Topología de estrella conocida como hub-spoke es la topología de red más popular en Frame Relay. Existe también la de malla pero esta demanda una gran cantidad de trabajo de configuración y es bastante costoso.

OSPF puede trabajar de dos maneras de acuerdo a RFC 2328.

1. *NBMA Nonbroadcast multiaccess*. El cual emula ambiente broadcast en el cual los Routers intercambian actualizaciones de tráfico para identificar sus vecinos y elegir DR y BDR.
2. *Punto a Multipunto* En este caso la red Nonbroadcast es tratada como una colección de enlaces punto a punto. En este ambiente los Routers identifican sus vecinos pero no existe elección de DR y BDR.

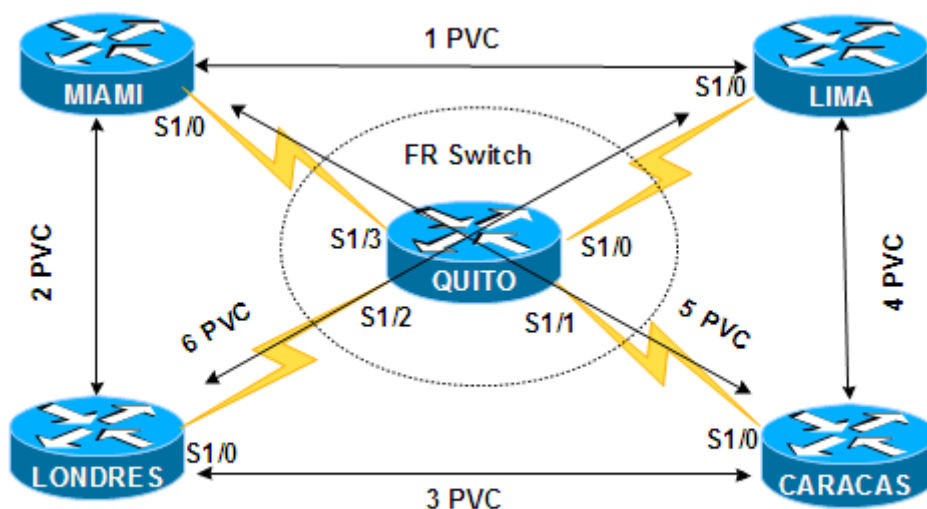
La siguiente tabla provee información sobre los diferentes modos de operación de OSPF, en relación con NBMA. En la práctica tres se realizó ya un laboratorio usando enlaces broadcast y punto a punto.

Mode	Preferred Topology	Subnet Address	Adjacency	RFC- or Cisco-defined
NBMA	Fully meshed	Neighbors must belong to the same subnet number	Manual Configuration DR/BDR elected	RFC
Broadcast	Fully meshed	Neighbors must belong to the same subnet number	Automatic DR/BDR elected	Cisco
Point-to-multipoint	Partially meshed or star	Neighbors must belong to the same subnet number	Automatic No DR/BDR	RFC
Point-to-multipoint nonbroadcast	Partially meshed or star	Neighbors must belong to the same subnet number	Manual configuration No DR/BDR	Cisco
Point-to-point	Partially meshed or star, using subinterface	Different subnets for each subinterface	Automatic No DR/BDR	Cisco

Tabla 5.1 Características de OSPF en distintos tipos de Red

En el siguiente esquema de red se presenta una topología de estrella para la configuración y encapsulamiento Frame Relay con enrutamiento OSPF.

5.1.3 ESQUEMA DE LA RED



6 PVC = 12 DLCI

Figura 5.2 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface	DLCI
FRAME RELAY SWITCH QUITO	DCE			S1/0	
	DCE			S1/1	
	DCE			S1/2	
	DCE			S1/3	
Miami	DTE	192.168.1.4	255.255.255.248	S1/0	701
					401
					501
		192.168.40.1	255.255.255.0	f/0	
Londres	DTE	192.168.1.3	255.255.255.248	S1/0	102
					103
					104
		192.168.10.1	255.255.255.0	f/0	
Lima	DTE	192.168.1.1	255.255.255.248	S1/0	301
					601
					107
		192.168.30.1	255.255.255.0	f/0	
Caracas	DTE	192.168.1.2	255.255.255.248	S1/0	201
					105
					106
		192.168.20.1	255.255.255.0	f/0	

Tabla 5.2 Datos de la Red Frame Relay

5.1.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

Primero establecemos el Frame Relay Switch con su respectivo encapsulamiento en cada interface serial.

```

Quito(config)#frame-relay switching
Quito(config)#interface serial 1/2
Quito(config-if)#encapsulation frame-relay
    
```

En los siguientes comandos se configura el tipo de *lmi* en este caso *ansi*, ya que Dynagen no trabaja con otros modos, luego damos la característica de sincronismo en el switch Frame Relay DCE,

```

Quito(config-if)#frame-relay lmi-type ansi
    
```

```
Quito(config-if)#frame-relay intf-type dce
```

Para concluir con el router Quito configuramos las interfaces seriales con sus respectivos DLCI tomando en cuenta siempre el esquema de red y la tabla de configuración.

```
Quito(config-if)#frame-relay route 102 interface serial 1/1 201
```

```
Quito(config-if)#frame-relay route 103 interface serial 1/0 301
```

```
Quito(config-if)#frame-relay route 104 interface serial 1/3 401
```

```
Quito(config-if)#no shut
```

```
Quito(config-if)#exit
```

Este proceso lo realizamos para cada interface, con el objetivo de configurar cada PVC con sus respectivos DLCI

```
Quito(config)#interface serial 1/1
```

```
Quito(config-if)#encapsulation frame-relay
```

```
Quito(config-if)#frame-relay lmi-type ansi
```

```
Quito(config-if)#frame-relay intf-type dce
```

```
Quito(config-if)#frame-relay route 201 interface serial 1/2 102
```

```
Quito(config-if)#frame-relay route 105 interface serial 1/3 501
```

```
Quito(config-if)#frame-relay route 106 interface serial 1/0 601
```

```
Quito(config-if)#no shut
```

```
Quito(config-if)#exit
```

```
Quito(config)#interface serial 1/0
```

```
Quito(config-if)#encapsulation frame-relay
```

```
Quito(config-if)#frame-relay lmi-type ansi
```

```
Quito(config-if)#frame-relay intf-type dce
```

```
Quito(config-if)#frame-relay route 301 interface serial 1/2 103
```

```
Quito(config-if)#frame-relay route 601 interface serial 1/1 106
```

```
Quito(config-if)#frame-relay route 107 interface serial 1/3 701
```

```
Quito(config-if)#no shut
```

```
Quito(config-if)#exit
```

```
Quito(config)#interface serial 1/3
```

```
Quito(config-if)#encapsulation frame-relay
```

```
Quito(config-if)#frame-relay lmi-type ansi
```

```
Quito(config-if)#frame-relay intf-type dce
```

```
Quito(config-if)#frame-relay route 701 interface serial 1/0 107
```

```
Quito(config-if)#frame-relay route 401 interface serial 1/2 104
```

```
Quito(config-if)#frame-relay route 501 interface serial 1/1 105
```

```
Quito(config-if)#no shut
```

```
Quito(config-if)#exit
```

Luego en los dispositivos terminales se configura las interfaces seriales con encapsulamiento Frame Relay y su dirección IP correspondiente.

```
Lima(config)#int s1/0
```

```
Lima(config-if)#encapsulation frame-relay
```

```
Lima(config-if)#frame-relay lmi-type ansi
```

```
Lima(config-if)#ip address 192.168.1.1 255.255.255.248
```

```
Lima(config-if)#no shut
```

```
Lima(config-if)#exit
```

```
Miami(config)#int s1/0
```

```
Miami (config-if)#encapsulation frame-relay
```

```
Miami (config-if)#frame-relay lmi-type ansi
```

```
Miami (config-if)#ip address 192.168.1.4 255.255.255.248
```

```
Miami (config-if)#no shut
```

```
Miami (config-if)#exit
```

```
Londres(config)#int s1/0
```

```
Londres (config-if)#encapsulation frame-relay
```

```
Londres (config-if)#frame-relay lmi-type ansi
```

```
Londres (config-if)#ip address 192.168.1.3 255.255.255.248
```

```
Londres (config-if)#no shut
```

```
Londres (config-if)#exit
```

```
Caracas(config)#int s1/0
```

```
Caracas (config-if)#encapsulation frame-relay
```

```
Caracas (config-if)#frame-relay lmi-type ansi
```

```
Caracas (config-if)#ip address 192.168.1.2 255.255.255.248
```

```
Caracas (config-if)#no shut
```

```
Caracas (config-if)#exit
```

Finalizado el proceso de configuración de IPs, DLCI y encapsulamiento Frame-Relay, configuramos OSPF. El protocolo de enrutamiento OSPF necesita que cada router sea notificado de sus vecinos es así que a continuación se realiza la siguiente configuración, sin ésta no sería posible alcanzar las redes ethernet que posee cada router.

```
Miami#config ter
```

```
Miami(config)#router ospf 101
```

```
Miami(config-router)#network 192.168.1.0 0.0.0.7 area 0
```

```
Miami(config-router)#network 192.168.40.0 0.0.0.255 area 0
```

```
Miami(config-router)#neighbor 192.168.1.1
```

```
Miami(config-router)#neighbor 192.168.1.2
```

```
Miami(config-router)#neighbor 192.168.1.3
```

```
Miami(config-router)#end
```

```
Lima#config ter
```

```
Lima (config)#router ospf 101
```

```
Lima (config-router)#network 192.168.1.0 0.0.0.7 area 0
```

```
Lima (config-router)#network 192.168.30.0 0.0.0.255 area 0
```

```
Lima (config-router)#neighbor 192.168.1.4
```

```
Lima (config-router)#neighbor 192.168.1.2
```

```
Lima (config-router)#neighbor 192.168.1.3
```

```
Lima (config-router)#end
```

```
Caracas#config ter
Caracas (config)#router ospf 101
Caracas (config-router)#network 192.168.1.0 0.0.0.7 area 0
Caracas (config-router)#network 192.168.20.0 0.0.0.255 area 0
Caracas (config-router)#neighbor 192.168.1.1
Caracas (config-router)#neighbor 192.168.1.4
Caracas (config-router)#neighbor 192.168.1.3
Caracas (config-router)#end
```

```
Londres#config ter
Londres (config)#router ospf 101
Londres (config-router)#network 192.168.1.0 0.0.0.7 area 0
Londres (config-router)#network 192.168.10.0 0.0.0.255 area 0
Londres (config-router)#neighbor 192.168.1.1
Londres (config-router)#neighbor 192.168.1.2
Londres (config-router)#neighbor 192.168.1.4
Londres (config-router)#end
```

5.4.5 VERIFICACIÓN DE FRAME RELAY.

Se realizará pruebas de conectividad ping desde el router Lima hacia los equipos terminales **Figura 5.3**. Recuerde que el router Quito funciona como Switch es decir desde este no es posible realizar pruebas de conectividad.

```
Lima#ping 192.168.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/130/248 ms
Lima#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/465/1744 ms
Lima#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/111/264 ms
```

Figura 5.3 Prueba de conectividad en Frame Relay

También se debe asegurar la conectividad hacia las redes vecinas configuradas con OSPF **Figura 5.4.**

```
Lima#ping 192.168.40.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/196/268 ms
Lima#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 112/189/284 ms
Lima#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/180/308 ms
```

Figura 5.4 Prueba de conectividad en Frame Relay

Con el comando *show run* podemos verificar que redes usan ospf, y cual es la configuración de vecinos, para el router Lima las redes vecinas son 192.168.1.2 192.168.1.3 192.168.1.4 **Figura 5.5**

```
router ospf 101
log-adjacency-changes
network 192.168.1.0 0.0.0.7 area 0
network 192.168.30.0 0.0.0.255 area 0
neighbor 192.168.1.2
neighbor 192.168.1.4
neighbor 192.168.1.3
```

Figura 5.5 Verificación de configuración de Vecinos

OSPF siempre guarda una tabla de vecinos la cual la podemos ver con el comando *show ip ospf neighbor*. En la **Figura 5.6**. Observaremos en recuadro verde el ID del router vecino, y la elección de DR y BDR que realiza el protocolo en rojo.

```
Lima#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.20.1	1	FULL/DROTHER	00:01:51	192.168.1.2	Serial1/0
192.168.40.1	1	FULL/DROTHER	00:01:54	192.168.1.4	Serial1/0
192.168.10.1	1	FULL/BDR	00:01:50	192.168.1.3	Serial1/0

Figura 5.6 Verificación de configuración de Vecinos

En este tipo de redes es necesario darse cuenta que interfaces son tipo broadcast o nonbroadcast, con el comando *show ip ospf interface*, encontramos información importante y muy detallada de cada interface. En la **Figura 5.7** vemos información de la interface fast ethernet, la cual indica que es broadcast, estado, ID de proceso y mas información para detectar fallas.

```
Lima#show ip ospf int
FastEthernet0/0 is up, line protocol is up
Internet Address 192.168.30.1/24, Area 0
Process ID 101, Router ID 192.168.30.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.30.1, Interface address 192.168.30.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 oob-resync timeout 40
 Hello due in 00:00:07
Supports Link-local Signaling (LLS)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
```

Figura 5.7 Verificación de configuración de Interfaces

Frame Relay es una red tipo NBMA, esta notación se encuentra en cada una de las interfaces con este encapsulamiento es por esta razón que en la interface s1/0 en la **Figura 5.8** indican información pertinente al encapsulamiento y procesos del protocolo de enrutamiento activo.


```

Serial1/0 is up, line protocol is up
Internet Address 192.168.1.1/29, Area 0
Process ID 101, Router ID 192.168.30.1, Network Type NON_BROADCAST, Cost: 64
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.30.1, Interface address 192.168.1.1
Backup Designated router (ID) 192.168.10.1, Interface address 192.168.1.3
Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
  oob-resync timeout 120
  Hello due in 00:00:09
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 4 msec, maximum is 4 msec
Neighbor Count is 3, Adjacent neighbor count is 3
  Adjacent with neighbor 192.168.20.1
  Adjacent with neighbor 192.168.40.1
  Adjacent with neighbor 192.168.10.1 (Backup Designated Router)
Suppress hello for 0 neighbor(s)

```

Figura 5.8 Verificación de configuración de Interfaces

Dentro del análisis de PVC y DLCI, se usa *show frame-relay map*, el cual permite ver todo lo referente a la red frame Relay implementada en el router donde se usa el comando, además también podemos verificar el tipo de LMI usado en este caso ANSI.

Figura 5.9.

```

Lima#show frame-relay map
Serial1/0 (up): ip 192.168.1.2 dlci 601(0x259,0x9490), dynamic,
  broadcast, status defined, active
Serial1/0 (up): ip 192.168.1.3 dlci 301(0x12D,0x48D0), dynamic,
  broadcast, status defined, active
Serial1/0 (up): ip 192.168.1.4 dlci 107(0x6B,0x18B0), dynamic,
  broadcast, status defined, active
Lima#show frame-relay lmi
LMI Statistics for interface Serial1/0 (Frame Relay DTE) LMI TYPE = ANSI
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 14 Num Status msgs Rcvd 11
Num Update Status Rcvd 0 Num Status Timeouts 3
Last Full Status Req 00:00:25 Last Full Status Rcvd 00:00:25

```

Figura 5.9 Verificación de DLCI y LMI

5.4.5.1 Verificación de Paquetes

Desde el router Lima capturaremos paquetes desde la interface s1/0. Desde Dynagen usamos el siguiente comando y realizamos un ping hacia la red del router Londres 192.168.10.1. **Figura 5.10**

>capture Lima s1/0 lima.cap HDLC

12	22.572000	192.168.1.2	192.168.1.1	OSPF	Hello Packet
13	26.210000	192.168.1.1	192.168.10.1	ICMP	Echo (ping) request
14	26.350000	192.168.10.1	192.168.1.1	ICMP	Echo (ping) reply
15	26.409000	192.168.1.1	192.168.10.1	ICMP	Echo (ping) request
16	26.556000	192.168.10.1	192.168.1.1	ICMP	Echo (ping) reply
17	26.579000	192.168.1.1	192.168.10.1	ICMP	Echo (ping) request
18	26.634000	192.168.10.1	192.168.1.1	ICMP	Echo (ping) reply
19	26.699000	192.168.1.1	192.168.10.1	ICMP	Echo (ping) request
20	26.809000	192.168.10.1	192.168.1.1	ICMP	Echo (ping) reply
21	26.855000	192.168.1.1	192.168.10.1	ICMP	Echo (ping) request
22	26.975000	192.168.10.1	192.168.1.1	ICMP	Echo (ping) reply

Figura 5.10 Verificación de de conexión.

En la pantalla ya se puede ir viendo el envío de paquetes Hello que realiza OSPF para conocer sobre el estado de la red. Con detenimiento se analizará el archivo con extensión *.cap* el cual en cada una de las prácticas se encuentra disponible. Ahora intencionalmente apagaremos la interface serial 1/0 del router Londres para provocar una actualización en la tabla de enrutamiento de OSPF. Nótese los paquetes de notificación de actualización son enviados desde otros Routers vecinos reportando el cambio en la red.

Figura 5.11 y Figura 5.12

394.446000	192.168.1.4	192.168.1.1	OSPF	LS Update
396.955000	192.168.1.2	192.168.1.1	OSPF	LS Acknowledge
397.103000	192.168.1.1	192.168.1.2	OSPF	LS Acknowledge
397.104000	192.168.1.1	192.168.1.4	OSPF	LS Acknowledge
399.997000	N/A	N/A	0x0308	
400.057000	N/A	N/A	0x0308	
407.684000	192.168.1.4	192.168.1.1	OSPF	Hello Packet
408.090000	192.168.1.1	192.168.1.2	OSPF	Hello Packet
408.090000	192.168.1.1	192.168.1.4	OSPF	Hello Packet

Figura 5.11 Notificación de cambio en la topología.

En las dos Figuras se encuentran las actualizaciones hacia el router Lima desde los Router Miami y Caracas respectivamente, con sus respectivas IPs origen Destino.

502.677000	192.168.1.2	192.168.1.1	OSPF	Hello Packet
506.011000	192.168.1.1	192.168.1.2	OSPF	LS Update
506.011000	192.168.1.1	192.168.1.4	OSPF	LS Update
508.638000	192.168.1.4	192.168.1.1	OSPF	LS Acknowledge
508.776000	192.168.1.2	192.168.1.1	OSPF	LS Acknowledge

Figura 5.12 Notificación de cambio en la topología

5.2 PRÁCTICA 8

Tema: CONFIGURACIÓN DE FRAME-RELAY CON EIGRP

5.2.1 OBJETIVOS

- ✓ Configurar un Switch Frame Relay para trabajar con una topología de estrella
- ✓ Configurar las direcciones IP del esquema de la red con su respectivo PVC y DLCI
- ✓ Reconocer las principales características de Frame Relay junto al protocolo de enrutamiento EIGRP
- ✓ Verificar el correcto funcionamiento del esquema de red, conectividad y envío de paquetes.

5.2.2 MARCO TEÓRICO.

EIGRP es escalable en enlaces punto a punto como se revisó en prácticas anteriores, debido a que es un protocolo de enrutamiento bastante robusto y versátil, su comportamiento en redes non-broadcast no deja de ser el mismo que en enlaces punto a punto.

Utilización del Enlace en EIGRP

EIGRP usa más del 50% del ancho de banda declarado en la interface donde es implementado. Este porcentaje puede ser ajustado con el siguiente comando.

```
Router(config-if)# ip bandwidth-percent eigrp as-number percent
```

El parámetro del porcentaje puede ser un valor mayor a 100. Esto es útil si el ancho de banda es configurado artificialmente por razones políticas de enrutamiento.

Cuando se configura interfaces multipunto como las prácticas que se han desarrollado, EIGRP comparte el ancho de banda de manera equitativa, es así que el ancho

de banda de la interfaz física es dividido por el número de vecinos que comparten el enlace. En la **Figura 5.13** se observa un enlace T1 con una topología multipunto parecida a la que será implementada en el laboratorio, en este caso se debe tomar en cuenta el CIR contratado en este caso 56Kbps por enlace, es decir que el ancho de banda de la Serial 0 del router A será 224 Kbps ya que este valor se divide entre los cuatro routers de manera equitativa.

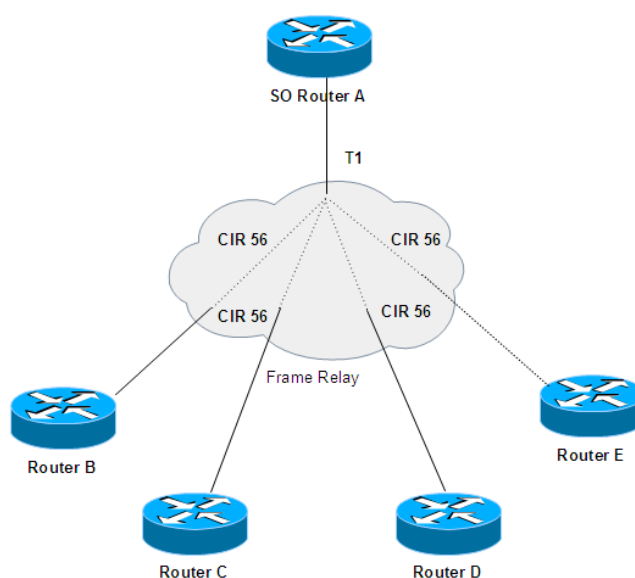


Figura 5.13 Red Frame Relay multipunto.

Cada instalación tiene su propia topología, hay casos en los que un diferente valor de CIR es requerido, en estos casos se puede usar un sistema híbrido es decir mezclar las características de enlaces punto a punto con multipunto. En la **Figura 5.14** se configura de la siguiente forma los routers B, C y D pertenecerán a un enlace multipunto el cual dividirá el ancho de banda en tres partes iguales, y para el router E un enlace punto a punto con un ancho de banda de 56 Kbps.

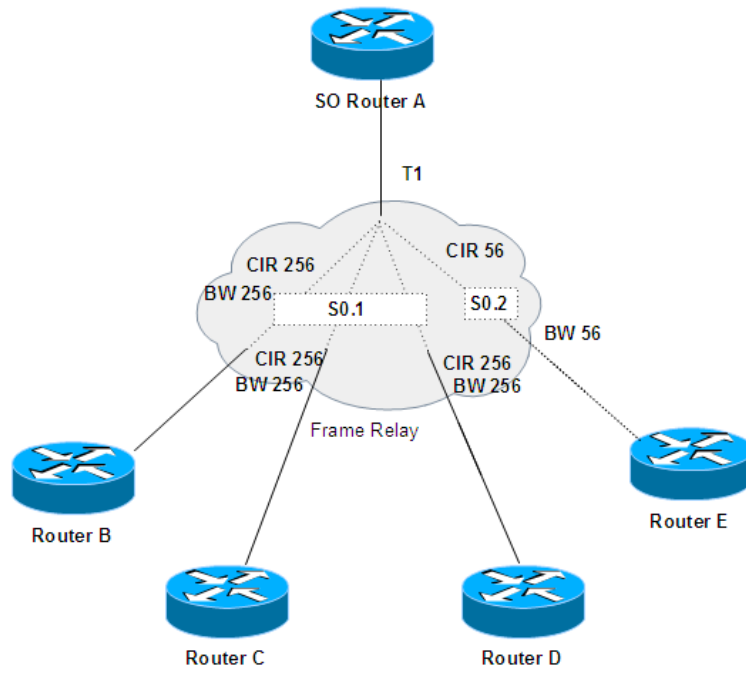
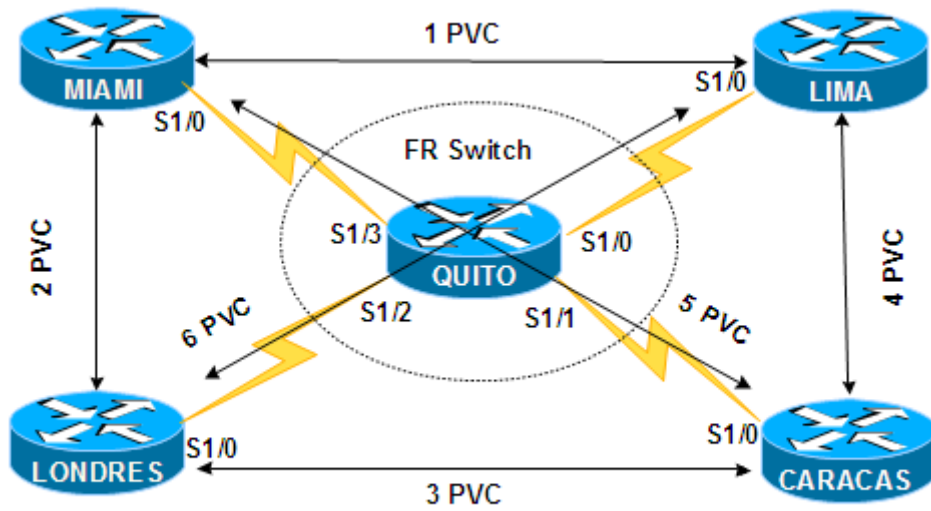


Figura 5.14 Red Frame Relay multipunto.

5.2.3 ESQUEMA DE LA RED



6 PVC = 12 DLCI

Figura 5.15 Diagrama de Red

Nombre Router	Sincronismo	IP Address	Mascara de Subred	Interface	DLCI
FRAME RELAY SWITCH QUITO	DCE			S1/0	
	DCE			S1/1	
	DCE			S1/2	
	DCE			S1/3	
Miami	DTE	192.168.1.4	255.255.255.248	S1/0	701
					401
					501
Londres	DTE	192.168.1.3	255.255.255.248	S1/0	102
					103
					104
Lima	DTE	192.168.1.1	255.255.255.248	S1/0	301
					601
					107
Caracas	DTE	192.168.1.2	255.255.255.248	S1/0	201
					105
					106

Tabla 5.3 Datos de la Red Frame Relay

5.2.4 LABORATORIO –PASOS DE CONFIGURACIÓN-

De igual manera configuramos el Switch Frame-Relay junto con los circuitos virtuales o simplemente podemos desactivar el protocolo de enrutamiento OSPF en los dispositivos terminales con los siguientes comandos.

```
Lima(config)#no router ospf 101
Lima(config)#end
Miami(config)# no router ospf 101
Miami(config)#end
Londres(config)# no router ospf 101
Londres(config)#end
Caracas(config)# no router ospf 101
Caracas(config)#end
```

Como podemos apreciar no es necesario modificar el router Quito que trabaja como switch, después de desactivar el protocolo de enrutamiento, configuramos EIGRP que es mucho más sencillo de implementar que OSPF.

```
Lima#config ter  
Lima(config)#router eigrp 101  
Lima(config-router)#network 192.168.30.0  
Lima(config-router)#network 192.168.1.0  
Lima(config-router)#end
```

```
Miami#config ter  
Miami(config)#router eigrp 101  
Miami (config-router)#network 192.168.40.0  
Miami (config-router)#network 192.168.1.0  
Miami (config-router)#end
```

```
Londres#config ter  
Londres(config)#router eigrp 101  
Londres(config-router)#network 192.168.10.0  
Londres(config-router)#network 192.168.1.0  
Londres(config-router)#end
```

```
Caracas#config ter  
Caracas (config)#router eigrp 101  
Caracas (config-router)#network 192.168.20.0  
Caracas (config-router)#network 192.168.1.0  
Caracas (config-router)#end
```

5.2.5 VERIFICACIÓN DE FRAME RELAY.

Verificamos el protocolo de enrutamiento EIGRP, con *show ip protocols*, como ya vimos en la práctica cuatro, podemos hacer uso de todos los comandos también en este tipo de redes NBMA **Figura 5.16**

En la pantalla se despliega información del protocolo, las redes que usan EIGRP, con summarización, y las Gateway por donde existe intercambio de información EIGRP.

```
Lima#show ip protocols
Routing Protocol is "eigrp 101"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 101
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.30.0/24 for Serial1/0
    192.168.1.0/24 for FastEthernet0/0
    Summarizing with metric 2169856
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.30.0
```

Figura 5.16 Comando show ip protocol

```
Routing Information Sources:
Gateway          Distance    Last Update
(this router)    90          00:13:09
192.168.1.3      90          00:11:25
Gateway          Distance    Last Update
192.168.1.2      90          00:11:31
192.168.1.4      90          00:11:32
Distance: internal 90 external 170
```

Figura 5.17 Comando show ip protocols router Lima

Verificamos la existencia de las redes vecinos de igual manera que en OSPF, solo cambiando el nombre del protocolo *show ip eigrp neighbor*. **Figura 5.18**

```
Lima#show ip eigrp neighbor
IP-EIGRP neighbors for process 101
H   Address          Interface          Hold Uptime    SRTT    RTT    Q   Seq
   192.168.1.2      Se1/0             (sec) (ms)          Cnt  Num
2   192.168.1.2      Se1/0             149 00:17:54  290 1740  0  9
1   192.168.1.3      Se1/0             162 00:18:47  902 5000  0  9
0   192.168.1.4      Se1/0             156 00:18:47  438 2628  0 10
```

Figura 5.18 Comando show ip neighbor router Lima

Podemos usar muchos otros comandos como *show ip route*, o *show ip eigrp topology* los cuales nos ayudan a observar información para detección de errores, queda a disposición del lector hacer uso de estos comandos para investigación, además un resumen de los comandos usados en la tesis se encuentra en la parte final en la sección de Anexos.

5.2.5.1 Verificación de Paquetes.

Para observar el tráfico de paquetes dentro de la interface Caracas, usamos el siguiente comando en el simulador Dynagen, el archivo.cap también se encuentra gravado en el directorio raíz de la práctica.

```
>capture Caracas s1/0 caracas.cap HDLC
```

Desconectamos un interface serial de un vecino para observar el comportamiento de EIGRP en el entorno Frame-Relay

```
Miami#config ter
```

```
Miami(config)#int s1/0
```

```
Miami(config-if)#shut
```

Cuando el tiempo de espera termina, nuevas actualizaciones de la topología se enviarán, tal como los mensajes *queries* y *acknowledges*, como ya se estudio en la práctica cuatro, todo esto para hacer el recálculo del algoritmo DUAL que usa EIGRP **Figura 5.19**

262.954000	192.168.1.3	192.168.1.2	EIGRP	Query
262.966000	192.168.1.3	224.0.0.10	EIGRP	Hello
263.326000	192.168.1.1	224.0.0.10	EIGRP	Hello
263.533000	192.168.1.2	192.168.1.1	EIGRP	Query
263.533000	192.168.1.2	192.168.1.3	EIGRP	Acknowledge
263.563000	192.168.1.2	224.0.0.10	EIGRP	Hello
263.563000	192.168.1.2	224.0.0.10	EIGRP	Hello
263.657000	192.168.1.2	192.168.1.3	EIGRP	Query
263.813000	192.168.1.1	192.168.1.2	EIGRP	Query
264.108000	192.168.1.2	192.168.1.1	EIGRP	Acknowledge
264.413000	192.168.1.1	192.168.1.2	EIGRP	Acknowledge
264.422000	192.168.1.1	192.168.1.2	EIGRP	Reply
264.426000	192.168.1.3	192.168.1.2	EIGRP	Acknowledge
264.616000	192.168.1.2	192.168.1.3	EIGRP	Reply
264.616000	192.168.1.2	192.168.1.1	EIGRP	Reply
265.266000	192.168.1.1	192.168.1.2	EIGRP	Acknowledge
265.313000	192.168.1.3	192.168.1.2	EIGRP	Reply
265.504000	192.168.1.2	192.168.1.3	EIGRP	Acknowledge

Figura 5.19 Comando show ip protocols router Lima

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El simulador Dynagen es una herramienta muy poderosa en el modelamiento de redes de área extendida, en comparación con otros simuladores, es versátil y posee una plataforma bastante estable, a diferencia de otros que no permiten el establecimiento de protocolos de enrutamiento como BGP, o incluso el establecimiento de claves de usuario.

El limitante del simulador Dynagen es la memoria ram de la cual hace uso, pero hay que recordar que está en sus primeras versiones y cada vez los computadores vienen con sistemas electrónicos mucho más rápidos y robustos.

El simulador Dynagen también es bastante grande a nivel de laboratorios, esto no implica que no se puedan realizar más experiencias, existen foros de investigación los cuales siguen probando el simulador con diferentes tecnologías, se invita al lector a que amplíe el conocimiento de esta poderosa herramienta.

En el capítulo III usamos Dynagen para establecer los protocolos de enrutamiento interior y exterior, las características más importantes de cada uno de ellos fue explicado y verificado en cada práctica.

Se concluyo de manera sistemática que ciertos protocolos de enrutamiento son mas robustos y versátiles dependiendo del tamaño de la red, por ejemplo RIP es una buena opción para redes pequeñas, OSPF lo es si una red mediana se intenta implementar, EIGRP tiene una aceptación para redes grandes.

Los Protocolos de enrutamiento RIP, OSPF y EIGRP son ejemplos de distintos planteamientos de reconocimiento de topología, RIP usa vector distancia, OSPF usa estado de enlace y EIGRP una sistema hibrido llamado DUAL como algoritmo de enrutamiento, todas estas características deben ser conocidas para el empleo de cada protocolo en determinada red. En la caso de RIP su métrica es el llamado *hop count*, el cual desprecia el ancho de banda y muchos otros parámetros que si son abarcados por OSPF y EIGRP.

El manejo jerárquico de OSPF por áreas es bastante lógico y amplio a la vez, el reconocimiento de rutas por costo, supero en la decisión que uso RIP, en la anterior práctica ya que este si uso el conocimiento del ancho de banda de cada interface, el retraso y la velocidad de transferencia.

En cada práctica se ha hecho hincapié sobre las formas que tienen cada protocolo de enrutamiento para escoger la mejor ruta hacia las redes. Es así como, de manera implícita se ha realizado una comparación entre estos protocolos, los cuales son los más usados actualmente.

RECOMENDACIONES

Todo este compendio de conocimientos debe ser esencial en el entender de un ingeniero en telecomunicaciones, el texto pretende además de entrenar, enseñar las tecnologías existentes en redes de área extendida, además presenta claves de cómo poder configurar distintas redes en el simulador Dynagen.

Desde la plataforma Windows, Dynagen tiene un límite por proceso que es de 2GB antes de que este colapse, se recomienda usar Linux en procesos muy grandes, Linux ofrece un tope de 3GB, se recomienda visitar la página de Dynagen donde constantemente se ofrece soluciones a problemas comunes del simulador.

Todas las prácticas realizadas en este documento son implementadas en routers 7200, esto hace que los archivos de las prácticas sean muy pesados por la cantidad de

información que guarda cada sistema operativo de los routers en la red. Para evitar este problema de espacio se puede usar routers más pequeños como el 3600, dependiendo del protocolo que se necesite implementar.

Los diseños de red y topologías, son tan solo algunos ejemplos con los que se puede trabajar, se puede emprender nuevas investigaciones con distintas topologías, queda abierta la discusión a distintas propuestas

ANEXOS

Archivos de RED DYNAGEN

Laboratorio Rutas Estáticas

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

f0/0 = LAN 1

s1/0 = Miami s1/0

s1/1 = Londres s1/1

s1/2 = Lima S1/0

[[router Miami]]

f0/0 = LAN 2

s1/1 = Londres s1/0

[[router Londres]]

f0/0 = LAN 3

s1/2 = Miami s1/2

[[router Lima]]

f0/0 = LAN 4

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

by the interface specification under Router R1

Laboratorio de protocolo de enrutamiento RIP

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

f0/0 = LAN 1

s1/0 = Miami s1/0

s1/1 = Londres s1/1

s1/2 = Lima s1/0

[[router Miami]]

f0/0 = LAN 1

s1/1 = Londres s1/0

s1/2 = Londres s1/2

[[router Londres]]

f0/0 = LAN 1

[[router Lima]]

f0/0 = LAN 1

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

by the interface specification under Router R1

Laboratorio de protocolo de enrutamiento OSPF

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

f0/0 = LAN 1

s1/0 = Miami s1/0

s1/1 = Londres s1/1

s1/2 = Lima S1/0

[[router Miami]]

f0/0 = LAN 2

s1/1 = Londres s1/0

s1/2 = Londres s1/2

[[router Londres]]

f0/0 = LAN 3

[[router Lima]]

f0/0 = LAN 4

[[ROUTER Caracas]]

f0/0 = LAN 5

s1/0 = Quito s1/3

s1/1 = Londres s1/3

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

by the interface specification under Router R1

Laboratorio de protocolo de enrutamiento EIGRP

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

f0/0 = LAN 1

s1/0 = Miami s1/0

s1/2 = Lima S1/0

[[router Miami]]

f0/0 = LAN 2

s1/1 = Londres s1/0

s1/2 = Londres s1/2

[[router Londres]]

f0/0 = LAN 3

[[router Lima]]

f0/0 = LAN 4

[[ROUTER Caracas]]

f0/0 = LAN 1

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

by the interface specification under Router R1

Laboratorio de protocolo de enrutamiento BGP

```
# Simple lab
autostart = false

[localhost]
  [[7200]]
  image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image
  # On Linux / Unix use forward slashes:
  # image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image
  npe = npe-400
  ram = 160

  [[ROUTER backbone_r1]]
  s1/0 = p1r1 s1/0
  s1/1 = p12r1 s1/0

  [[router p1r1]]
  s1/1 = p1r2 s1/0
  s1/2 = p1r2 s1/1
  s1/3 = p1r3 s1/0

  [[router p1r2]]
  f0/0 = LAN 1

  [[router p1r3]]
  f0/0 = LAN 1

  [[ROUTER p12r1]]
  f0/0 = LAN 2

  [[router p12r2]]
  f0/0 = LAN 2

# No need to specify an adapter here, it is taken care of
# by the interface specification under Router R1
```

Laboratorio de encapsulamiento PPP

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

f0/0 = LAN 1

s1/0 = Miami s1/0

s1/1 = Londres s1/1

s1/2 = Lima s1/0

[[router Miami]]

f0/0 = LAN 2

s1/1 = Londres s1/0

s1/2 = Londres s1/2

[[router Londres]]

f0/0 = LAN 3

[[router Lima]]

f0/0 = LAN 4

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

by the interface specification under Router R1

Laboratorio de encapsulamiento Frame Relay

Simple lab

[localhost]

[[7200]]

image = \Archivos de programa\Dynamips\images\c7200-js-mz.124-13b.image

On Linux / Unix use forward slashes:

image = /opt/7200-images/c7200-jk9o3s-mz.124-7a.image

npe = npe-400

ram = 160

[[ROUTER Quito]]

s1/0 = Lima s1/0

s1/1 = Caracas s1/0

s1/2 = Londres s1/0

s1/3 = Miami s1/0

[[ROUTER Lima]]

F0/0 = LAN 1

[[ROUTER Caracas]]

F0/0 = LAN 2

[[ROUTER Miami]]

F0/0 = LAN 3

[[ROUTER Londres]]

F0/0 = LAN 4

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

by the interface specification under Router R1

Tabla de Costos en enlaces usados por OSPF:

Tipo de enlace y ancho de banda	Costo
Enlace serial de 56 Kbps	1785
Enlace serial T1 1.544 Mbps	64
Enlace serial E1 2.048 Mbps	48
4 Mbps Token Ring	25
Ethernet de 10 Mbps	10
16 Mbps Toquen Ring	6
100 Mbps Fast Ethernet FDDI	1

En la tabla se muestra el costo asignado por defecto por OSPF basado en el ancho de banda de cada enlace.

REFERENCIAS BIBLIOGRÁFICAS

1. **Tanenbaum, Andrew S.** *Redes de Computadoras*. México : Pearson Educación, 2003.
2. **Academy Resources-Training Resources-Cisco Systems.** [En línea] [Citado el: 13 de Agosto de 2007.] <http://www.cisco.com/web/learning/netacad/index.html>.
3. **Wikipedia.** Wikipedia. [En línea] 4 de Septiembre de 2007. [Citado el: 11 de Septiembre de 2007.] <http://wikipedia.org/>.
4. **MediaWiki.** [En línea] 26 de Mayo de 2007. [Citado el: 10 de Agosto de 2007.] http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator.
5. **Rubio, Sergio.** Dynagen. [En línea] 2006-2007. [Citado el: 15 de Agosto de 2007.] <http://dynagen.org/>.
6. **Degioanni, Loris, y otros.** WinPcap: The Windows Packet Capture Library. [En línea] 28 de Junio de 2007. [Citado el: 15 de Agosto de 2007.] <http://www.winpcap.org/>.
7. **CiscoPress.** [En línea] [Citado el: 13 de Agosto de 2007.] http://www.ciscopress.com/content/images/chap01_1587051486/elementLinks/1587051486content.pdf.
8. **Anuzelli, Greg.** Dynagen. [En línea] 2006-2007. [Citado el: 2 de Septiembre de 2007.] <http://dynagen.org/>.
9. **Navarra, Universidad Publica de.** Tipos de Protocolo de enrutamiento. [En línea] 25 de Septiembre de 2007. <http://helios.tlm.unavarra.es/asignaturas/lpr/0506/slides/clase7-TiposRouting.pdf>.
10. **Gerald Combs.** Wireshark. [En línea] 2006-2007. [Citado el: 27 de Septiembre de 2007.] <http://www.wireshark.org/download.html>.
11. **Paquet, Catherine y Teare, Diane.** *CCNP Self Study*. Indianapolis : Cisco Press, 2003.

FECHA DE ENTREGA

Sangolquí, _____

Sr. Fernando David Suárez Sánchez

C.I.: 1802117463

AUTORIDADES:

Sr. Ing. Gonzalo Olmedo

Coordinador de Carrera de Ingeniería en Electrónica y Telecomunicaciones

Sr. Dr. Jorge Carvajal Rodríguez

Secretario Académico del Departamento de Eléctrica y Telecomunicaciones