879316

UNIVERSIDAD LASALLISTA BENAVENTE

ESCUELA DE INGENIERIA EN COMPUTACION

Con Estudios Incorporados a la
Universidad Nacional Autónoma de México

CLAVE: 8793-16

"RUTEADORES: ARQUITECTURA, FUNCIONAMIENTO Y CONFIGURACION"

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

PRESENTA:

JOSE LUIS CORTES OLIVARES

ASESOR: ING. MIGUEL ANGEL JAMAICA ARREGUIN

CELAYA, GUANAJUATO MARZO 2004

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ESTA TESIS NO SALE
DE LA BIBLIOTECA

AGRADECIMIENTOS

A mis Padres
Por estar siempre a mi lado apoyándome

A mi Hermano
Por tener siempre su amistad y cariño

A Mary
Por haberme dado su amor y compresión

A mi Universidad
Por haberme dado los conocimientos adecuado para ejercer una vida profesional.

A mi Padrino Salvador
Que desde el cielo siempre siento su cariño y apoyo.

A TODOS MUCHAS GRACIAS

Autorizo a la Direccion General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.
NOMBRE: Jose Luis Cortés Olivares
FECHA: 31/marzo/04
FIRMA:

INDICE

INTRODUCCIÓN .....

CAPITULO 1. MODELO DE INTERNETWORKING Y MODELO OSI. 10

.1 LA EVOLUCION DE LA REDES 10

1.1.1 1960 Y 1970: PROCESO CENTRALIZADO 10

1.1.2 1970 Y 1980: REDES 11

1.1.3 1980 Y 1990: REDES GLOBALES 12

1.1.4 1990: REDES (APLICACIONES MÁS GRANDES) 13

1.2 OBJETIVOS DE DISEÑO DE RED 14

1.3 EL MODELO OSI 15

1.3.1 ENCAPSULACION DE DATOS Y ENCABEZADO 17

1.4 CAPA DE APLICACIÓN 19

1.5 CAPA DE PRESENTACIÓN 19

1.5.1 FORMATOS DE TEXTO Y CONVERSION 20

1.5.2 FORMATOS DE GRAFICOS Y CONVERSION 20

1.5.3 FORMATOS DE AUDIO Y VIDEO Y CONVERSION 20

1.6 CAPA DE SESIÓN 20

1.7 CAPA DE TRANSPORTE 21

1.7.1 MULTIPLEXACION 22

1.7.2 SERVICIOS DE RED ORIENTADOS A CONEXIÓN Y NO ORIENTADOS A CONEXIÓN 23

1.7.3 CONTROL DE CONGESTION 24

1.7.4 WINDOWING 24

1.7.5 ACUSE DE RECIBO POSITIVO 25

1.8 FUNCIONES BASICAS DE LAS CAPAS FÍSICAS Y DE ENLACE DE DATOS 27

1.9 ESTANDARES DE LAN Y ORGANIZACIONES 27

1.10 SUBCAPAS DE LA CAPA DE ENLACE DE DATOS 28

1.10.1 FUNCIONES DE LA SUBCAPA DE RED 28

1.10.2 FUNCIONES DE LA SUBCAPA MAC 29

1.10.3 DIRECCIONAMIENTO FISICO Y LOGICO 29

1.10.4 DIRECCIONES MAC 29

1.10.5 ENCONTRADO UNA DIRECCION MAC 30

1.11 TECNOLOGIAS COMUNES DE LAN 31

1.11.1 ETHERNET Y IEEE 802.3 31

1.11.1.1 CAPA FISICA ETHERNET/802.3 31

1.11.1.2 INTERFAZ ETHERNET/802.3 33

1.11.1.3 OPERACIÓN ETHERNET/802.3 33

1.11.1.4 BROADCAST Y MULTICAST ETHERNET/802.3 34

1.11.1.5 FORMATO DE FRAME ETHERNET/802.3 35

1.11.1.6 CONFIABILIDAD ETHERNET/802.3 36

1.11.1.7 OPCIONES ETHERNET DE ALTAVELOCIDAD 36

1.11.2 TOKEN RING/IEEE 802.5 37

1.11.2.1 CAPA FISICA TOKEN RING/802.5 38

1.11.2.2 INTERFAZ TOKEN RING/802.5 39
1.11.2.3 OPERACION DE TOKEN RING/802.5 39
1.11.3.4 CONTROL DE MEDIO TOKEN RING 40
1.11.3 FIBER DISTRIBUTE DATA INTERFACE (FDDI) 40
1.11.3.1 CAPA FISICA: FDDI 41
1.11.3.2 INTERFAZ FDDI 42
1.11.3.3 CONFIABILIDAD DE FDDI 42
1.12 TECNOLOGIAS COMUNES DE WAN 43
1.12.1 CAPA WAN: FISICA 43
1.12.2 CAPA DE ENLACE DE DATOS: PROTOCOLOS WAN 44

CAPITULO 2 CAPA DE RED Y DETERMINACIÓN DE RUTAS 45
2.1 FUNDAMENTOS DE CAPA DE RED 45
2.1.1 DETERMINACION DE UNA RUTA 45
2.1.2 INFORMACION DE LA COMUNICACIÓN DE UNA RUTA 46
2.1.3 DIRECCIONAMIENTO: RED Y NODO 47
2.1.4 VARIACIONES EN EL DIRECCIONAMIENTO DE PROTOCOLO 48
2.1.5 DIRECCIONAMIENTO DE RED TCP/IP 48
2.1.6 EL RUTEO UTILIZA DIRECCIONES DE RED 49
2.1.7 PROTOCOLOS RUTEADOS VS. PROTOCOLOS DE RUTEO 50
2.1.7.1 PROTOCOLOS RUTEADOS 50
2.1.7.2 PROTOCOLOS DE RUTEO 50
2.1.8 OPERACIONES DE PROTOCOLOS DE CAPA DE RED 51
2.1.9 RUTAS ESTÁTICAS VS. RUTAS DINAMICAS 52
2.1.10 RUTA POR DEFECTO 52
2.1.11 ADAPTANDOSE AL CAMBIO DE TOPOLOGÍA 53
2.1.12 OPERACIONES DE RUTEO DINAMICO 54
2.1.13 REPRESENTANDO DISTANCIAS CON METRICAS 54
2.2 PROTOCOLOS DE RUTEO 55
2.2.1 RUTEO DE VECTOR DISTANCIA 56
2.2.2 DESCUBRIMIENTO DE LA RED DE VECTOR DISTANCIA 56
2.2.3 CAMBIOS DE TOPOLOGIA DE VECTOR DISTANCIA 57
2.2.4 PROBLEMA: LOOPS DE RUTEO 58
2.2.5 SINTOMA: CUENTA A INFINITO 58
2.2.6 SOLUCION: DEFINIENDO UN MAXIMO 58
2.2.7 SOLUCION: SPLIT HORIZON 59
2.2.8 SOLUCION: POISON REVERSE 60
2.2.9 SOLUCION: HOLD DOWN TIMERS 60
2.2.10 SOLUCION TRIGGERED UPDATES 61
2.2.11 IMPLEMENTACION DE SOLUCIONES EN RUTAS MULTIPLES 62
2.3 ROUTING INFORMATION PROTOCOL (RIP) 63
2.3.1 METRICA DE RIP 64
2.3.2 TEMPORIZADOR DE RIP 64
2.3.3 CARACTERISTICAS DE ESTABILIDAD 65
2.3.4 FORMATO DE PAQUETE DE RIP 65

2.3.5 RIP VERSION 2 66
2.3.5.1 ETIQUETAS DE RUTA EXTERNA 67
2.3.5.2 MASCARA DE SUBRED 67
2.3.5.3 DIRECCIONES DEL PROXIMO SALTO 67
2.3.5.4 AUTENTIFICACION 67
2.3.5.5 MULTICASTING 67
2.3.6 FORMATO DE PAQUETE RIP VERSION 2 68
2.4 INTERIOR GATEWAY PROTOCOL (IGRP) 68
2.4.1 TEMPORIZADORES DE IGRP 68
2.4.2 RUTEO DE ESTADO DE ENLACE 69
2.4.3 DESCUBRIMIENTO DE LA RED DE ESTADO DE ENLACE 69
2.4.4 CAMBIOS DE TOPOLOGIA DE ESTADO DE ENLACE 70
2.4.5 PREOCUPACIONES DE ESTADO DE ENLACE 70
2.4.6 PROBLEMA: ACTUALIZACIONES DE ESTADO DE ENLACE 71
2.4.7 SOLUCION: MECANISMO DE ESTADO DE ENLACE 72
2.4.8 COMPARANDO RUTEO DE VECTOR DISTANCIA CON RUTEO DE ESTADO DE ENLACE 72
2.4.9 RUTEO HIBRIDO 73
2.5 OPEN SHORTEST PATH FIRST (OSPF) 74
2.5.1 ALGORITMO OSPF 74
2.5.2 FORMATO DE PAQUETE OSPF 75
2.6 PROCESOS BÁSICOS DE RUTEO 76
2.7 RUTEO LAN-TO-LAN 76
2.8 RUTEO LAN-TOWAN 77

CAPITULO 3 DESCRIPCION DE TCP/IP 79
3.1 CAPAS DEL PROTOCOLO TCP/IP 80
3.2 DESCRIPCION DE LA CAPA DE APLICACIÓN 81
3.3 DESCRIPCION DE LA CAPA DE TRANSPORTE 81
3.3.1 FORMATO DE SEGMENTO TCP 82
3.3.2 NUMEROS DE PUERTO 83
3.4 DESCRIPCION DE LA CAPA DE INTERNET 84
3.4.1 DATAGRAMA IP 84
3.4.2 INTERNET CONTROL MESSAGE PROTOCOL (ICMP) 86
3.4.3 PROBANDO ICMP 87
3.4.4 ADDRESS RESOLUTION PROTOCOL 88
3.4.5 REVERSE ARP 88

CAPITULO 4 RUTADORES COMERCIALES
4.1 1700 SERIES 89
4.1.1 CARACTERÍSTICAS CLAVE 89
4.2 2500 SERIES 90
4.2.1 CARACTERISTICAS CLAVE 90
4.2.2 ESPECIFICACIONES 90
4.3 2600 SERIES 92
4.3.1 CARACTERISTICAS CLAVE 93
4.3.2 ESPECIFICACIONES 93

4.4 3600 SERIES 95
4.4.1 CARACTERISTICAS CLAVE 95
4.4.2 ESPECIFICACIONES 95

CAPITULO 5 TAREAS PRELIMINARES EN UN RUTEADOR 98
5.1 INICIALIZANDO UN RUTEADOR 98
5.1.1 FUENTES DE CONFIGURACION EXTERNAS 98
5.1.2 COMPONENTES INTERNOS DE CONFIGURACION 99
5.1.3 DESCRIPCION DEL SISTEMA DE INICIALIZACION 99
5.2 ACCESANDO LA INTERFAZ DE USUARIO 101
5.2.1 MODOS DE RUTEADOR 101
5.2.2 ENTRANDO EN EL RUTEADOR 102
5.2.3 UTILIZANDO PASSWORD 102
5.2.5 PASSWORDS DE LINEA INDIVIDUAL 102
5.2.4 PASSWORDS DE MODE EXEC PRIVILEGIADO 102
5.2.6 PASSWORD ENCRIPTADO 102
5.2.7 LISTA DE COMANDOS DE MODO USUARIO 103
5.2.8 LISTA DE COMANDOS DE MODO PRIVILEGIADO 104
5.2.9 AYUDA DE CONTEXTO 104
5.2.10 UTILIZANDO COMANDOS ENHANCED EDITING 105
5.2.11 REVISANDO LA HISTORIA DE COMANDO 105
5.3 EXAMINADO EL ESTADO DEL RUTEADOR 106
5.3.1 COMANDO SHOW VERSION 107
5.3.2 COMANDOS SHOW STARTUP-CONFIG Y SHOW RUNNING-CONFIG 107
5.3.3 COMANDO SHOW INTERFACES 108
5.3.4 COMANDOS SHOW PROTOCOLS 109

CAPITULO 6 CONFIGURACION DE UN RUTEADOR 111
6.1 CARGANDO ARCHIVOS DE CONFIGURACION 111
6.1.1 CARGANDO ARCHIVOS DE CONFIGURACION DESDE UN SERVIDOR 112
6.2 TAREAS FUNDAMENTALES DE CONFIGURACIÓN 113
6.2.1 DESCRIPCION DE LOS MODOS DE CONFIGURACION DEL RUTEADOR 113
6.2.2 CONFIGURANDO LA IDENTIFICACION DEL RUTEADOR 114
6.2.3 CONFIGURACION DE PASSWORD 115
6.2.4 PASSWORD DE CONSOLA 116
6.2.5 PASSWORD DE TERMINAL VIRTUAL 116
6.2.6 PASSWORD DEL MODO PRIVILEGIADO 116
6.2.7 ENCRIPTACION DE PASSWORD 116
6.2.8 CONFIGURACION Y MANEJO DE UNA INTERFAZ 117
6.2.9 COMANDO SHOW INTERFACES 117
6.2.10 INTERPRETANDO EL ESTADO DE LA INTERFAZ 118
6.2.11 CONFIGURANDO UNA LINEA SERIAL 119
6.2.12 DETERMINADO EL ESTADO DE DTE/DCE 120
6.2.13 VERIFICANDO LOS CAMBIOS 121

6.2.14 DANDO DE BAJA UNA INTERFAZ 122
6.3 MANEJANDO EL AMBIENTE DE CONFIGURACIÓN 122
6.3.1 LOCALIZACION DEL CISCO IOS SOFTWARE 122
6.3.2 DETERMINANDO EL VALOR DE REGISTRO DE CONFIGURACION ACTUAL 123
6.3.3 OPCIONES DE BOOT SYSTEM EN SOFTWARE 125
6.3.4 PREPARANDO UN RESPALDO DE IMAGEN DE SISTEMA ... 126
6.3.5 OBSERVANDO LA MEMORIA DISPONIBLE Y EL NOMBRE DEL ARCHIVO DE LA IMAGEN 127
6.3.6 CREANDO UN RESPALDO DE IMAGEN DE SOFTWARE 127
6.3.7 ACTUALIZANDO LA IMAGEN DE SISTEMA DESDE LA RED 128
6.3.8 SOBREESCRIBIENDO LA IMAGEN EXISTENTE 129
6.3.9 CREANDO O CAMBIANDO UNA CONFIGURACION UTILIZANDO EL COMANDO SETUP 130
6.3.10 PARAMETROS DEL MODO SETUP GLOBAL 131
6.3.11 PARAMETROS DEL MODO SETUP DE INTERFAZ 131
6.3.12 REVISANDO EL SCRIPT DEL MODO SETUP 133
6.4 MECANISMOS BASICOS Y COMANDOS DE RUTEO IP 134
6.4.1 CREANDO UNA TABLA DE RUTEO INICIAL 134
6.4.2 ENTENDIENDO LA MANERA EN QUE EL RUTEO IP APRENDE DESTINOS 135
6.4.3 ESPECIFICANDO LOS VALORES DE DISTANCIA ADMINISTRATIVA 135
6.4.4 CONFIGURANDO RUTAS ESTATICAS 137
6.4.5 CONFIGURANDO RUTEADORES POR DEFECTO 138
6.4.6 AGRUPANDO EN SISTEMAS ATÓNOMOS 139
6.4.7 UTILIZANDO PROTOCOLOS DE RUTEO INTERIOR Y EXTERIOR 140
6.4.7.1 PROBLEMAS DE PROTOCOLOS DE RUTEO 141
6.4.7.2 PROTOCOLOS DE RUTEO INTERIOR 141
6.4.8 COMPLETANDO LAS TAREAS DE CONFIGURACION DE RUTEO IP 142
6.4.9 CONFIGURANDO RUTEO DINAMICO 142
6.4.10 CONFIGURANDO RIP 143
6.4.10.1 COMANDOS DE CONFIGURACION DE RIP 144
6.4.10.2 VISTA DE LA INFORMACION DE RIP 145
6.4.11 CONFIGURANDO IGRP 147
6.4.11.1 ENTENDIENDO LA OPERACIÓN DE IGRP 147
6.4.11.2 UTILIZANDO LA METRICA COMPUESTA DE IGRP 148
6.4.11.3 CARACTERISTICA DE BALANCE DE CARGAS DE COSTO DESIGUAL 149
6.4.11.4 CREANDO UN PROCESO DE RUTEO IGRP 150
6.4.11.5 DESPLEGANDO INFORMACION DE RUTEO IGRP 152
6.5 CONFIGURACION DE NOVELL IPX 154
6.5.1 RUTEADORES CISCO CON REDES NETWARE 154

6.5.2 CONJUNTO DE PROTOCOLOS DE NOVELL NETWARE 155
6.5.3 CARACTERÍSTICA CLAVE DE NOVELL NETWARE 156
6.5.4 DIRECCIONAMIENTO NOVELL IPX 157
6.5.5 DETERMINANDO UNA DIRECCION IPX 157
6.5.6 MULTIPLES ENCAPSULACIONES NOVELL 158
6.5.7 NOVELL UTILIZA RIP PARA RUTEO 159
6.5.8 SAP: SOPORTANDO LA PUBLICACION DE SERVICIOS 160
6.5.9 GNS: PROCESO GET NEAREST SERVER 161
6.5.10 CONFIGURACION RUTEO IPX 162
6.5.10.1 COMANDOS DE CONFIGURACION GLOBAL 162
6.5.10.2 COMANDOS DE CONFIGURACION DE INTERFAZ 163
6.5.10.3 EJEMPLO DE CONFIGURACION IPX 163
6.5.11 VERIFICANDO Y MONITOREADO EL RUTEO IPX 164
6.6 ADMINISTRACION CON LISTAS DE ACCESO 169
6.6.1 ¿POR QUÉ UTILIZAR LISTAS DE ACCESO? 169
6.6.2 ¿CÓMO TRABAJAN LAS LISTA DE ACCESO? 171
6.6.3 UNA LISTA DE PRUEBAS: NEGAR O PERMITIR 172
6.6.4 DESCRIPCION DEL COMANDO ACCESS LIST 172
6.6.5 IDENTIFICACION DE LISTAS DE ACCESO 173
6.7 LISTAS DE ACCESO TCP/IP 174
6.7.1 PREPARANDO PAQUETES CON LISTAS DE ACCESO IP 174
6.7.2 CONCEPTOS CLAVE PARA LISTAS DE ACCESO 174
6.7.3 USO DE MASCARA WILDCARD 174
6.7.4 CORRESPODENCIA CON CUALQUIER DIRECCIONAMIENTO IP 176
6.7.5 CORRESPONDIENDO UNA DIRECCION DE HOST ESPECIFICA 177
6.7.6 CONFIGURACION DE LISTAS DE ACCESO ESTANDAR 178
6.7.6.1 EJEMPLO 1: PERMITIR SOLO MI RED 178
6.7.6.2 EJEMPLO 2: NEGAR UN HOST ESPECÍFICO 179
6.7.6.3 EJEMPLO 3: NEGAR UNA SUBRED ESPECÍFICA 180
6.7.7 LISTA DE ACCESO EXTENDIDAS 181
6.7.8 CONFIGURACION DE LISTA DE ACCESO EXTENDIDAS 181
6.7.8.1 EJEMPLO 1: NEGAR FTP PARA E0 182
6.7.8.2 EJEMPLO 2: DENEGAR SOLO TELNET FUERA DE E0 183
6.7.9 NOMBRAMIENTO DE LISTA DE ACCESO 184
6.7.10 ¿DÓNDE SE UTILIZAN LAS LISTAS DE ACCESO? 185
6.7.11 VERIFICANDO LISTA DE ACCESO 186
6.7.12 MONITOREANDO DECLARACIONES DE LISTA DE ACCESO
6.8 LISTAS DE ACCESO IPX 187
6.8.1 PROBANDO PAQUETES UTILIZANDO LISTA DE ACCESO NOVELL IPX 187
6.8.2 CONCEPTOS CLAVE PARA LISTAS DE ACCESO IPX 188
6.8.3 CONTROLANDO LA SOBRECARGA DE IPX 188
6.8.4 CONFIGURACION DE LISTAS DE ACCESO ESTANDAR IPX 189
6.8.4.1 EJEMPLO DE LISTA DE ACCESO IPX ESTANDAR 190
6.8.5 CONFIGURACION DE LISTA DE ACCESO EXTENDIDAS 191

6.8.6 OPERACIÓN NORMAL DE IPX SAP 192
6.8.7 USO DE LOS FILTRO SAP 193
6.8.8 COMANDOS DE CONFIGURACION DE FILTROS SAP 194
6.8.8.1 EJEMPLO1: FILTRADO DE SAP EN SALIDA 195
6.8.8.2 EJEMPLO 2: FILTRO SAP DE ENTRADA 196
6.8.9 VERIFICANDO LAS LISTAS DE ACCESO IPX 197

CAPITULO 7 INTRODUCCION A LAS CONEXIONES DE WAN 198
7.1 SERVICIOS DE WAN 198
7.1.1 INTERCONECTANDO CON LOS PROVEEDORES DE SERVICIOS WAN 199
7.1.1.1 CUSTOMER PREMISES EQUIPMENT 200
7.1.1.2 DEMARCACION 200
7.1.1.3 LOCAL LOOP 200
7.1.1.4 SWITCH DE CO 200
7.1.1.5 RED TOLL 200
7.1.2 DE LA ORGANIZACIÓN SOLICITADORA A LA INTERFAZ DEL PROVEEDOR DE SERVICIOS 201
7.1.3 UTILIZANDO LOS SERVICIOS WAN CON RUTEADORES 202
7.1.4 RESUMEN DEL FORMATO DE FRAME WAN 203
7.2 UNA DESCRIPCION DE PPP 204
7.2.1 ELEMENTOS DE CAPA PPP 204
7.2.2 OPCIONES DE CONFIGURACION DE LCP 205
7.2.3 ESTABLECIMIENTO DE SESION PPP 206
7.2.4 SELECCIONANDO UN PROTOCOLO DE AUTENTIFICACION PPP 207
7.2.4.1 PAP 207
7.2.4.2 CHAP 208
7.2.5 CONFIGURANDO LA AUTENTIFICACION PPP 208
7.2.6 VERIFICANDO PPP 210
7.3 CONFIGURACION X.25 210
7.3.1 DESCRIPCION DE X.25 210
7.3.2 PROTOCOLOS X.25 211
7.3.3 DTE Y DCE X.25 212
7.3.4 FORMATO DE DIRECCIONAMIENTO X.25 (X.121) 213
7.3.5 ENCAPSULACIÓN X.25 214
7.3.6 CIRCUITOS VIRTUALES X.25 215
7.3.7 USO DE SVC 216
7.3.8 CIRCUITO VIRTUAL DE UN PROTOCOLO SIMPLE 216
7.3.9 CIRCUITOS VIRTUALES MULTIPROTOCOLOS 217
7.3.10 CONFIGURANDO X.25 217
7.3.10.1 COMANDO ENCAPSULATION X.25 218
7.3.10.2 COMANDO X.25 ADDRESS 218
7.3.10.3 COMANDO X.25 MAP 218
7.3.11 EJEMPLO DE CONFIGURACION X.25 219
7.3.12 TAREAS ADICIONALES DE CONFIGURACION 220

7.3.13 CONFIGURACION DE RANGOS DE CIRCUITOS VIRTUALES X.25 220
7.3.14 CONFIGURANDO TAMAÑOS DE PAQUETES X.25 221
7.3.15 CONFIGURANDO LOS PARAMETROS DE VENTANA X.25 222
7.3.16 EJEMPLO DE CONFIGURACION ADICIONAL X.25 223
7.3.17 CONFIGURANDO UN RUTEADOR COMO UN SWITCH 223
7.3.18 X.25 LOCAL Y SWITCH XOT 224
7.3.19 MONITOREANDO X.25 225
7.4 CONFIGURACION FRAME RELAY 226
7.4.1 DESCRIPCION DE FRAME RELAY 226
7.4.2 TERMINOLOGIA FRAME RELAY 227
7.4.2.1 RANGO DE ACCESO LOCAL 227
7.4.2.2 DATA-LINK CONNECTION IDENTIFIER (DLCI) 227
7.4.2.3 LOCAL MENAGEMENT INTERFACE (LMI) 228
7.4.2.4 COMMITED INFORMATION RATE (CIR) 228
7.4.2.5 SOBRESATURACION 228
7.4.2.6 COMMITED BURST (Bc) 228
7.4.2.7 EXCESS BURST 228
7.4.2.8 FORWARD EXPLICIT CONGESTION NOTIFICATION (FECN) 229
7.4.2.9 BACKWARD EXPLICIT CONGESTION NOTIFICATION (BECN) 229
7.4.2.10 DISCARD ELIGIBILITY (DE) INDICATOR 229
7.4.3 OPERACION FRAME RELAY 229
7.4.4 CONFIGURANDO FRAME RELAY 231
7.4.5 COMANDO DE CONFIGURACION OPCIONAL 232
7.4.6 VERIFICANDO LA OPERACION FRAME RELAY 234
7.4.7 SELECCIONANDO UNA TOPOLOGÍA DE FRAME RELAY 234
7.4.7.1 TOPOLOGIA DE ESTRELLA 235
7.4.7.2 TOPOLOGIA FULL-MESH 235
7.4.7.3 TOPOLOGIA PARTIAL-MESH 235
7.5 ACCESIBILIDAD Y RECURSOS DISTRIBUIDOS PARA FRAME RELAY 235
7.6 RESOLVIENDO LA ACCESIBILIDAD Y RECURSOS DISTRIBUIDOS: SUBINTERFACES 236
7.7 CONFIGURANDO SUBINTERFACES 237
7.8 EJEMPLO DE CONFIGURACION DE SUBINTERFACES MULTIPUNTO 238
7.9 EJEMPLO DE CONFIGURACION DE SUBINTERFACES PUNTO A PUNTO 239

CONCLUSION .....

BIBLIOGRAFIA .....

INTRODUCCION

- **PANORAMA GENERAL**

Actualmente vivimos en la era de las comunicaciones, debido a que en las últimas décadas las tecnologías en sistemas de comunicación se han desarrollado a pasos agigantados jugando un papel importante en el desarrollo y progreso de la humanidad.

En el ambiente de los negocios, el acceso inmediato a los datos es la clave para que las pequeñas y mediana empresas tengan éxito, por eso se crearon las REDES GLOBALES[1].

Las redes globales crecen y se expanden para soportar múltiples sitios, protocolos, sistemas operativos, la interconexión de dispositivos que son elementos críticos a lo largo de una red de datos. Entendiendo estos dispositivos, su configuración y la integración de ellos en diseños de redes eficientes y confiables se concluye que son esenciales para cualquier soporte de comunicación de red.

- **OBJETIVO PRINCIPAL**

El objetivo principal de este trabajo es que el lector entienda la arquitectura, el funcionamiento y aprenda la configuración de estos dispositivos de redes llamados "ruteadores". Nos enfocaremos específicamente a los ruteadores de Cisco Systems.

- **CISCO SYSTEMS**

La empresa Cisco Systems, Inc. es el líder en el mundo de redes para Internet. Los ruteadores de Cisco con la base del 80% de la infraestructura de Internet y el 60% para soluciones de acceso utilizados por las compañías para proveer conectividad a los usuarios remotos y conectividad a Internet. Además, Cisco, conduce al camino de las soluciones de tecnologías LAN de alto desempeño.

Las soluciones de Cisco diseñadas para la pequeña y mediana empresa ayudan a maximizar los negocios potanciales.

---

[1] Las redes globales son una colección de redes individuales conectadas por dispositivos de red intermedios que funciona como una sola red y así se puede compartir y pasar información de una red a otra.

CAPITULO 1

MODELO DE INTERNEWORKING Y MODELO OSI

1.1 EVOLUCION DE LAS REDES

La evolución de redes es, a grandes rasgos, una evolución de funciones y capacidades. Cada nueva fase en la evolución de red se incorpora y expande en la funcionalidad (tales como métodos de comunicación y velocidades de acceso) de la fase anterior, empezando en 1960 y continuando hasta los días presentes.

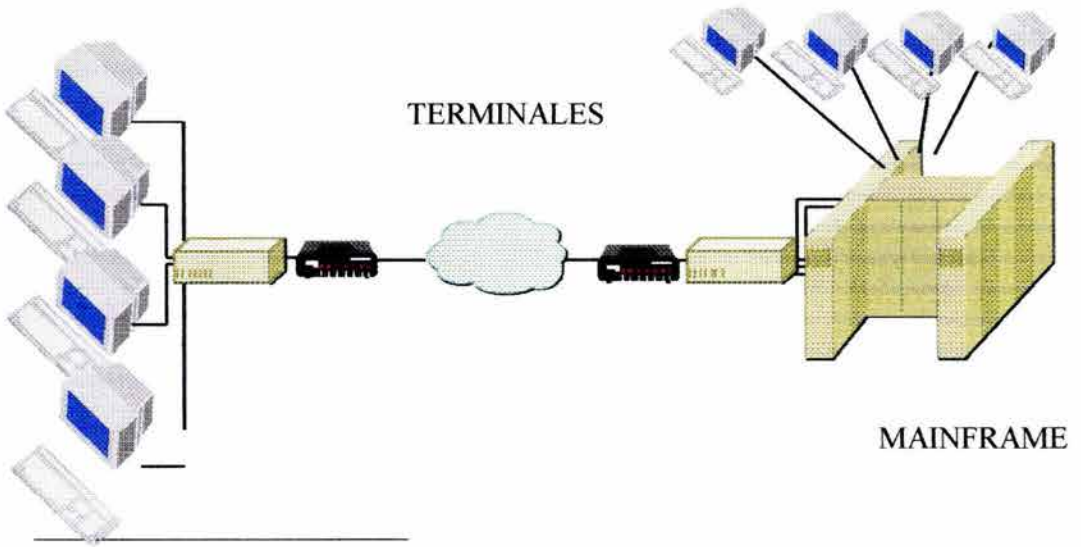
1.1.1 1960 y 1970: PROCESO CENTRALIZADO

En 1960 y principios de 1970, la comunicación de computadoras estaba organizada en forma de terminales tontas conectadas a un host (mainframe) y el poder de procesamiento y toda la memoria pertenecía al host.

El ambiente de proceso centralizado requiere de líneas de acceso de baja velocidad que las terminales utilizan para conectarse con el host y así era posible que los usuarios accesarán datos centralizados compartidos y recursos de impresión.

Las computadoras IBM con sistemas de redes SNA[2] y computadoras que no son de IBM con X.25[3] público son ejemplos típicos de este tipo de arquitectura de red. La figura 1.1 muestra una comunicación simple basada en host.

FIGURA 1.1



[2] System Network Arquitecture. Aquitectura de red desarrollada por IBM en 1970.
[3] Tecnología de comunicación para redes WAN.

En una sola computadora, acceso a los recursos, ejecución de programas y copia de archivos son relativamente tareas directas. La computadora debe de identificar la solicitud del usuario y el dispositivo deseado o programa y coordinar el acceso entre ellos. La sola computadora en este escenario es el maestro de todos los recursos y así puede coordinar y manejar fácilmente los recursos.

En una red, la cual consiste en dos computadoras, la coordinación de recursos es más compleja. La transferencia de información requiere de direccionamiento, detección de errores, corrección de errores, sincronización y coordinación, entre otras.

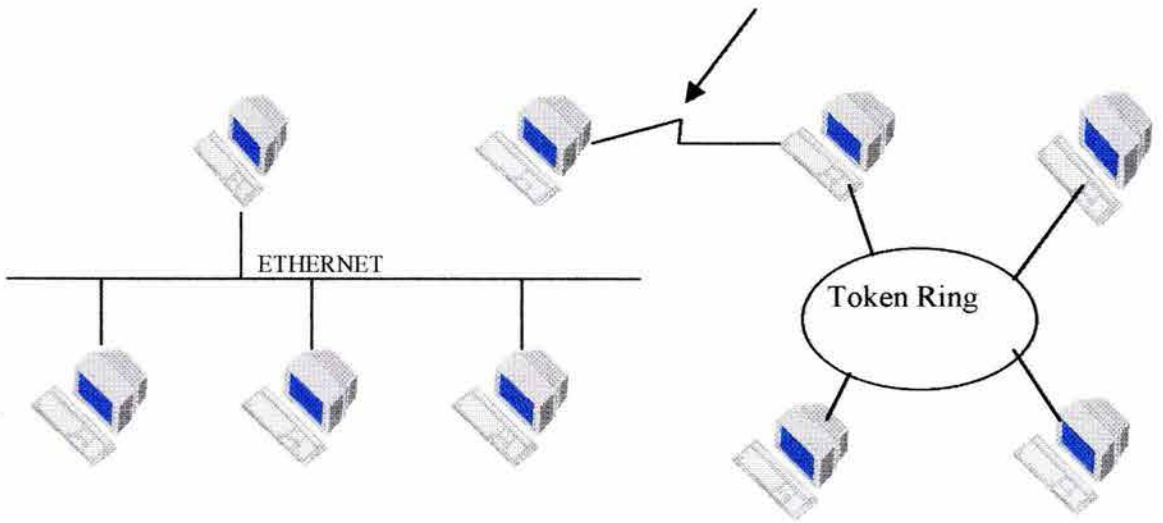
1.1.2 1970 y 1980: REDES

La introducción de PCs revolucionó la comunicación tradicional y las redes de computadoras. Inicialmente, las PCs fueron dispositivos aislados que colocaban capacidades de procesamiento y amplia memoria en cada escritorio de usuario. Conforme los negocios crecían el uso de estos dispositivos se acrecentaba.

Sin embargo, algunos recursos de red (tales como impresoras y discos duros para grandes aplicaciones) no eran un costo eficiente para cada escritorio. Las redes LAN se desarrollaron primeramente para compartir recursos y permitieron la combinación de las mejores características de las PCs aisladas y el proceso centralizado, entonces la importancia de conectar redes rápidamente fue realizada, como muestra la figura 1.2.

La interconexión de redes proporciona la base para grandes aplicaciones (como correo electrónico y transferencia de archivos) que aumentaron la productividad y la competitividad de compañías.

FIGURA 1.2



Además de PCs y redes LAN, las minicomputadoras y las redes WAN también se desarrollaron en esta década. Las minicomputadoras, frecuentemente localizadas fuera de la central de datos, facilitaron la aparición de la información distribuida, permitiendo que el proceso de la información ocurra fuera de la minicomputadora en una terminal que soporte un procesador. Las redes DECnet[4] son un ejemplo de redes de esta década.

Sin embargo, aplicaciones de diferentes ambientes de comunicación (como el Mainframe y ambiente LAN), siguen siendo independientes. Diferentes protocolos de comunicación fueron desarrollados para soportas comunicaciones entre varios ambientes. Por ejemplo, el sistema Mainframe usa SNA como método de comunicación, mientras algunas redes LAN utilizan IPX/SPX (Internetwork Packet Exchange/Sequence Packet Exchange) de Novell y TCP/IP (Transmisión Control Protocol/Internet Protocol) como métodos de comunicación.

IPX/SPX y TCP/IP fueron desarrollados para permitir conexiones entre múltiples redes a través de ruteadores.

1.1.3 1980 y 1990: REDES GLOBALES

Las redes globales enlazan redes LAN y redes WAN, sistemas operativos y una gran variedad de diferentes dispositivos unidos para formar una infraestructura de comunicaciones. Por ejemplo, la figura 1.3 muestra una red que consiste de Mainframes, PCs unidos por una gran variedad de interconexiones a través de enlaces públicos o privados (Internet). Las redes globales mueven la información a donde sea dentro de una corporación a los socios y/o a los clientes externos. Sirviendo como una carretera de información de una organización, las redes globales se han convertido en la clave estratégica y en una gran ventaja competitiva.

Los ruteadores son un elemento clave en este tipo de redes porque ellos permiten o niegan la comunicación entre redes LAN y WAN. Debemos entender cómo podemos configurar un ruteador y seleccionar el protocolo de ruteo más apropiado para la internetwork.

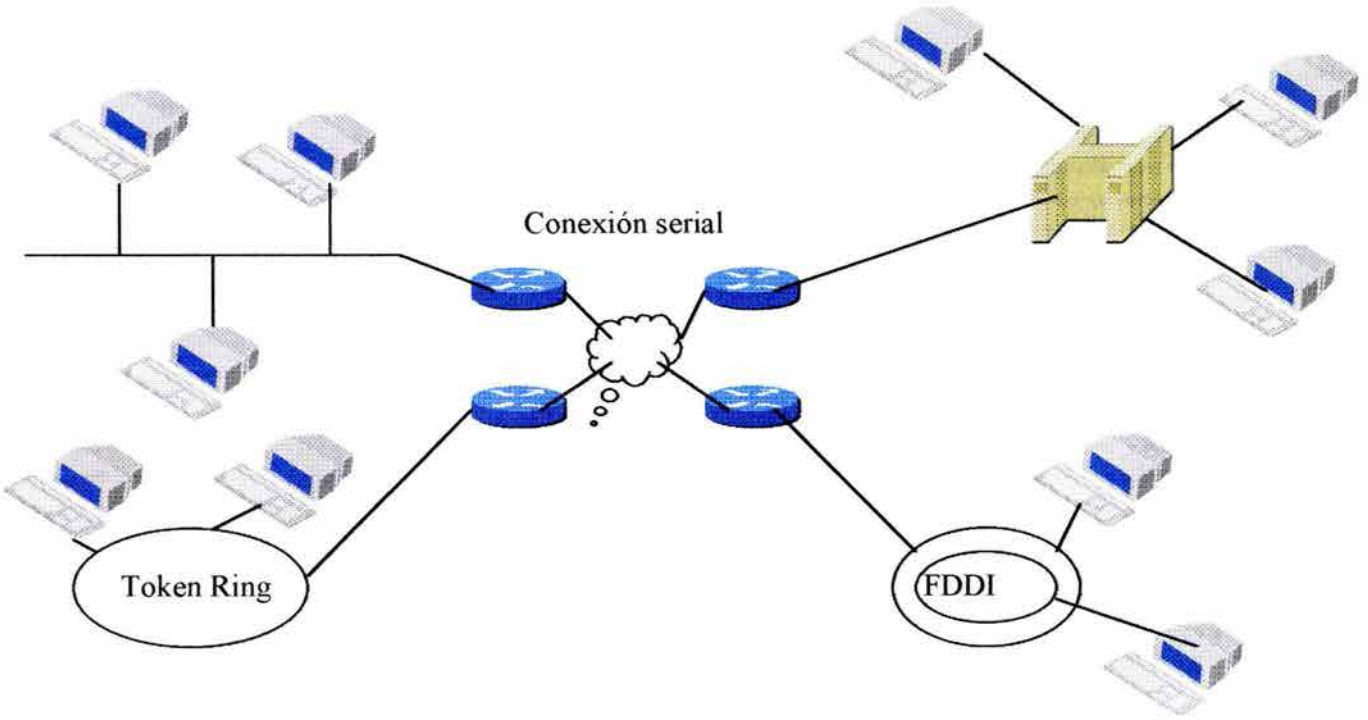
Las redes globales de hoy combinan una gran variedad de dispositivos, tipos de medio y métodos de transmisión. Para algunas compañías las redes de hoy son una mezcla de tecnologías viejas y nuevas, por ejemplo, las redes viejas de IBM puede operar virtualmente en paralelo con las nuevas redes LAN interconectadas.

La comunicación entre computadoras en la mayoría de las organizaciones esta cambiando rápidamente en respuesta a las nuevas tecnologías desarrollando requerimientos de negocios y la necesidad de transferencias de información. Para satisfacer estos requerimientos estas redes globales deben ser flexibles, escalables y adaptables para satisfacer cualquier nivel de organización (sucursal, regional o corporativo). Tambien debe

[4] Grupo de productos de comunicaciones desarrollado y soportado por Digital Equipment Corporation.

ser cuidadosamente diseñado para reflejar modelos de tráfico de red para evitar congestiones en el medio.

FIGURA 1.3



Los ingenieros y administradores de red deben saber y entender cómo los paquetes de datos son ruteados a través de la red para asegurar que un sistema de interconexión eficiente esté funcionado en óptimas condiciones para manejar las demandas de red.

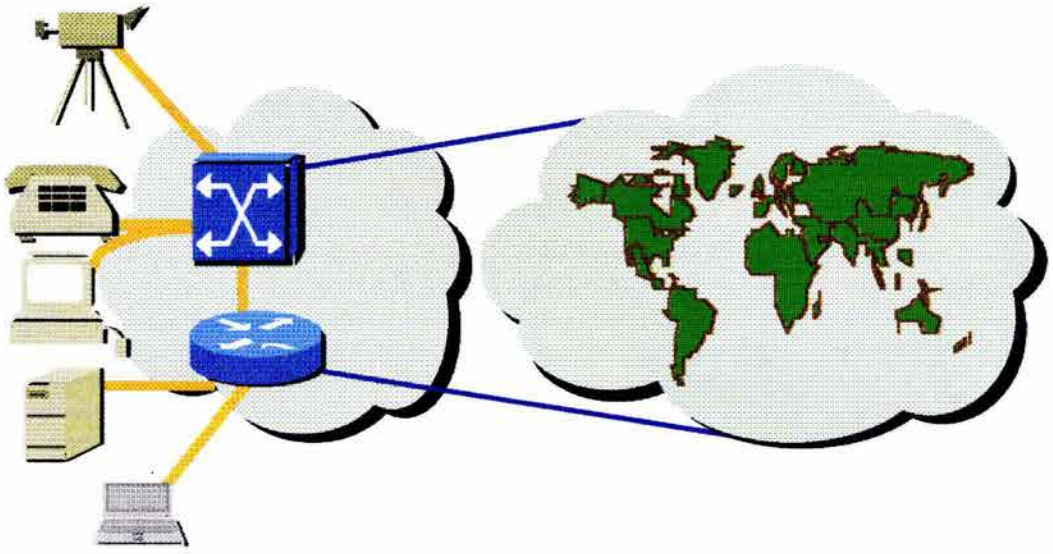
1.1.4 1990: REDES (APLICACIONES MÁS GRANDES)

La más grande urgencia en redes del futuro inmediato es la globalización de negocios y el soporte a aplicaciones requeridas para dirigir los negocios internamente. No es inusual ahora encontrar que una compañía requiera de 100 aplicaciones para funcionar en una red global.

Estudios muestran que las redes cada vez más requieren de más ancho de banda para soportar aplicaciones y conexiones y para resolver demandas de solicitudes por parte de los usuarios ya que ahora existe una intergración muy importante de voz, datos y video dentro de una misma red. Considere la figura 1.4 como ejemplo, esta red global soporta una gran variedad de dispositivos y aplicaciones que tienen un ancho de banda variante y requieren de velocidades más altas. En caso de flujo de video, transferencia de audio y transferencia

de gráficos pesados, la ruta del dato debe proveer de una comunicación confiable bajo tecnología ATM[5] por ejemplo.

FIGURA 1.4



Las siguientes son características de las redes globales:

- Incremento en uso de gráficos e imágenes.
- Archivos grandes.
- Aplicaciones grandes.
- Procesamiento Cliente/ servidor.
- Tráfico pesado.

Una red global proveerá una ambiente de aplicaciones que requieran mayores cantidades de ancho de banda. Algunas de estas aplicaciones son dirigidas hacia la evolución de requerimientos de multimedia que tienen imágenes de alta definición, video o un componente de audio digitalizado.

1.2 OBJETIVOS DE DISEÑO DE RED

Sin importar si es de área local o si es de área amplia una red es una colección de software y hardware. Como se mencionó anteriormente, las redes globales de hoy y las redes globales del futuro deben ser bien diseñadas para satisfacer las únicas necesidades de la organización que ellas soportan. El papel del administrador de red es crear y definir un diseño de red.

[5] Asyncronus Transfer Mode. Es un estándar internacional que soporta voz, datos y video.

El administrador debe cumplir con cuatro objetivos de diseño:

- **Conectividad:** Las redes globales deben servir a las organizaciones que dependan de ellas. Sin importar el rango de conexiones del medio, la velocidad de transmisión y otros detalles técnicos, el diseño de red conecta los recursos previamente separados.
- **Confiabilidad de desempeño:** La organización llega a ser más independiente en herramientas de red, la habilidad para distribuir las actualizaciones de software de red, monitoreo de desempeño operaciones redundantes y de respaldo y las funciones acceso seguro a algún recurso. Hacer confiable una red es crítico para asegurar que la organización opere competitivamente.
- **Control de administración:** Una red global provee de funciones cruciales y también consumen recursos críticos. Los administradores se preguntan cómo ellos pueden mejorar los controles de administración por medio de tareas como medición de desempeño y análisis, reporte de seguridad. Después de que la red está diseñada y operando, se sigue con la localización de errores, si lo hay.
- **Escalabilidad:** La flexibilidad es un importante objetivo en el diseño de una red. La expansión y consolidación requieren vencer las fronteras físicas y geográficas. También, como las organizaciones buscan medios para ofrecer nuevos servicios y productos para una red accesible, ellas recurrirán a nuevas o diferentes aplicaciones de red. Las redes deben ser diseñadas para que puedan ser escalables.

1.3 EL MODELO OSI

Para que una red global opere, sus dispositivos deben ser capaces de comunicarse unos con otros. La industria de redes utiliza un modelo, el modelo OSI[6] que provee normas para comunicación entre dispositivos. Esta sección muestra el concepto de encapsulación de datos y la forma de viajar a través de las capa del modelo OSI.

Las funciones de ruteo ocurren en la capa de red del modelo OSI, por lo tanto la capa de red es muy importante en este documento, sin embargo, todas las capas del modelo OSI son resumidas aquí porque se necesita entender los procesos de comunicación en las redes.

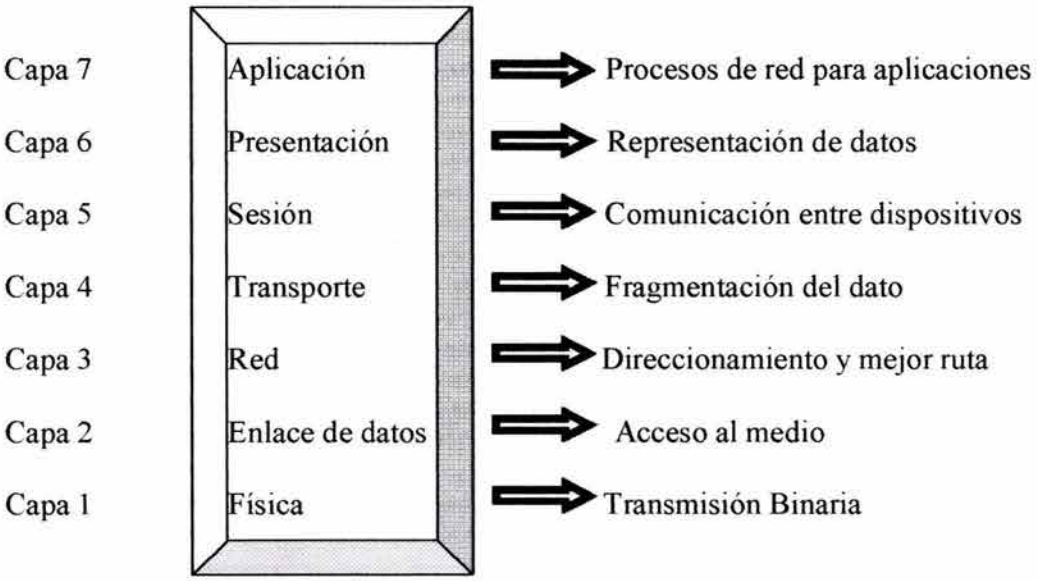
En la mayoría de los ambientes de comunicación se separa funciones de red del proceso de aplicación. La separación de las funciones de red se llama "LAYERING".

En al figura 1.5 se muestran las siete capas del modelo OSI.

---

[6] Open System Interconnection. Es un programa internacional creado por ISO para desarrollar estándares para facilitar la comunicación entre dispositivos de red.

FIGURA 1.5



CAPA DE APLICACIÓN: La capa de aplicación provee servicios de red para las aplicaciones.

CAPA DE PRESENTACIÓN: La capa de presentación representa datos y formatos de código. Esto asegura que el dato que llega de la red pueda ser usado por una aplicación y garantiza que la información enviada por la aplicación pueda ser transmitida por la red. En los ejemplos de representación incluyen ASCII, EBDCDIC, JPG, TIFF y encriptación.

CAPA DE SESION: La capa de sesión establece, mantiene y maneja sesiones entre dos aplicaciones. Por ejemplo, tareas de comienzo, terminación, interrupción, y abandono de una sesión son funciones definidas por esta capa.

CAPA DE TRANSPORTE: La capa de transporte segmenta y reensambla un dato en una secuencia de datos. Esto define la confiabilidad de la transmisión de los datos.

CAPA DE RED: La capa de red determina la mejor ruta para transmitir de una red a otra. El ruteador opera en esta capa. IP es un ejemplo de un protocolo que provee de funciones definidas por esta capa.

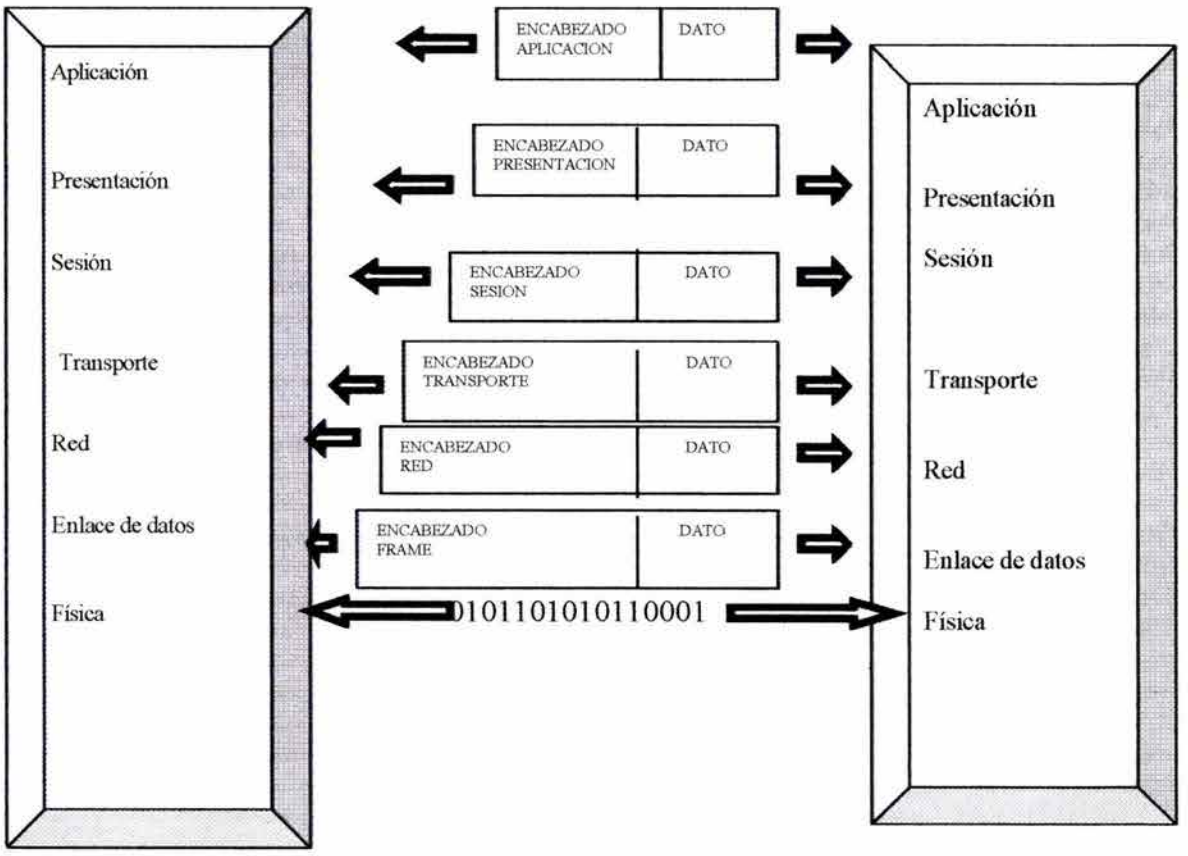
CAPA DE ENLACE DE DATOS: La capa de enlace de datos provee de transmisión física a través del medio. Maneja notificaciones, de error, topología de red, y control de flujo. Ethernet, Token Ring y FDDI son métodos de acceso al medio que ofrecen funcionalidades definidas en esta capa.

CAPA FÍSICA: La capa física provee medios eléctricos, mecánicos y funcionales para activar y mantener un enlace físico entre sistemas.

1.3.1 ENCAPSULACION DE DATOS Y ENCABEZADO

Cada capa del modelo OSI depende de la función del servicio de la capa que está debajo de ella. Para proveer un servicio las capas más bajas utilizan la encapsulación para poner el PDU[7] de las capas más altas en el campo del dato, entonces la capa inferior puede añadir encabezados que utilizará para realizar su función. La figura 1.6 muestra los encabezados añadidos para cada capa.

FIGURA 1.6



La capa de enlace de datos provee un servicio a la capa de red. Esto encapsula la información de la capa de red en un Frame. El encabezado del Frame contiene la información requerida para completar las funciones requeridas de la capa de enlace de datos. Por ejemplo, el encabezado de capa de red contiene direcciones físicas.

[7] Protocol Data Unit. Unidad de dato pasada de una capa a otra . Cada capa encapsula el PDU de la capa de arriba en la información la cual es añadida

La capa física también provee un servicio a la capa de enlace de datos. Este servicio incluye codificación del Frame de la capa de enlace de datos en un patrón de 0 y 1 para la transmisión en el medio (usualmente un cable).

Como las redes globales desempeñan servicios para los usuarios, el flujo y el empaquetado de la información cambia. Empezando en la capa de transporte, cinco pasos de encapsulación ocurren:

1. Construcción del dato.
2. Empaquetado del dato para el transporte.
3. Añadir la dirección de red al encabezado.
4. Añadir la dirección local al encabezado de enlace de datos.
5. Conversión del dato en bits para transmisión.

Examinemos cada uno de los pasos anteriores para observar cómo el dato es afectado y preparado para su transmisión.

PASO 1 CONSTRUCCIÓN DEL DATO.

Un usuario realiza una solicitud para abrir una página específica enviando un URL (Uniform Resource Locator) al Web. La solicitud incluyendo el URL es convertido a un dato que puede atravesar la red.

PASO 2 EMPAQUETADO DEL DATO PARA EL TRANSPORTE.

El dato es empaquetado para el subsistema de transporte. Un encabezado de la capa de transporte es añadido al principio del dato. En el ejemplo de la solicitud al Web, el encabezado es un encabezado TCP e indica que el dato es direccionado a un servidor http.

PASO 3 AÑADIR DIRECCIÓN DE RED AL ENCABEZADO.

El dato es puesto en un paquete o datagrama, entonces la función de transporte puede direccionarlo sobre la red. El paquete incluye un encabezado con direcciones lógicas de fuente y destino (por ejemplo, direcciones IP). Estas direcciones lógicas ayudan a los dispositivos de red a enviar paquetes a través de la red a lo largo de una ruta elegida.

PASO 4 AÑADIR UNA DIRECCIÓN LOCAL EN LA CAPA DE ENLACE DE DATOS.

Cada dispositivo de red debe poner el paquete en un Frame, entonces el dispositivo puede comunicarse sobre una interfaz local a otra interfaz específica en la red. El Frame permite la conexión del dispositivo siguiente conectado a la red. El tipo de Frame debe correspoder con el tipo de enlace de dato. Por ejemplo, si el dato es enviado en una red Ethernet usando el tipo de Frame Ethernet II, el paquete de red es colocado dentro de un Frame Ethernet II.

PASO 5 CONVERTIR A BITS EL DATO PARA LA TRANSMISIÓN.

Ahora, el Frame es convertido a un patrón de 0 y 1 para la transmisión en el medio. Algunas funciones de reloj son habilitadas para que los dispositivos sepan distinguir entre esos 0 y 1 bits. El medio en la red global puede variar a lo largo de la ruta utilizada. Por

ejemplo, la solicitud HTTP se puede originar en una red LAN, atravieza el Backbone[8]. Sale para un enlace de WAN de alta velocidad hasta que es alcanzado por el destino en otra LAN remota.

1.4 CAPA DE APLICACIÓN

El término aplicación en este sentido no se refiere a las aplicaciones de computadora como procesadores de textos, bases de datos, hojas de cálculo, sino a las aplicaciones de red como:

- Transferencias de archivos
- Accesso Remoto
- Procesos Cliente/Servidor
- Administración de red

Las aplicaciones de computadoras no tienen el conocimiento de una red en capas, así que no pueden conectarse directamente en la red. Pero una aplicación de computadora tal como un procesador de textos puede ser incorporada a una aplicación de red como un componente de transferencia de archivos que permite que un documento sea transferido electrónicamente por una infraestructura de comunicaciones. Este componente califica al procesador de textos como una aplicación el contexto de OSI y pertenece a la capa 7.

Intercambios de información entre organizaciones compromete cada vez más a las aplicaciones de redes globales como se muestra en la figura 1.7

FIGURA 1.7

1.5 CAPA DE PRESENTACIÓN

La capa de Presentación provee de formatos de código y servicios de conexión. El formato de código garantiza tener información significativa a procesar. Si es necesario, la capa de Presentación traduce entre múltiples representaciones de formatos de datos para texto, audio, video y gráficos.

[8] Parte de una red que actúa como ruta primaria para el tráfico. Es la columna vertebral de la red.

1.5.1 FORMATOS DE TEXTOS Y CONVERSIÓN

La capa de presentación se ocupa no sólo del formato y de la representación de los datos reales, sino también de la estructura de datos usada por los programas. Por lo tanto, la capa de Presentación negocia la sintaxis de transferencia de datos para la capa de Aplicación. Por ejemplo, la capa de Presentación es la responsable de la conversión de sintaxis entre sistemas que tienen diferentes representaciones de texto y datos, tales como EBCDIC y ASCII. Otro ejemplo de representación es Hypertext Markup Languaje (HTML), el cual describe la forma en la que la multimedia es usada en la Web y debe aparecer cuando es visto por un Browser.

Las funciones de la capa de Presentación incluyen la encriptación de datos. Procesos y códigos convierten el dato, así que el dato puede ser transmitido con la información protegida de receptores no autorizados. Otras rutinas comprimen el texto o convierten imágenes gráficas en tramas de bits para la transmisión a través de la red.

1.5.2 FORMATOS DE GRAFICOS Y CONVERSIÓN

Los formatos gráficos incluyen PICT, un formato de película utilizado para transferir gráficos QuickDraw en Macintosh y PowerPC; Tagged Image File Format (TIFF) es un formato de gráficos estándar de alta resolución, imágenes de trazado de Bits (BMP) y JPG, un formato de gráficos estándar definido por Joint Photographic Experts Group.

1.5.3 FORMATOS DE AUDIO Y VIDEO Y CONVERSIÓN

Para el audio y video, la capa de Presentación incluye Musical Instrument Digital Interface (MIDI) para música digitalizada. La aceptación está creciendo para el estándar Motion Picture Experts Group (MPEG) para compresión y codificación de la señal de video para CDs, almacenamiento digital y rangos de bits arriba de 1.5Mbps. QuickTime maneja audio y video para programas Macintosh y PowerPC.

1.6 CAPA DE SESION

La capa de sesión establece, maneja y termina sesiones de comunicación entre aplicaciones. Esencialmente, la capa de sesión coordina solicitudes de servicios y respuestas que ocurren cuando las aplicaciones se comunican en diferentes hosts.

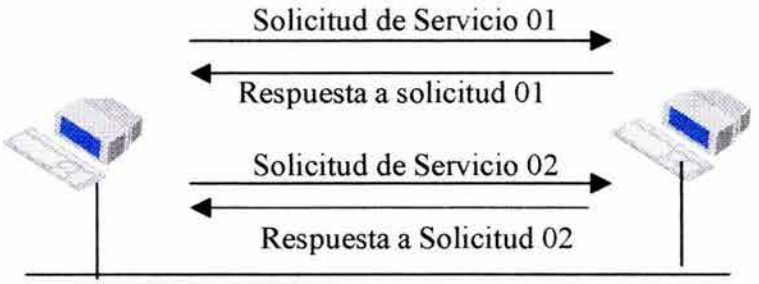
Por ejemplo, la capa de sesión puede establecer el intercambio para ser Full duplex o Half duplex[9], definir o agrupar los datos formateados y ofrecer la recuperación de la sesión o el mecanismo de punto de verificación entre aplicaciones coordinadas entre hosts.

---

[9] **Full Duplex:** Capacidad para transmisiones de datos entre una estación emisora y una estación receptora. **Half Duplex**: Capacidad para transmisiones de datos en una sola dirección en un tiempo entre una estación emisora y una estación receptora.

La figura 1.8 representa una comunicación entre diferentes hosts. La capa de sesión está establecida para ser Half Duplex (solicitud simple, contestación simple) e incluye un punto de verificación (número de sesión) para asegurar que las transacciones sean parejas entre peticiones y respuestas.

FIGURA 1.8



Los siguientes son ejemplos de protocolos e interfaces de capa de sesión:

- Structured Query Languaje: Lenguaje de Base de datos desarrollado por IBM para dar a los usuarios una manera más fácil de especificar sus necesidades en sistemas locales y remotos.
- Remote Procedure Call (RPC): Mecanismo de redirección para distribuir servicios. Los procedimientos RPC son construidos por clientes y ejecutado por servidores.
- Apple Talk Session Protocol: Establece y mantiene sesiones entre un cliente Apple Talk y un servidor.

1.7 CAPA DE TRANSPORTE

La capa de Transporte define conectividad punto a punto entre hosts de aplicaciones. Los servicios de transporte incluyen cuatro funciones básicas:

- Segmentar aplicaciones de capas superiores: Los servicios de transporte pueden segmentar varias aplicaciones de capas superiores en la misma trama de datos de la capa de transporte.
- Establece operaciones de punto a punto: Esta trama de dato provee transporte de servicios de extremo a extremo. Esto constituye una conexión lógica entre puntos finales de la red global: host emisor y host receptor.
- Envío de segmentos de un host terminal a otro host terminal: Como la capa de Transporte envía esos segmentos, puede también asegurar la integridad del dato por medio de un checksum[10] en el dato y proveer mecanismos de control de flujo. El control de flujo evita el problema de que un host en un lado de la conexión, desborde el buffer del host del otro lado. El desbordamiento puede causar pérdidas de datos.

[10] Un valor computado que es el resultado de una función matemática se aplicó al contenido de un paquete para asegurar que el paquete llegó correctamente a su destino.

- Asegurar la confiabilidad del dato: Los servicios de transporte permiten a los usuarios solicitar un transporte confiable del dato entre sistemas. El transporte asegura que la trama del dato enviada en una máquina puede ser enviada a otra sin duplicación o pérdida del dato. La confiabilidad puede también asegurar que el dato es recibido en el mismo orden en el cual fue enviado. Una sesión orientada a conexión entre sistemas es requerida para un transporte confiable. La sesión orientada a conexión será discutida más adelante.

Las siguientes secciones examinan las tecnologías de la capa de transporte disponibles para el control y optimización de comunicaciones.

1.7.1 MULTIPLEXACION

La multiplexación se refiere a la capacidad de múltiples aplicaciones para compartir una conexión. Diferentes aplicaciones puede enviar en la base "Primero enviado-Primero servido".

El software en la máquina debe fijar el número de puerto necesario para cada aplicación antes de la transmisión. Cuando se envía un mensaje, la computadora emisora incluye bits extras que codifique el tipo de mensaje originando el programa y el protocolo usados. Cada software de aplicación que envía un segmento de trama de dato, usa el mismo número de puerto previamente definido.

Cuando la computadora emisora recibe una trama de dato, ésta la separa en segmentos individuales y reensambla cada segmento de aplicación. Este proceso permite a la capa de Transporte pasar los datos hasta la aplicación destino.

TCP utiliza los números de puerto desde la capa de transporte hasta la capa de aplicación. Estos números de puerto han asignado rangos. Números de puerto 1 al 1023 son llamados números de puerto WELL-KNOW y son reservados para protocolos particulares. Por ejemplo, si la transferencia de archivos gráficos es FTP, el valor del puerto de aplicación usa ^1. La sesión de Telnet usa el puerto 23. La siguiente tabla muestra el número de puerto para algunos de los protocolos comúnmente usados.

NUMERO	PROTOCOLO
Puerto 20	File Transfer Protocol [Default Data]
Puerto 21	File Transfer Protocol [Control]
Puerto 23	Telnet
Puerto 25	Simple Mail Transfer Protocol
Puerto 53	Domani main Server
Puerto 67	Bootstrap/DHCP Protocol Server
Puerto 68	Bootstrap/DHCP Protocol Client
Puerto 69	Trivial File Transfer protocol

Puerto 70	Gopher
Puerto 80	World Wide Web http
Puerto 119	Network News Transfer Protocol
Puerto 123	Network Time Protocol
Puerto 161	SNMP
Puerto 162	SNMP TRAP
Puerto 179	Border Gateway Protocol

Otros conjuntos de protocolos como IPX/SPX tienen definiciones similares.

1.7.2 SERVICIOS DE RED ORIENTADOS A CONEXIÓN Y NO ORIENTADOS A CONEXCION

En general, los protocolos de red y los datos que soportan pueden ser orientados y no orientados a conexión.

Los datos orientados a conexión implican el uso de una ruta específica que es establecida por el tiempo que dura la transmisión. Los datos no orientados a conexión implican el paso de los datos a través de una conexión permanente.

Los servicios orientados a conexión involucran tres fases: establecimiento de conexión, transferencia de datos y terminación de la conexión. Durante la fase de establecimiento de conexión, una simple ruta entre los sistemas emisor y receptor es determinada. Los recursos de red son reservados para garantizar un buen grado de servicios.

En la fase de transferencia de datos, los datos son transmitidos secuencialmente sobre la ruta que se ha establecido. Los datos siempre llegan al destino en el orden en el cual fueron enviados.

Durante la fase de terminación, una conexión establecida que no es necesitada más, es terminada. En un futuro, si se quieren comunicar emisor y receptor, se requerirá de una nueva conexión establecida.

Los servicios de red orientados a conexión tienen dos desventajas sobre los servicios no orientados a conexión; selección de una ruta estática y reservación estática de recursos de red. La ruta estática puede crear dificultades porque todo el tráfico debe viajar sobre la misma ruta. Alguna falla en la ruta y la conexión se pierde. La reservación estática de recursos de red causa dificultades porque requiere una tasa garantizada de Througput[11]. Los servicios no orientados a conexión, sin embargo, son útiles para la transmisión de datos desde aplicaciones que no soportan retardos.

Los servicios no orientados a conexión no determinan la ruta del emisor al receptor, ni la secuencia del paquete. Cada paquete debe ser completamente direccionado porque

[11] Cantidad de datos que son transferidos correctamente entre nodos por unidad de tiempo, usualmente en segundos.

diferentes rutas a través de la red pueden ser seleccionadas para diferentes paquetes. Cada paquete es transmitido independientemente por el sistema fuente y es manipulado por dispositivos de red.

Los servicios no orientados a conexión ofrecen dos ventajas importantes sobre los servicios orientados a conexión: selección de ruta dinámica y asignación dinámica de ancho de banda.

La selección de ruta dinámica habilita el tráfico alrededor de fallas de red porque las rutas son seleccionadas en paquete por paquete. Con la asignación dinámica de ancho banda es más eficiente porque los recursos de red no son asignados a un ancho de banda que ellos no utilizarán.

Los servicios orientados a conexión son útiles para transmisiones de datos que pueden tolerar retardos y transmisiones.

1.7.3 CONTROL DE CONGESTION

Una vez que la transferencia de datos está en proceso, la congestión puede presentarse por diferentes razones. Primero, una computadora de alta velocidad puede generar tráfico más rápido que una red puede transferir. Segundo, si algunas computadoras necesitan enviar datagramas simultáneamente a través de un gateway, ese gateway puede experimentar congestión aunque ninguna fuente cause problemas.

Cuando los datagramas llegan muy rápido para el proceso de un host, éste almacena en memoria temporalmente. Si el tráfico continúa, el host eventualmente agota su memoria y debe descartar los datagramas que lleguen y se genera un "cuello de botella".

1.7.4 WINDOWING

En la forma más básica de transferencia de datos orientados a conexión, los segmentos de datos deben ser entregados al recipiente en la misma secuencia en que fueron transmitidos.

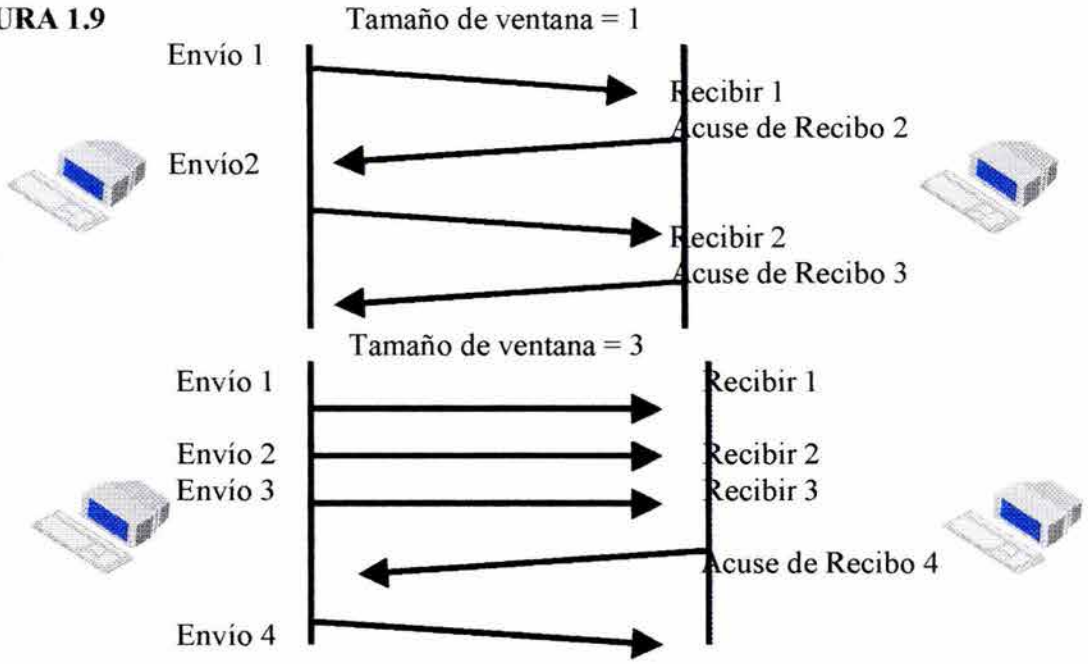
El protocolo en cuestión falla si algunos segmentos de datos son perdidos, dañados, duplicados y recibidos en diferente orden.

Si el emisor tiene que esperar un acuse de recibo (un reconocimiento) después de enviar cada segmento, la tasa de transferencia bajará. El número de segmento de dato que el emisor tiene permitido, sin recibir acuse de recibo todavía, se conoce como "Windowing".

Windowing es un método de control de información transferida. TCP/IP usa el campo Windowing en el encabezado TCP para indicar que hay espacio disponible en el buffer para datos. Cuando el tamaño de la ventana es igual a 0, el emisor debe parar el envió hasta que reciba un paquete con tamaño de ventana de no 0.

La figura 1.9 consta de un tamaño de ventana de 1 con un tamaño de ventana 3. Con un tamaño de ventana de 1, el emisor espera por un acuse de recibo para cada segmento de red transmitido. Con un tamaño de ventana 3, el emisor puede transmitir tres segmentos de datos antes de esperar un acuse de recibo.

FIGURA 1.9



Windowing es una facilidad en que emisor y receptor son estaciones de trabajo en una red pequeña. Los ruteadores no intervienen en la función de Windowing.

1.7.5 ACUSE DE RECIBO POSITIVO

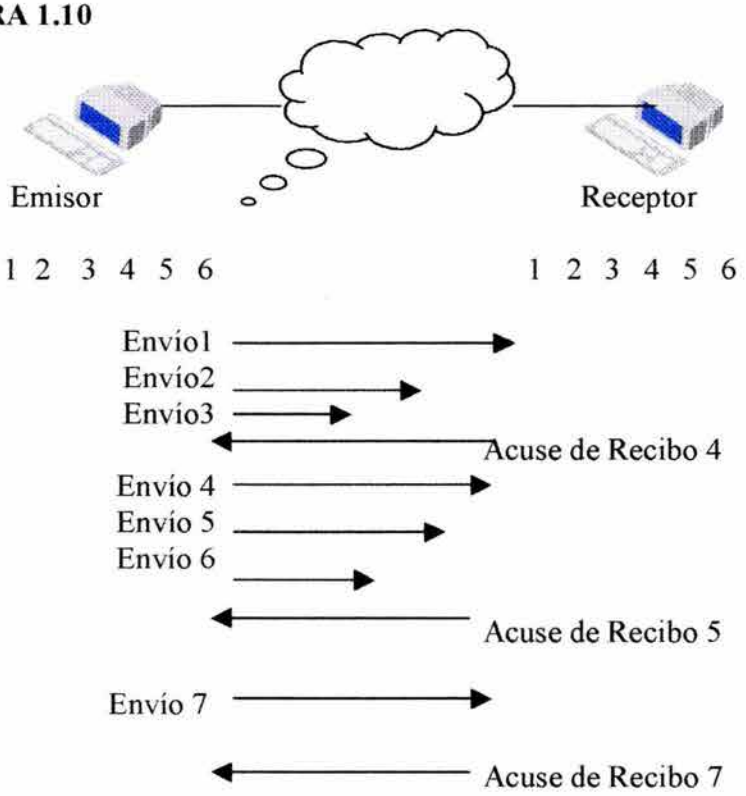
El acuse de recibo positivo con retransmisión es una técnica que garantiza la confiabilidad en la entrega de trama de datos. El acuse de recibo positivo requiere un recipiente para comunicarse con el emisor enviando de regreso un Acuse de Recibo cuando se recibe el dato. El emisor mantiene un record de cada segmento que envía y espera un acuse de recibo antes de enviar el próximo segmento.

Este sistema de espera de un acuse de recibo antes de enviar más datos es llamado sistema de acuse de recibo excepcional y es usado por TCP y SPX.

El emisor también tiene un reloj que es activado cuando se envía un segmento y retransmite un segmento si el tiempo expira antes de recibir el acuse de recibo.

En la figura 1.10, el emisor transmite los segmentos 1, 2, 3. El emisor, recibiendo el acuse de recibo envía los segmentos 4, 5 y 6. Si el segmento número 5 no llega a su destino, el destino envía un acuse de recibo al emisor con una solicitud de reenvió del segmento 5. El emisor reenvía y debe recibir un acuse de recibo para continuar con la transmisión del segmento número 7.

FIGURA 1.10



Varios protocolos manejan transmisiones en diferentes caminos. Algunos protocolos piden el reenvío sólo del segmento perdido. Otros piden retransmisión del conjunto entero de segmentos. Un protocolo que sólo pide la retransmisión del segmento perdido es más eficiente.

1.8 FUNCIONES DE CAPA FÍSICA Y ENLACE DE DATOS

La capa de enlace de datos provee de transporte de datos por un enlace fisico. Entonces, la capa de enlace de datos maneja las siguientes operaciones:

- Direccionamiento fisico
- Topología de red
- Notificación de errores
- Acceso ordenado al medio fisico
- Control de flujo

La capa física especifica los requerimientos eléctricos, mecánicos y funcionales para la activación, mantenimiento y desactivación del enlace físico entre sistemas.

La capa física especifica características como:

- Niveles de voltaje
- Rango de datos
- Distancias máximas de transmisión
- Conectores físicos

Estos requerimientos y características son codificados en estándares. Por ejemplo, EIA/TIA-232, que estandariza una conexión física para accesos de voz.

1.9 ESTANDARES DE LAN Y ORGANIZACIONES

Hoy, el trabajo de muchos estándares LAN es definido por el Institute of Electrical and Electronic Engineers (IEEE). El IEEE fue desarrollado en febrero de 1980 ('80, 2do. Mes, de ahí el nombre del comité IEEE) Para estandarizar las tecnologías LAN. El comité tiene los siguientes subcomités:

- 802.1 cubre puntos concernientes a todas las LAN como Spaning- Tree.
- 802.2 es responsable de la subcapa Logical Link Control (LLC).

- 802.3 es responsable de LAN basados en la metodología de acceso Carrier Sense Múltiple Access/ Collision Detect (CSMA/ CD). Ethernet es un ejemplo de red CSMA/ CD.

- 802.4 concerniente a las redes Token Ring. Token bus fue desarrollado por General Motors para la manufactura controlada por computadora y no se usa en estos días.

- 802.5 es responsable de las redes Token Ring. Token Ring de IBM y los estándares IEEE 802.5 son funcionalmente equivalentes.

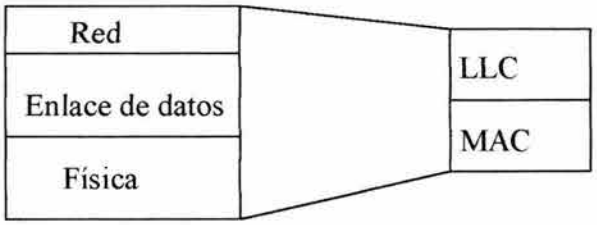
Otro tipo de tecnología LAN comúnmente utilizada es Fiber Distribute Data Interface (FDDI). El estándar FDDI es el responsable de American National Standars Institute (ANSI).

TIA (Telecomunications Industry Associates) es la organización responsable de los estándares de equipamiento de telecomunicaciones que conecta las redes de telecomunicaciones. TIA esta cercamente alineado con Electronic Industries Association (EIA) fundado en 1994. La ITU (International Telecomunication Union), con sede en Génova, Suiza, es una organización internacional el cual el gobierno y el sector privado coordina redes globales de telecomunicación y servicios.

1.10 SUBCAPAS DE ENLACE DE DATOS

Los protocolos de LAN ocupan dos capas inferiores del modelo OSI: la capa física y la capa de enlace de datos. El comité IEEE 802 subdivide la capa de enlace de datos en dos subcapas: La capa Logical Link Control (LLC) y la subcapa media Access Control (MAC). La figura 1.11 ilustra las capas.

FIGURA 1.11



1.10.1 FUNCIONES DE LA SUBCAPA DE RED

La capa de LLC provee ambientes que necesitan servicios orientados a conexión y no orientados en la capa de enlace de datos. La capa de LLC, maneja la comunicación entre dispositivos sobre un simple enlace de red. Esto define el campo que múltiples protocolos superiores compartan el uso del enlace de datos.

Los protocolos de capas superiores (por ejemplo, IP en la capa 3) pueden operar autónomamente sin considerar el tipo específico de medio de LAN. Esta dependencia ocurre porque, a diferencia de la subcapa MAC, LLC no es limitado a un protocolo MAC específico. En lugar de eso, la subcapa LLC puede depender de las capas superiores para proveer acceso al medio.

La subcapa LLC usa un conjunto de campos: Destination Service Access Point (DASP) y Source Service Access Point (SASP) para definir un enlace a las capas superiores del modelo OSI.

Las opciones de la subcapa incluyen soporte para conexiones entre aplicaciones corriendo en una LAN, control de flujo a las capas superiores y control de secuencia de bits.

1.10.2 FUNCIONES DE LA SUBCAPA MAC

La subcapa MAC provee acceso al medio LAN de manera ordenada.

Para que múltiples estaciones compartan el mismo medio, ellos deben tener direcciones únicas. La función más importante de la subcapa MAC es definir un hardware único o una dirección de enlace de datos llamada Dirección MAC, para cada interfaz de LAN. En la

mayoría de las tarjetas de red, las direcciones MAC están almacenadas en la memoria ROM. Cuando la tarjeta se inicializa, la dirección MAC es copiada en la memoria RAM.

Antes de entrar a detalle con las direcciones MAC es importante el direccionamiento lógico y direccionamiento fisico.

1.10.3 DIRECCIONAMIENTO FISICO Y LOGICO

La localización de sistemas de computadoras en una red es un componente esencial. Hay varios esquemas direccionamiento usados para este propósito, dependiendo de la familia de protocolos que se está usando. En otras palabras, el direccionamiento Apple Talk es diferente del direccionamiento TCP/IP que a su vez difiere del direccionamiento de IPX.

Dos tipos de direccionamiento son importantes: direccionamiento de capa de enlace y direccionamiento de capa de red. Las direcciones de capa de enlace (también llamadas direcciones fisicas) son únicas para conexión de red.

Como la mayoría de los sistemas de los sistemas de computadora tienen una conexión fisica, ellos sólo tienen una simple dirección de capa de enlace. Ruteadores y otros dispositivos conectados a una red fisica múltiple pueden tener direcciones de capa de enlace de direcciones de capa de enlace múltiples, como su nombre lo dice, las direcciones de capa de enlace existen en la capa número de 2 del modelo OSI.

Las direcciones de capa de red (también llamadas direcciones virtuales o lógicas) existen en la capa 3 del modelo OSI. A diferencia de las direcciones de capa de enlace, la cual existe en una red plana, las direcciones de red son usualmente jerárquicas.

1.10.4 DIRECCIONES MAC

La dirección MAC es una dirección de 48 bits expresada en 12 dígitos hexadecimales. Los primeros 6 dígitos hexadecimales de una dirección MAC contienen una identificación del fabricante (un código del vendedor) también conocido como Organizational Unique Identifier (OUI). Para asegurar la unidad del vendedor, el IEEE es el que administra los OUI. Los últimos dígitos hexadecimales son administrados por cada vendedor y representan el número serial de interfaz.

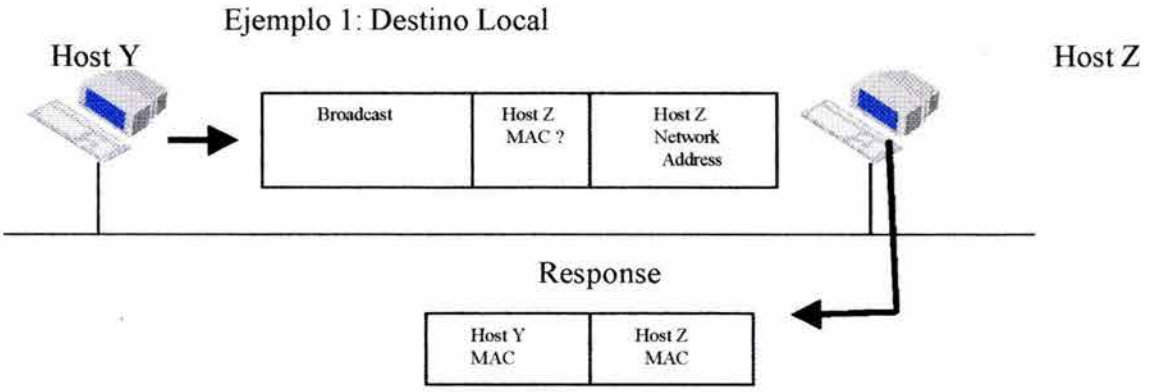
1.10.5 ENCONTRANDO UNA DIRECCION MAC

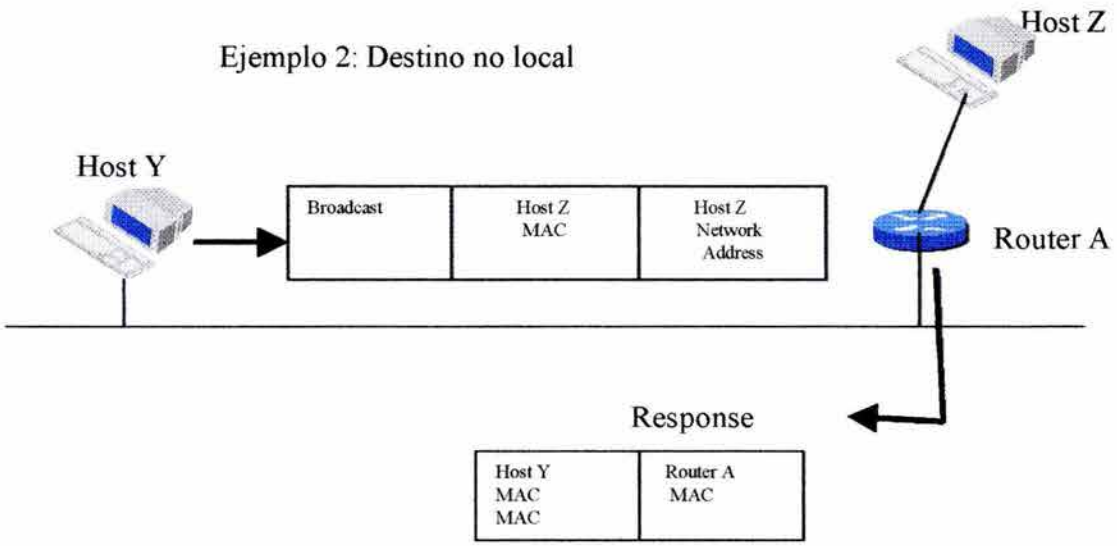
Antes que un frame sea intercambiado por un dispositivo conectado al dispositivo emisor, necesita resolver una dirección lógica a la capa de enlace o dirección MAC. La resolución de direcciones provee una búsqueda entre dos diferentes direcciones lógicas y de enlace de datos. Un protocolo de resolución de direcciones comúnmente usado es ARP en redes TCP/IP.

La figura 1.12 ilustra dos escenarios en los cuales un dispositivo descubre la dirección MAC del dispositivo destino enviando una solicitud de resolución de direcciones.

En el primer escenario, el host Y y el host Z están en la misma red LAN. El host Y envía un broadcast en la red indicando que el host Y está buscando una dirección de enlace de datos para el host Z. Como el host Y ha enviado un broadcast, todos los dispositivos, incluyendo el host Z procesarán la solicitud. Sin embargo, como la solicitud es solo para el host Z y solo el host Z debe responder con su propia dirección MAC. El host Y recibe la respuesta del host Z y guarda la dirección de enlace de datos del host Z en memoria. La próxima vez que el host Y necesite comunicarse con el host Z, se puede hacer una búsqueda a memoria y llamar a la dirección MAC del host Z.

FIGURA 1.12





En el segundo escenario, el host Y y el host Z están en diferente red pero puede accesarse uno con el otro a través del ruteador A. Cuando el broadcast del Host Y es solicitado, el ruteador A reconoce la dirección lógica como el perteneciente al host Z en una red diferente. Como el ruteador sabe que esto retrasa algunos paquetes para el host Z, el ruteador A provee su propia dirección MAC en respuesta a la solicitud. El Host Y recibe la respuesta y almacena la dirección MAC del ruteador en memoria: la próxima vez que el host Y quiera comunicarse con el host Z, el host Y buscará la dirección MAC del ruteador en memoria.

Hay actualmente tres métodos para encontrar las direcciones MAC:

- Un host pregunta por una dirección y recibe una respuesta del Address Resolution Protocol (ARP).
- Un host es notificado de otra dirección de otro host por paquete "hello".
- Las direcciones son asignadas en la ruta determinada como en DECnet.

1.11 TECNOLOGIAS LAN COMUNES

En esta sección se explican las funciones de la capa de enlace de datos, explorando las tecnologías LAN comunes:

- Ethernet
- Token Ring
- FDDI

1.11.1 ETHERNET Y IEEE 802.3

Ethernet actualmente corre en un gran número de redes LAN. Xerox desarrolló inicialmente y se unió Digital Equipment Corporation e Intel para definir Ethernet I en 1980, el mismo grupo relacionado con el Ethernet II en 1984. Ethernet describe un Carrier Sense Múltiple Access/ Collision Detect (CSMA/ CD) como método de acceso.
El IEEE 802.3 adopta Ethernet como modelo para CSM/CD. Como resultado, Ethernet II y IEEE 802.3 son idénticos en el medio físico.

Dos especificaciones difieren en sus descripciones de la capa de enlace de datos: IEEE 802.3 divide la capa de enlace de datos en dos entidades: la subcapa MAC y la subcapa LLC. La especificación Ethernet II no hace esta división u ofrece servicios LLC. Estas diferencias no prohíben a los fabricantes desarrollar tarjetas de red que soporten la capa física, direccionamiento MAC y software que reconozca las diferencias entre las capas las dos capas LLC.

1.11.1.1 CAPA FÍSICA ETHERNET/802.3

Ethernet y 802.3 define una topología de bus que opera en señalización de banda base en un rango de 10 a 100Mbps (Fast Ethernet) o 1000Mbps (Gigabit Ethernet). Hay varios estándares definidos:

- 10base2 (Thin Ethernet), permitidos en segmentos de red arriba de 185 metros en cable coaxial.
- 10base5 (Thick Ethernet), permitidos en segmentos de red arriba de 500 metros en cable coaxial.
- 10baseT, transporta frames Ethernet en cables de par trenzado (UTP).
- 100baseFX, es una implementación de Ethernet a 100Mbps en Fibra óptica.
- 100baseT4, es una implementación de Ethernet a 100Mbps usando 4 pares de cable UTP categoría 3, 4 y 5.
- 100baseTX, es una implementación de Ethernet sobre cable UTP categoría 5.

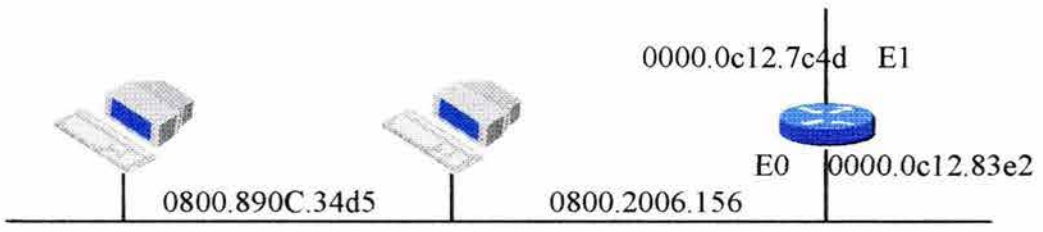
Los estándares 10base5 y 10base2 proveen acceso a varias estaciones en el mismo segmento. Las estaciones son conectadas al segmento por un cable que corre desde un Attachment Unit Interface (AUI) en la estación hasta un transceiver que es directamente conectado al cable coaxial Ethernet.

Como el estándar 10baseT provee acceso para una sola estación, las estaciones conectadas a una red LAN Ethernet, casi siempre se conectan a un concentrador.

1.11.1.2 INTERFAZ ETHERNET/ 802.3

Los enlaces de datos Ethernet/ 802.3 proveen transporte de datos a través de un enlace físico conectado a dos dispositivos, cada dispositivo en la red tiene uno o más interfaces al medio físico. Las interfaces físicas de dispositivos tales como estaciones de trabajo y servidores, son identificadas por sus direcciones MAC.
La figura 1.13 muestra tres dispositivos directamente conectados unos a otros por medio de una red LAN Ethernet.

FIGURA 1.13



Para indicar la interfaz 803.2 en los estatutos en la configuración de un ruteador Cisco, se usará el tipo de interfaz Cisco IOS con abreviación E seguido del número de la interfaz (por ejemplo, E0, como en la figura 1.13).

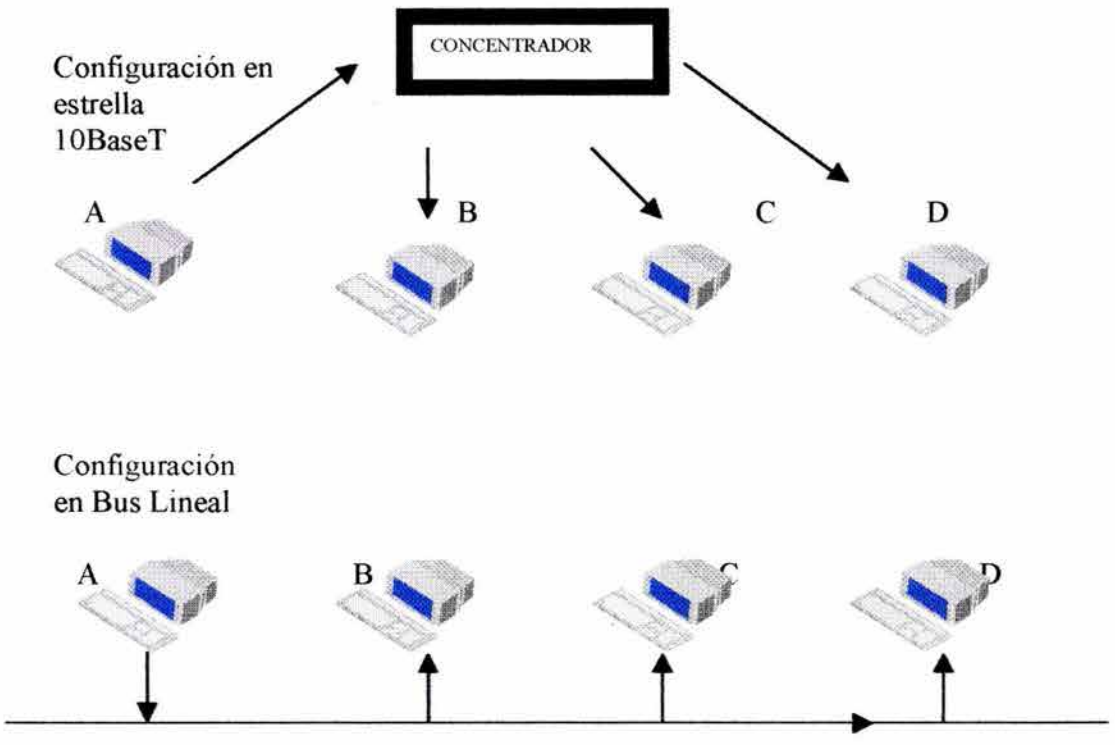
1.11.1.3 OPERACIÓN DE ETHERNET/ 802.3

En una red CSMA/CD, usando el diseño de una topología de bus lineal, la transmisión de un host atraviesa toda la red y es recibido y examinado por cada host. Cuando la señal alcanza el final del segmento, los terminadores absorben la señal para que no se regrese.

En una red 10baseT, la transmisión de un host es repetido a todos los hosts del concentrador.

En la figura 1.14 dos redes Ethernet/ 802.3 son: una red de bus lineal y una red de estrella. En cada caso la estación A transmite un paquete direccionado a la estación D. Este paquete es recibido por todas las estaciones. La estación D reconoce la dirección MAC y el proceso del frame, las estaciones B y C no reconocen esta dirección y descartan el frame.

FIGURA 1.14



1.11.1.4 BROADCAST Y MULTICAST ETHERNET/ 802.3

Las redes Ethernet/ 802.3 incluyen métodos para enviar paquetes a todos o a un solo grupo de dispositivos Ethernet usando técnicas de Broadcast y Multicast. Estas técnicas habilitan el dispositivo para transmitir un paquete que es procesado por algunas estaciones.

Broadcasting es una herramienta de gran alcance que envía un frame a todas las estaciones al mismo tiempo. El brodcasting utiliza direcciones de destino de enlace de datos de todas las estaciones (FFFF.FFFF.FFFF en hexadecimal).

Cuando el broadcasting tiene un uso incorrecto, puede afectar seriamente el desempeño de la red. Por esta razón, sólo el broadcast debe usarse cuando la dirección MAC del destino se desconoce o cuando el destino son todas las estaciones de la red.

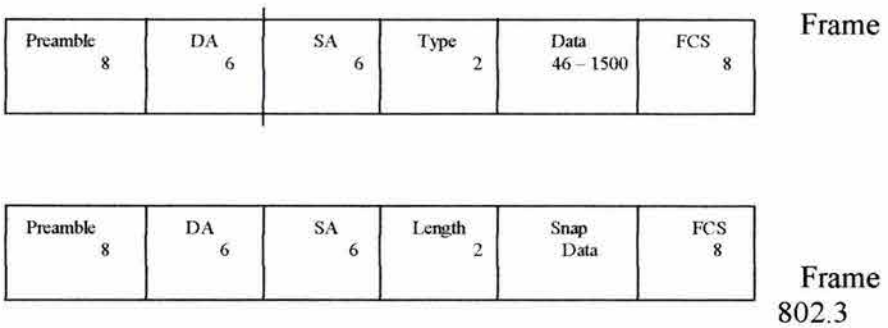
Una dirección multicast es una dirección MAC usada para identificar un número de destinos y es indicado por el primer bit transmitido de la dirección destino que fija en 1.

Para Ethernet, este bit aparece como bit de bajo orden (por ejemplo, xxxx.xxx1) en el primer bit de la dirección MAC del destino.

1.11.1.5 FORMATO DE FRAME ETHERNET/ IEEE 802.3

La figura 1.15 ilustra los campos de frames asociados con los frame Ethernet/ IEEE 802.3.

FIGURA 1.15



Preamble: El modelo de unos y ceros dice a las estaciones que la recepción del frame está ejecutándose.

Destination and Source Address (DAS Y SAS): Los primeros tres bytes de las direcciones son especificadas por IEEE en base al vendedor. Los últimos tres bytes son especificados por el vendedor Ethernet o 802.3. La dirección fuente (Source Address) es siempre una dirección unicast (un nodo destino) y la dirección destino (Destination Address) puede ser unicast, broadcast o multicast.

Type (Ethernet): El tipo especifica el protocolo de la capa superior para recibir el dato después de que el procesamiento Ethernet es completado.

Length (IEEE 802.3): La longitud indica en número de bytes de datos que siguen este campo.

Data (Ethernet): Después de que le proceso de capa física y de enlace de datos es terminada, el dato contenido en el frame es enviado al protocolo de la capa superior, el cual es identificado en el campo tipo.

Data (IEEE 802.3): Después de que le proceso de capa física y de enlace de datos es terminada, el dato contenido en el frame es enviado al protocolo de la capa superior, el cual debe ser definido en la porción del dato del frame. Si el dato en el frame es insuficiente para llenar el frame para un mínimo de 64 Bytes, el relleno de bytes es insertado para garantizar los últimos 64 Bytes del frame.

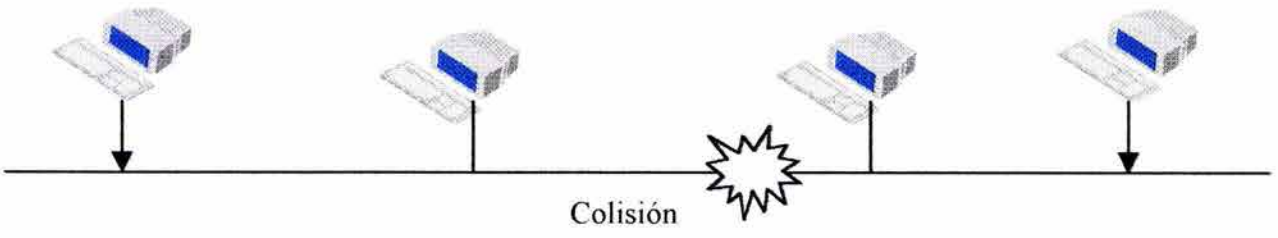
Frame Check Sequence (FCS): Esta secuencia contiene un valor de un Cyclic Redundancy Check (CRC)[12] de 4 byte, el cual es creacdo por el dispositivo de envío y es recalculdado por el dispositivo receptor para checar los frames dañados.

1.11.1.6 CONFIABILIDAD ETHERNET/ 802.3

Para enteder cómo CSMA/ CD provee un método de transmisión ordenada, se debe considerar lo que más ocurre cuando cada estación transmite. Cuando cada estación quiere transmitir, revisa la red para determinar si alguna otra estación está transmitiendo. Si la red no está siendo usada, la estación procede a la transmisión. Mientras está transmitiendo, la estación monitorea la red para garantizar que otra estación no transmita.

Dos estaciones pueden estar transmitiendo si determinan que la red está disponible. Si dos estaciones envían, al mismo tiempo, ocurre una colisión, como se ilustra en la figura 1.16

FIGURA 1.16



[12] Mecanismo de chequeo de errores.

Cuando un nodo reconoce una colisión envia una señal de atasco que causa la colisión y es reconocida por los demás nodos. Entonces todos los nodos que están transmitiendo detienen el envío de frames por un periodo de tiempo periodicamente seleccionado llamado *BackOffTime*, antes de retransmitir. Si intentos subsecuentes resultan en colisiónes, el nodo trata de retransmitir arriba de 16 veces antes de abandonar.

Si dos *BackOff Time* son suficientemente diferentes, una estación tendrá éxito la próxima vez que trate de transmitir.

1.11.1.7 OPCIONES ETHERNET DE ALTA VELOCIDAD

Nuevas aplicaciones pueden causar que usuarios experimenten retardos y otros problemas como insuficiente ancho de banda entre estaciones. En respuesta a esos problemas, las redes Ethernet han puesto disponibles tecnologías de 100Mbps tales como:

- 100BaseFX: Una implementación Ethernet a 100Mbps sobre Fibra Optica. La capa MAC es compatible con la capa MAC de 802.3.
- 100BaseT4: Una implementación de Ethernet usando 4 pares de categoría 3,4 o 5. de cable UTP.
- 100baseT: Una implementación de Ethernet a 100Mbps Sobre categoría 5 de cable UTP.
- 100VG AnyLAN: Una especificación para una implementación de Ethernet y Token Ring sobre 4 pares de cable UTP.

El aumento de ancho de banda Ethernet a 100Mbps soluciona una parte del problema. Las implementaciones 100BaseFX, 100BaseT4 y 100BaseTX son compatibles con la subcapa MAC, pero la especificación 100VG AnyLAN no es compatible con las otras tecnologías.

La otra parte de la solución es la reducción del conflicto de medio Ethernet. Un método para reducir el conflicto es construir en el medio Ethernet, el CSMA/CD. Usuarios del medio Ehternet tradicional, el medio LAN compartido, deben someterse a CSMA/CD de modo que dos usuarios no puedan comunicarse simultáneamente con el segmento de LAN compartido.

El switcheo también reduce el conflicto de medio creando múltiples segmentos para dispositivos de escritorio y aplicaciones grandes.

La segmentación del tráfico Ethernet puede llevar a un punto donde el switch dedica un segmento de LAN a un solo usuario. Dos estaciones trabajo usan su propio segmento Ethernet para recibir un ancho de banda dedicado de 10Mbps o 100Mbps para aplicaciones alto ancho de banda.

Una parte final para el ancho de banda insufiente es proveer al administrador de red de herramientas necesarias para diseñar, desarrollar y manejar una transición a este ambiente de redes switcheadas.

Otra tecnología de alta velocidad es Gigabit Ethernet (1000BaseX). Gigabit Ethernet incrementa 10 veces la velocidad de Fast Ehternet (100Mbps).

1.11.2 TOKEN RING/ IEEE 802.5

Token Ring fue desarrollado por IBM y Texas Instrument en 1970. Esta es aún la tecnología LAN primaria de IBM. La especificación IEEE 802.5 es casi idéntica al Token Ring de IBM.

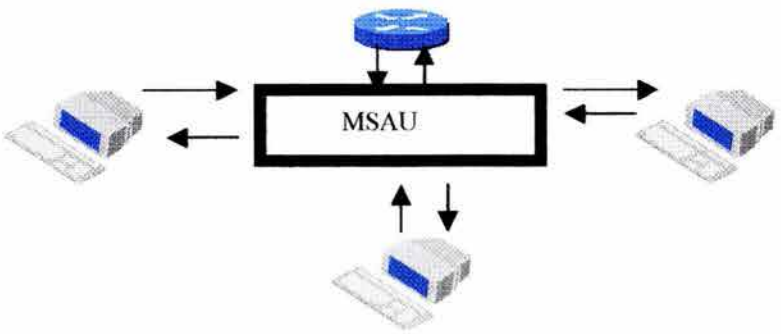
1.11.2.1 CAPA FISICA: TOKEN RING/ 802.5

La topología de red lógica de 802.5 es un anillo en el cual cada estación recibe señales desde su Nearest Active Upstream Neighbor (NAUN)[13] y repite esas señales a su vecino. Físicamente, sin embargo, las redes 802.5 es presentado como estrella con cada nodo conectado a un concentrador central en una una Unidad de Acceso Multiestación (MSAU)[14].

La configuración física y lógica es ilustrada en la figura 1.17. Físicamente, las estaciones conectadas al concetrador central con cable UTP.

Típicamente, un MSAU conecta arriba de 8 estaciones Token Ring. Para el aumento de desempeño y densidad de puerto, se pueden reemplazar los MSAUs compartidos y concentradores por switches Token Ring apilables.

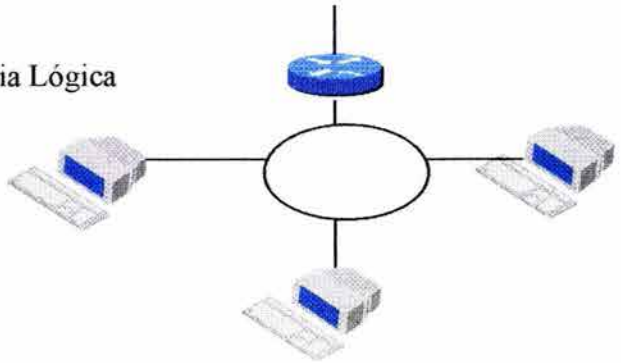
FIGURA 1.17



[13] En las redes Token Ring o IEEE 802.5, el dispositivo de la red más cercano de cualquier dispositivo que siga estando activo

[14] Es un concentrador en el cual todas las estaciones de una red Token Ring son conectadas. El MSAU provee de una interfaz entre esos dispositivos y la interfaz Token Ring del ruteador. Algunas veces se abrevia MAU.

Topologia Lógica



1.11.2.2 LA INTERFAZ TOKEN RING/ 802.5

IEEE 802.5 Token Ring está en paralelo con 802.3 para proveer de los servicios de la subcapa MAC y la capa fisica en un solo estándar.

Todas las estaciones Token Ring utilizan direcciones MAC incluyendo el ruteador mostrado en la figura 1.17. Para la configuración de la interfaz 802.5 en el ruteador se utilizará el tipo de abreviación de la interfaz del Cisco IOS software (To) seguido por el número de la interfaz (To0). Las redes Token Ring operan a velocidades de acceso de 4 Mbps o 16Mbps.

1.11.2.3 OPERACIÓN DE TOKEN RING/ 802.5

El acceso de una estación a Token Ring es determinístico; una estación puede transmitir sólo cuando ésta reciba un Token[15]. Este método es conocido como *Token Passing*. Aunque hay excepciones que pueden ser negociadas, las estaciones tiene el permiso para transmitir sólo un frame simple cuando ellos poseen un Token.

Si estación que recibe un Token no tiene información para transmitir, simplemente pasa el Token a la siguiente estación. Si la estación que tiene el Token tiene información para transmitir, añade la información que quiere transmitir y envia la información del frame a la otra estación del Token Ring.

La información del frame circula por el anillo hasta que es alcanzado por la estación destino donde es copiado por la estación y marcado. La información del frame continúa por el anillo hasta que regresa a la estación que la originó y es removida.

---

[15] Frame que contiene control de información. La posesión de un Token permite a una estación transmitir datos en la red.

A menos que el Early Token Release (ETR) sea usado en Token Ring, sólo un frame puede circular en el Token Ring. Otras estaciones que deseen transmitir deben esperar hasta que el frame en circulación sea removido y un Token vuelva a ser liberado.

Early Token Release (ETR) es una característica opcional que permite insertar el Token en el Token Ring inmediatamente después de la transmisión de un frame de información.

Como los frames viajan en serie por el anillo y como una estación recoge el Token antes de transmitir, no hay colisiones en una red Token Ring.

Token Ring soporta broadcasting y multicasting para mejorar la eficiencia de una o varias transmisiones. El broadcasting puede ser usado para localizar la ruta a algún destino. El multicasting es usado para enviar paquetes a direcciones de administración especiales de Token Ring para propósitos de integridad del anillo y reporte de errores.

1.11.2.4 CONTROL DE MEDIO TOKEN RING

Las redes Token ring utilizan sistema de prioridad que permite a cierto usuario señalado y a estaciones de alta prioridad, utilizar la red más frecuentemente que otras estaciones. Los frames de Token Ring tienen dos campos en el campo de control de acceso que controla la prioridad: el campo de prioridad y el campo de reservación,

La figura 1.18 ilustra los bits en el campo de control de acceso es usado para definir la prioridad actual y la proridad de reservación.

FIGURA 1.18

CAMPO DE CONTROL DE ACCESO

P	P	P	T	M	R	R	R

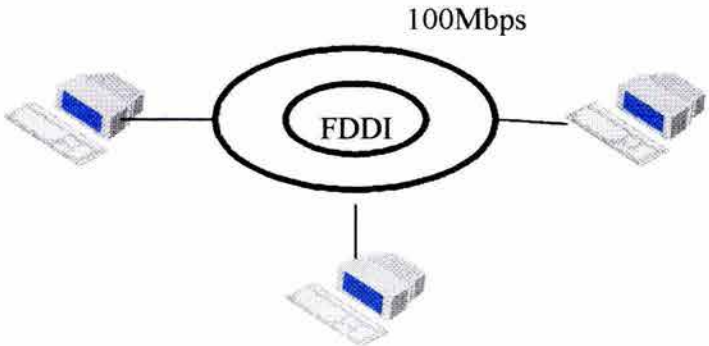
P Bits de prioridad
T Bit de Token
M Bit de monitoreo
R Bits de reservación

Sólo estaciones con una prioridad igual o una prioridad más alta que la de Token Ring pueden recoger el Token. Después que el Token es recogido y cambiado a un frame de información, sólo la estación con prioridad más alta que la estación de transmisión puede reservar el Token para el siguiente paso alrededor de la red.

1.11.3 FIBER DISTRIBUTE DATA INTERFACE (FDDI)

FDDI es un estándar de American National Standars Intitute (ANSI) que define un Token Ring Dual operando a 100Mbps sobre fibra óptica, como muestra la figura 1.19. Los estándares FDDI fueron publicados en 1987. Actualmente, FDDI es una tecnología LAN popular.

FIGURA 1.19



ANSI también ha definido el estándar Twisted-Pair Physical Medium Dependent. Basado en este estándar, Copper Distribute Data Interface (CDDI) provee operaciones de FDDI, pero es utilizado en cableado de cobre.

1.11.3.1 CAPA FISICA: FDDI

El estándar FDDI describe la capa física y la subcapa MAC. La capa física es dividida en dos subcapas: subcapa de protocolo de capa física (PHY) y subcapa physical medium dependent (PMD).

El PHY se ocupa de la codificación de los datos y símbolos. PHY especifica un método de codificación llamado 4B/5B. Este método traduce los octetos de las capas superiores en pares de símbolos de 5 bits que realizan funciones duales de paso de datos y mantiene un reloj de sincronización entre nodos.

Como FDDI especifica comunicación sobre fibra óptica, tiene operaciones donde los nodos son separados por largas distancias o donde las redes deben operar en ambientes electrónicamente hostiles como los pisos de una fábrica.

FDDI especifica los siguientes límites:

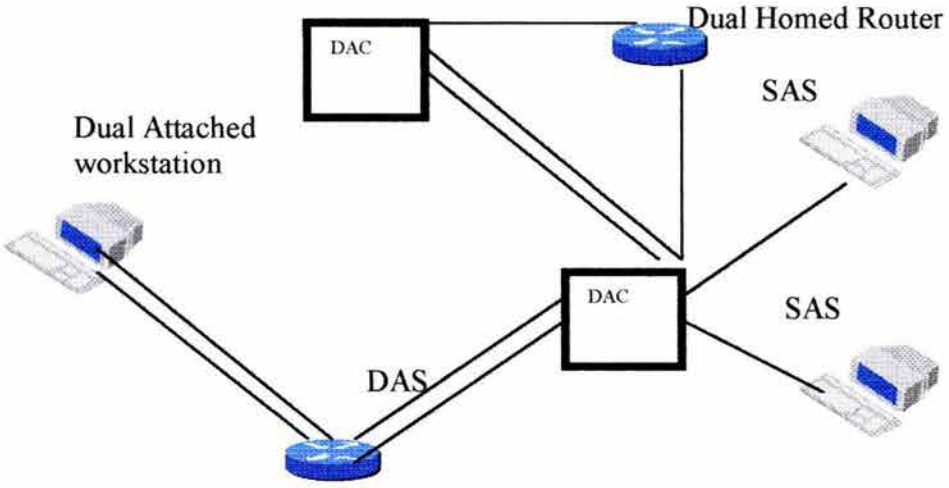
- 500 nodos por LAN FDDI
- 100Km de circinferencia de anillo

- 2Km entre nodos FDDI usando fibra Multimodo[16].

FDDI puede soportar altas velocidades, lo que es apropiado para aplicaciones de red que requieren de gran ancho de banda, por ejemplo, aplicaciones de video y gráficos.

FDDI utiliza un protocolo Token Passing que opera en anillos duales contrarrotacionales. Bajo operación normal, los datos fluyen en el primer anillo, mientras el segundo anillo no está en funcionamiento. Algunas estaciones conocidas como Dual Attachments Stations (DAS) conectan ambos anillos. Single Attechments Stations (SAS) tiene solo un PMD al anillo primario por un Dual Attachments Concentrator (DAC).

FIGURA 1.20



Las estaciones de misión crítica, tales como ruteadores o mainframes pueden utilizar una técnica llamada Dual Homing para proveer tolerancia de fallas y ayuda o asegura la operación.

1.11.3.2 LA INTERFAZ FDDI

FDDI es lógica y fisicamente una topología de anillo. Aunque opera a altas valocidades, FDDI es similar a Token Ring.

Todas las estaciones FDDI usan direcciones MAC incluyendo el ruteador mostrado en la figura 1.20.

---

[16] Una forma de cable de fibra óptica en el cual el rayo de luz puede seguir multiples caminos en el cable.

Para configurar la interfaz FDDI en un ruteador se usa el tipo de abreviación del Cisco IOS software F seguido del número de la interfaz (F0).

1.11.3.3 CONFIABILIDAD DE FDDI

El acceso a FDDI es determinado por la posesión del Token. Sin embargo, las estaciones unen nuevos Tokens al final de sus transmisiones. Así, varios Frames pueden circular por el anillo.

Todas las estaciones monitorean el anillo para condiciones inválidas, tales como Tokens perdidos o una ruptura en el anillo. Si una estación determina que un Token no ha sido recibido desde el NAUN durante un periodo de tiempo predeterminado, la estación empieza a transmitir frames para identificar la falla. Si la estación recibe su propio frame, éste asume que el anillo ha sido reparado.

1.12 TECNOLOGIAS COMUNES WAN

Los protocolos de WAN de capa fisica describen cómo proveer conexiones eléctricas, mecánicas, operacionales y funcionales para servicios de red de área amplia. Estos servicios son obtenidos de los proveedores de servicios WAN como agencias telefónicas y Carriers.

Los protocolos WAN describen cómo los frames son transportados entre sistemas por medio de un enlace. Ellos incluyen protocolos diseñados para operar sobre diferentes tipos de facilidades como:

- Facilidades de punto a punto dedicado: por ejemplo, una oficina conectada a otra a través de una conexión WAN. Un punto conectado a otro punto.
- Facilidades Multipunto: por ejemplo, una oficina corporativa conectada a tres sucursales.
- Servicios multiacceso switcheados: por ejemplo, un corporativo y tres sucursales conectados a la red WAN, como Frame Relay. Sus conexiones son switcheados a través de la nube WAN, no necesariamente toman la misma ruta.

Los estándares WAN son definidos y administrados por un número de autoridades reconocidas, incluyendo las siguientes agencias:

- International Telecommunication Union-Telecommunication Strandarization Sector (ITU-T).
- International Organization for Standarization (ISO).
- Internet Engineering Task Force (IETF)
- Electronic Industries Association (EIA).

Los estándares WAN decriben los requerimientos de la capa de enlace y fisica.

1.12.1 CAPA FISICA: WAN

La capa física de la red WAN describe la interfaz entre el Data Terminal Equipment (DTE)[17] y el Data Circuit-terminating Equipment (DCE)[18].

Típicamente el DCE es el proveedor de servicios y el DTE es el dispositivo de conexión. En este modelo, los servicios ofrecidos al DTE se hacen disponibles por un modem o un Channel Service Unit/ Data Service Unit (CSU/ DSU).

Varios estándares de capa física especifican esta interfaz:

- EIA/ TIA-232
- EIA/ TIA-499
- V.24
- V.35
- X.21
- G.703
- EIA-530
- High Speed Serial Interface (HSSI)

Es importante saber que el EIA/ TIA-232 y el EIA/ TIA-499 eran conocidos como RS-232 y RS-499 antes de su aceptación como estándares como EAI y TIA.

1.12.2 CAPA DE ENLACE DE DATOS: PROTOCOLOS WAN

Synchronous Data Link Control (SDLC): SDLC es un bit orientado a protocolo desarrollado por IBM . SDLC define un ambiente de WAN multipunto que permite que varias estaciones se conecten a una estación. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación es siempre entre la estación primaria y una de las estaciones secundarias. Las estaciones secundarias pueden no estar comunicadas unas con otras directamente.

High Level Data Link Control (HDLC): HDLC no es compatible entre diferentes vendedores porque cada vendedor tiene su manera de implementarla. HDLC soporta configuraciones punto a punto y multipunto.

Link Access Procedure, Balanced (LAPB): LAPB fue primeramente usada en X.25 pero también es usado como transporte de datos. LAPB incluye capacidades para detectar frame perdidos.

---

[17] Interfaz usuario-red que sirve como fuente de datos, destino o ambas.

[18] Provee una conexión física a la red, como un módem.

Frame Relay: Frame Relay usa técnicas de calidad digital en la cual el chequeo de errores del LAPB no es necesario. Usando un frame sin mecanismos de errores, Frame Relay puede enviar de información de capa 2 muy rápido comparado con otros protocolos de WAN.

Point to Point Protocol (PPP): PPP, descrito por RFC 1661, fue desarrollado por el IETF. PPP contiene un campo protocolo para identificar el protocolo de capa de red.

Integrated Services Digital Network (ISDN): ISDN es un conjunto de servicios digitales que transmiten voz y datos sobre líneas telefónicas.

CAPITULO 2

CAPA DE RED Y DETERMINACION DE RUTAS

En este capítulo se discute la capa de red del modelo OSI. Aquí se verá la información básica de cómo trabaja el direccionamiento de la capa de red en diferentes protocolos. También se explica la diferencia entre protocolos ruteados y protocolos de ruteo y el contraste de rutas dinámicas y rutas estáticas.

2.1 FUNDAMENTOS DE CAPA DE RED

Las interfaces de la capa de red proveen el mejor esfuerzo de entrega de servicios al usuario, la capa de transporte. La capa de red envía paquetes desde la red fuente a la red destino.

Primero, este capítulo examina el desempeño general de la capa de red, incluyendo cómo se determina y comunica una ruta a un destino, cómo los protocolos de esquemas de direccionamiento trabajan y cómo trabajan los protocolos de ruteo.

2.1.1 DETERMINACION DE UNA RUTA

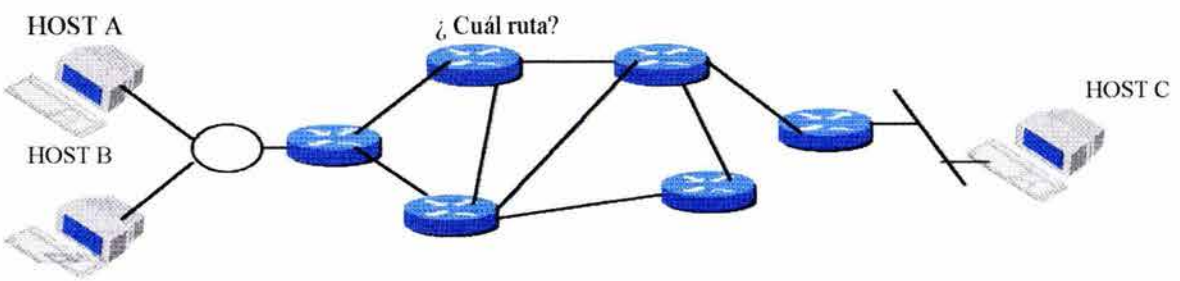
¿Qué ruta debe tomar el tráfico a través de una nube de redes? La determinación de una ruta ocurre en la capa 3, la capa de red. La función de la detereminación de la ruta habilita un ruteador para evaluar las rutas disponibles al destino y establecer la ruta preferida para un paquete.

Los protocolos de ruteo usan la información de la topología de red cuando evalúan las rutas de red. Esta información puede ser configurada por el administrador de red o recogida a través de procesos que se ejecutan en la red.

Después de que el ruteador determina la ruta a usar, puede proceder con el switcheo de paquetes: toma un paquete para colocarlo en una interfaz y envía el paquete a otra interfaz o a otro puerto que refleja mejor ruta del paquete al destino.

Por ejemplo, la figura 2.1 representa una red de malla. Hay varias posibles rutas entre el host A y el host C. El proceso de determinación de una ruta es usado para encontrar la mejor ruta posible.

FIGURA 2.1



Para habilitar la determinación de la ruta, los servicios de ruteo proveen:

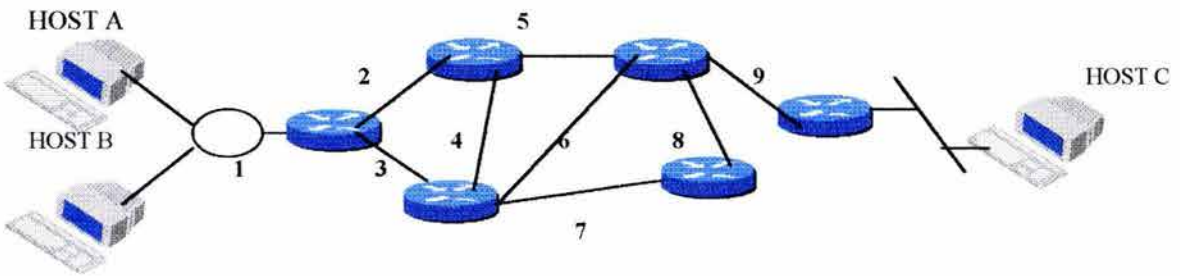
- Inicialización y mantenimiento de la tabla de ruteo.
- Proceso de actualización de la tabla de ruteo y protocolos.
- Dominios de ruteo y especificiones de dirección.
- Asignación de métricas de ruteo[19] y control.

2.1.2 INFORMACION DE LA COMUNICACION DE UNA RUTA

Los rutadores intercambian información acerca de las rutas disponibles a través de la red. Para identificar una ruta, un nombre debe ser asignado a cada una de las redes a lo largo de la ruta. Las direcciones de red son usadas para identificar cada enlace de red. La información de la ruta contiene los nombres de todas las redes que deben cruzar a lo largo de la ruta.

En la figura 2.2, cada línea entre ruteadores tienen un número que los ruteadores usan como dirección de red: esas direcciones transportan información acerca del camino de ruteo para pasar paquetes de una fuente a un destino.

FIGURA 2.2



Los ruteadores utilizan la información de la ruta con sus mecanismos de determinación, sus mecanismos de switcheo y funciones de procesamiento de ruteo para localizar la mejor ruta a través de una red.

La consistencia de las direcciones de capa 3 a través de toda la red, mejora el ancho de banda por la prevensión de los broadcast innecesarios.

IMPORTANTE:

Los rutadores contienen broadcast para permitir que la capa de red encuentre al destino.

[19] Método por el cual un algoritmo de ruteo determina que una ruta es mejor que otra. Se verá más adelante.

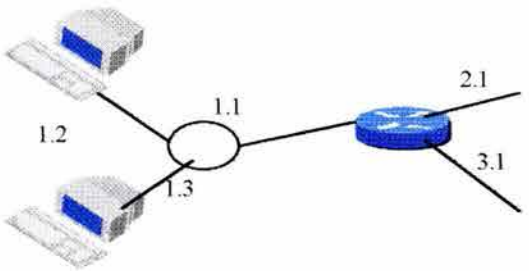
2.1.3 DIRECCIONAMIENTO: RED Y NODO

Las direcciones de red consisten en una porción de red y una porción de nodo. Ambos son necesarios para entregar paquetes de una fuente a un destino. En la figura 2.3, dos partes de números (1.2, 1.3 y 2.1) representan el conjunto de direcciones de red y nodo. El primer dígito es la porción de red y el segundo dígito es la porción de host.

El ruteador utiliza la porción de host para identificar la fuente o el destino del paquete en la red. La figura 2.3 muestra tres números de red (1, 2 y 3) conocidos por el ruteador.

FIGURA 2.3

RED	HOST
1	1 2 3
2	1
3	1



La porción de red de las direcciones se refiere a un puerto específico o dispositivo de la red. Por ejemplo, en la figura 2.3 tres nodos (1, 2 y 3) son mostrados compartiendo el número de red 1, la dirección de nodo en un paquete identifica que el paquete está en el puerto fuente o destino. Para una red LAN, este puerto puede reflejar la dirección MAC real del dispositivo.

Algunos sistemas de direccionamiento de red, como direccionamiento IP, requiere de una asignación manual de dirección de host única para cada dispositivo. Otros sistemas de direccionamiento como Novell IPX, toma la dirección MAC única como dirección de host.

IMPORTANTE:

Las porciones de red y de host de una dirección de red manejan diferentes niveles de localización. Una dirección es similar a Calle Terán. Las direcciones de host son similares al número del edificio como Calle Terán #239.

El proceso de ruteo en una red típicamente es interesado sólo en la porción de red de una dirección que es la información requerida para la entrega de datos a la red apropiada.

Después que el destino ha sido alcanzado, sin embargo, el ruteador final en la ruta debe usar la porción del host para enviar el paquete a la dirección apropiada del dispositivo del hardware al final de la red.

Los dispositivos de redes globales pueden tener más de una dirección de red. Diferentes direcciones deben ser asignadas para cada protocolo de la capa de red por un dispositivo en particular. Por ejemplo, un dispositivo asignado a redes AppleTalk y DECNet debe tener asignadas dos direcciones de red.

Para algunos protocolos de capa de red, un administrador de red asigna dirección de red de acuerdo con el plan de direccionamiento. Para otros protocolos, la asignación de direcciones, es dinámica.

No todos los protocolos de red utilizan la dirección del host en la manera como muestra la figura 2.3, por ejemplo:

- Novell IPX utiliza direcciones MAC como direcciones de host; para interfaces que no tienen direcciones MAC, Novell IPX puede aplicar una dirección MAC para la dirección del nodo.
- DECnet modifica las direcciones MAC para conetener una dirección de nodo.

2.1.4 VARIACIONES EN EL DIRECCIONAMIENTO DE PROTOCOLO

En TCP/IP están las direcciones IP. Números en decimal separados por puntos que muestran una parte de red y una parte de host. La red 10 (binario) usa el primero de 4 números como la parte de red y los tres conjuntos de números como una red de host.

En IPX de Novell se utiliza una variación de un direccionamiento en dos partes. La dirección de red 01ac.eb01b, por ejemplo, es un número hexadecimal que no puede exceder un número fijo de dígitos. La dirección de host 0000.0c00.6e25 (también un número hexadecimal) es un número fijo de 48 bits. La dirección de host deriva automáticamente desde el hardware de un dispositivo LAN específico.

2.1.5 DIRECCIONAMIENTO DE RED TCP/IP

Las redes TCP/IP representan direcciones como entidades de 32 bits divididos en una porción de red y una porción de host.

El Internet Request For Comments (RFC) 1117 divide la porción de red en clases. Todas las clases de direcciones de red viene de una autoridad central: InterNIC (Internetwork Information Center). Las clases más comunes son las siguientes:

- Clase A: Usando 8 bits para la red y los 24 bits restantes para la dirección de host.
- Clase B: Usando 16 bits para la red y 16 bits restante para la dirección de host.
- Clase C: Usando 24 bits de la red y 8 bits restante para la dirección de host.
- Clase D: Usando por las direcciones IP de multicast.

Las redes IP típicas se dividen en subredes. Cuando una dirección IP ha sido dividida para subredes, la parte de red de la dirección es descrita por dos elementos: el número de red, asignado por la NIC y el número de subred, asignado por el administrador de la red local.

Un ruteador puede manejar otros esquemas de direccionamiento. La siguiente tabla resume los principales detalles acerca de tres de los esquemas más comunes de direccionamiento.

PROTOCOLO	DIRECCION DE RED	DIRECCION DE HOST
Novell IPX	Arriba de 32 bits (hex); se refiere al medio (por ejemplo, Ethernet).	48 bits (hex), usualmente la dirección MAC .
AppleTalk	Arriba de 16 bits (dec), refiere una o una de muchas redes en rango del cable	Arriba de 8 bits añadidos al numero de red.

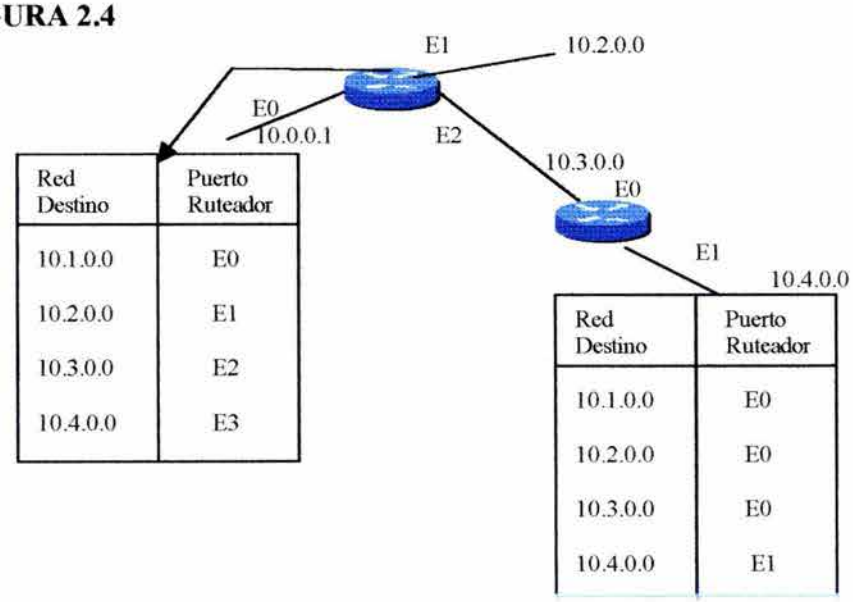
Los ruteadores de Cisco pueden manejar esos y algunos otros esquemas de direccionamiento de capa 3.

2.1.6 EL RUTEO UTILIZA DIRECCIONES DE RED

Los ruteadores transmiten paquetes de enlace de datos a otro. Para transmitir un paquete un ruteador utiliza dos funciones básicas: determinación de una ruta y switcheo.

La figura 2.4 muestra la manera en que los rutadores usan el direccionamiento para funciones de ruteo y switcheo. Cuando un paquete destinado para la red 10.1.0.0 llega al ruteador 1, el ruteador sabe que el paquete debe ser enviado por el puerto E0.

FIGURA 2.4



Aunque algunas veces la funcion de determinación de la ruta es capaz de calcular la ruta completa desde el ruteador al destino, un ruteador es sólo el responsable de pasar un paquete a la mejor red a lo largo de un camino. Por ejemplo, en la figura 2.4, si un paquete que es destinado para la red 10.4.0.0 llega al ruteador 1, el ruteador conoce que la mejor dirección para enviar el paquete fuera es la interfaz E2: el ruteador 2 es el próximo salto a lo largo del camino. El ruteador usa la porción de la red de la dirección para hacer esas selecciones de ruta.

La función de switcheo permite a un ruteador aceptar un paquete en una interfaz y enviarla a otra interfaz. La función de determinación de ruta habilita al ruteador para seleccionar la interfaz más apropiada para enviar el paquete.

IMPORTANTE:

Con respecto a la capa 3, el término *switcheo* es usado para describir el movimiento de paquetes de un puerto a otro. Es diferente del switcheo de capa 2 el cual se refiere en el envio de paquetes de un puerto a otro basados solo en la dirección MAC.

2.1.7 PROTOCOLOS RUTEADOS VS. PROTOCOLOS DE RUTEO

Existe confusión entre los protocolos de ruteados y los protocolos de ruteo.

2.1.7.1 PROTOCOLOS RUTEADOS

Un protocolo ruteado es un protocolo que contiene información de direccionamiento de capa de red suficiente para que el tráfico sea direccionado desde una red a otra. Los protocolos ruteados definen el formato y el uso de los campos de un paquete. Los paquetes que usan un protocolo ruteado son transportados de un sistema a otro a través de una red. IP e IPX son ejemplos de protocolos ruteados.

2.1.7.2 PROTOCOLOS DE RUTEO

Un protocolo de ruteo soporta un protocolo ruteado para proveer mecansimos para compartir información de ruteo. Los mensajes de protocolo de ruteo permiten a los ruteadores comunicarse con otros ruteadores y mantener actualizadas sus tablas de ruteo[20].

Los mensajes de protocolos de ruteo no llevan el tráfico de red en red. Un protocolo de ruteo usa un protocolo ruteado para pasar la información entre ruteadores. Unos ejemplos de protocolos de ruteo son: Routing Information Protocol (RIP), Interior Gateway Protocol (IGRP) y Open Shortest First Path (OSPF).

---

[20] Una tabla almecenada en los ruteadores que contiene información de las rutas y sus destinos.

Usualmente, los protocolos de ruteo funcionan sólo entre ruteadores; pero como algunos protocolos de ruteo son ignorantes de otros ruteadores, ellos transportan mensajes de broadcast para proveer información a otros ruteadores.

Algunas veces esos mensajes de broadcast son usados por sistemas finales para sus propósitos. Por ejemplo, un sistema final recibiendo un broadcast de actualización puede registar la existencia del ruteador y usar éste en el tiempo que requiera información acerca de la topología de la red.

Por ejemplo, un mecanismo de descubrimiento de direcciones AppleTalk (AARP), lleva su información a los sistemas finales acerca de sus ruteadores vecinos.

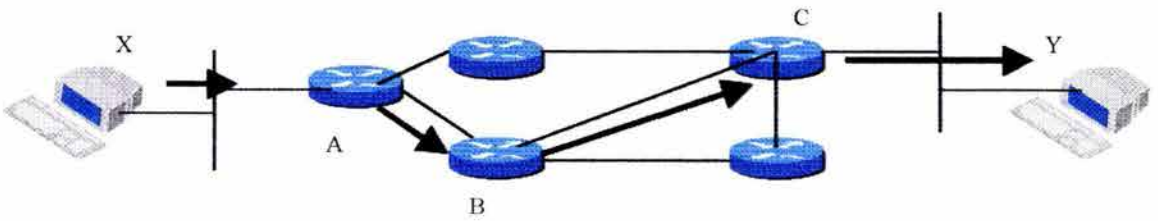
IMPORTANTE:

Las comunicaciones que utilizan protocolos ruteados, como IP, pueden ser transmitidos de una red a otra. Los protocolos de ruteo como IP RIP, son usados para tomar desiciones sobre la mejor ruta para el envío de paquetes.

2.1.8 OPERACIONES DE PROTOCOLOS DE CAPA DE RED

Cuando una aplicación envía un paquete a un destino en una red diferente, un frame de enlace de datos es recibido en una de las interfaces del ruteador. El ruteador quita el encabezado MAC y examina el frame del encabezado de la capa de red, tal como el encabezado IP, IPX, para tomar la decisión de envío. Como muestra la figura 2.5.

FIGURA 2.5



El dato de la capa de red es enviado al proceso de la capa de red apropiado y el frame de enlace de datos es descartado.

El proceso de la capa de red examina el encabezado para determinar la red destino y entonces hace referencia a la tabla de ruteo que asocia redes a interfaces de salida.

El paquete es encapsulado otra vez en el frame de enlace de datos para seleccionar la interfaz y hace cola para la entrega al próximo salto en la ruta.

Este proceso ocurre cada vez que el paquete se manda a otro ruteador. En el ruteador conectado a la red conteniendo el host destino, el paquete es otra vez encapsulado en el tipo de frame de enlace de datos de la red LAN destino.

2.1.9 RUTAS ESTÁTICAS VS RUTAS DINAMICAS

El concepto estático se conoce como administrado manualmente: un administrador de red entra en la configuración del ruteador. El administrador debe actualizar manualmente una ruta estática siempre que una topología de red cambia. El conocimento estático puede ser privado; por defecto, éste no es transportado a otros ruteadores como proceso de actualización; sin embargo, se puede configurar el ruteador para compartir este conocimiento.

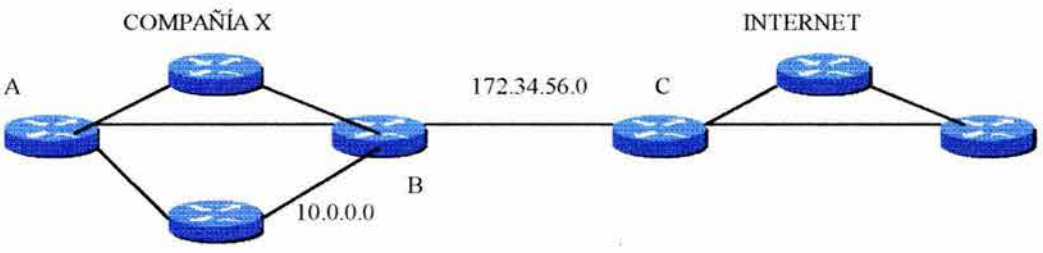
El concepto dinámico trabaja diferente. Después de que el administrador de red entra en los comandos de configuración para empezar el ruteo dinámico, la ruta es actualizada automáticamente por el proceso de ruteo siempre que la información de la nueva topología sea recibida desde la red.

2.1.10 RUTA POR DEFECTO

Una ruta por defecto es un camino por el cual un ruteador debe enviar el paquete si éste no tiene un conocimiento específico acerca del destino del paquete.

La figura 2.6 muestra el uso de una ruta por defecto –una entrada de la tabla de ruteo para direccionar frames para la cual el próximo salto no está explícito en la tabla de ruteo. Las rutas por defecto pueden ser fijas manualmente por el administrador de red (configuración estática) o pueden ser fijadas por una configuración dinámica con conocimiento de algunos protocolos.

FIGURA 2.6



En la figura 2.6 se muestra una compañía x con ruteadores que poseen un conocimiento específico de la topología de red, pero no de otras redes. Mantener el conocimiento de cada una de las otras redes accesibles por el camino de Internet, es innecesario, pero no

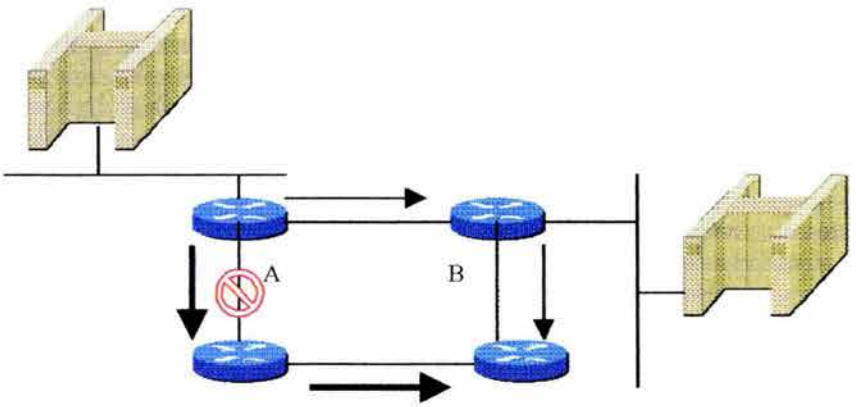
imposible. En lugar de mantener un conocimiento específico de la red, cada ruteador de la compañía x es informada por la ruta por defecto que puede alcanzar un destino desconocido direccionando el paquete a la red.

2.1.11 ADAPTANDOSE AL CAMBIO DE LA TOPOLOGIA

La red mostrada en la figura 2.7, se adapta diferentemente a los cambios de topología dependiendo si se usa una configuración estática o dinámica.

La configuración estática permite a los ruteadores transportar correctamente un paquete de una red a otra. En la figura 2.7, el ruteador A se refiere a su tabla de ruteo y sigue la configuración estática para transmitir al paquete al ruteador D. El ruteador D hace lo mismo y transmite el paquete al ruteador C. El ruteador C entrega el paquete al ruteador destino.

FIGURA 2.7



Pero ¿Qué sucede si la ruta entre el ruteador A y el ruteador D falla? Obviamente, el ruteador no es capaz de transmitir el paquete al ruteador D con una ruta estática, hasta que el ruteador A es manualmente reconfigurado para transmitir el paquete por el ruteador B, la comunicación con el destino es imposible

La configuración dinámica ofrece mayor flexibilidad. De acuerdo con la tabla de ruteo generada por el ruteador A, un paquete puede alcanzar su destino sobre la ruta preferida por el ruteador D. Sin embargo, una segunda ruta al destino es disponible por el camino del ruteador B. Cuando el ruteador A reconoce que el enlace al ruteador D está caído, ajusta su tabla de ruteo, haciendo la ruta por el ruteador B la más adecuada hacia el destino. Los ruteadores continúan enviando paquetes sobre este enlace.

Cuando el enlace entre el ruteador A y el ruteador D es restaurado, el ruteador A puede hacer otra vez el cambio a su tabla de ruteo para indicar una preferencia por la ruta del ruteador D y C al destino.

2.1.12 OPERACIONES RUTEO DINAMICO

El éxito del ruteo dinámico depende de dos funciones básicas de ruteador:

- Mantenimiento de la tabla de ruteo.
- Oportuna distribución de conocimiento en la forma de tablas de ruteo para otros ruteadores.

El ruteo dinámico confia en los protocolos de ruteo para expandir el conocmiento de las rutas. Un protocolo de ruteo define un conjunto de reglas usadas por un rutedor cuando éste se comunica con los demás ruteadores. Por ejemplo, un protocolo de ruteo describe:

- Cómo las actualizaciones son transportadas.
- Cómo localizar los recipientes de las actualizaciones.
- Qué conocimiento es transportado.
- Cuándo transportar el conocimiento.

2.1.13 REPRESENTANDO DISTANCIAS CON METRICAS

Cuando un algoritmo de ruteo actualiza la tabla de ruteo, el objetivo primario es determinar la mejor información incluida en la tabla. Cada algoritmo de ruteo interpreta el "mejor" a su propia manera. El algoritmo genera un número llamado Métrica para cada ruta en la red. Tipicamente, la métrica más pequeña es la mejor ruta.

Las métricas puden estar basadas en una característica simple de una ruta o por combinación de varias características. Las métricas comunmente utilizadas son las siguientes:

- Cuenta de saltos: Se refiere al número de rutadores que un paquete debe pasar hasta alcanzar su destino. La cuenta de saltos más baja es la mejor ruta. El largo de la ruta es usada para indicar la suma de saltos al destino.
- Ticks: Usado con Novell IPX RIP para reflejar retraso. Cada tick es 1/18 segundos.
- Costo: El costo de la ruta es la suma de los costos asociados con cada enlace al destino. Los costos son asignados (manual o automáticamente) al proceso de cruzar una red. Las redes lentas tienen un costo mayor a la redes más rapidas.
- Ancho de banda: Es la tasa máxima de throughput[21] en un enlace. El ruteo a través de enlaces con un amplio rango de ancho de banda no siempre provee la mejor ruta. Por ejemplo, si un enlace de alta velocidad está ocupado, el paquete se envía a través de un enlace más lento, y puede ser más rápido.
- Retraso: Depende de algunos factores, incluyendo el ancho de banda de los enlaces de red, la longitud de colas a cada ruteador en la ruta, la congestión de enlaces de

[21] Es la cantidad de información transferida exitosamente entre nodos por unidad de tiempo, usulmente segundos.

red y la distancia fisica a atravesar. Una conglomeración de variables que cambian las condiciones de la red, el retardo que es una métrica util y común.

- Carga: Factor dinámico que puede ser basado en una gran variedad de mediciones, incluyendo el uso de CPU y los paquetes procesados por segundo.
- Confiabilidad: Refleja la propensión del enlace de red a fallar y la velocidad con la cual fue reparada. Se pueden tomar múltiples factores al asignar grados de confiabilidad. Los grados de confiabilidad son usualemente asignados por el administrador de la red, pero puede ser calculado dinámicamente por el protocolo.
- MTU (Maximum Transmission Unit): La longitud máxima del menasaje en octetos que es aceptable a todos los enlaces de la ruta.

Aunque no está directamente conectado al ruteador, el gasto es otra métrica importante. Algunas organizaciones no tienen el cuidado en el desempeño en los gastos de operación. Por ejemplo, aunque el ancho de banda es menos y el retardo es más grande, el envío de paquetes sobre líneas dedicadas en lugar de líneas públicas más caras puden ser preferibles para algunas empresas.

2.2 PROTOCOLOS DE RUTEO

Los algoritmos de ruteo pueden ser clasificados en dos algoritmos básicos.

- Vector distancia
- Estado de enlce

El ruteo de vector distancia determina la dirección (vector) y distancia a algún enlace en la red.

El ruteo de estado de enlace (tambien llamado Shortest Path First) aprende la topología exacta de la red entera en la cual el ruteador está situado.

El tercer ruteo es un ruteo híbrido que combina aspectos de estado de enlace y vector distancia.

IMPORTANTE:

No hay ningún mejor algoritmo para toda la red. Los administradores de red deben conocer los aspectos técnicos y no técnicos de su red para determinar el mejor algoritmo. El software Cisco IOS puede configurar todas las opciones de ruteo convenientes.

El algoritmo de ruteo es fundamentalmente para el ruteo dinámico. Siempre que la topología de red cambia por crecimiento, por reconfiguración o por alguna falla, el conocimiento base del ruteador tambien debe cambiar.

El conocimiento de la topología de red necesita ser excacto y consistente de ruteador a ruteador. Esta exactitud y consistencia se llama "convergencia". Cuando todos los

ruteadores en una red están operando con el mismo conocimiento, se dice que la red ha convergido.

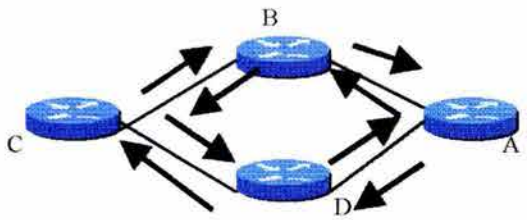
La rápida convergencia es una característica deseable de toda red porque esto reduce el período de tiempo que tienen los ruteadores para actualizar el anticuado conocimiento y evitar tomar decisiones que puden ser incorrectas.

2.2.1 RUTEO DE VECTOR DISTANCIA

Los algoritmos de ruteo basados en vector distancia (también conocidos como algoritmos Bellman-Ford) periódicamente pasan una copia de la tabla de ruteo de un ruteador a otros ruteadores. Las actualizaciones entre ruteadores también comunican cambios en la topología inmediatamente que ellos ocurren.

Cada ruteador recibe una tabla de ruteo desde otros ruteadores conectados a la misma red, como muestra la figura 2.8, el ruteador B recibe información desde el ruteador A, éste es el ruteador vecino a través de un enlace de WAN. El ruteador B agrega un número de vector distancia (tal como el número de saltos) incrementando el vector distancia y pasando la tabla de ruteo a otro vecino. Este proceso de paso a paso ocurre en todas las direcciones entre los ruteadores vecino.

FIGURA 2.8



En este camino el algortimo acumula distancias de red, entonces puede mantener una base de datos de la información de la red. Los algoritmos de vector distancia no permiten a los ruteadores conocer la topología exacta de la red.

Ejemplos de protocolos de vector distancias son IPX RIP e IP RIP.

2.2.2 DESCUBRIMIENTO DE LA RED DE VECTOR DISTANCIA

Cada ruteador usando ruteo de vector distancia, empieza por identificar sus propias redes conectadas directamente. En la figura 2.9, una interfaz a cada red conectada directamente, es mostrada en las tablas de ruteo con una distancia de 0.

Como procede el proceso de descubrimiento de red de vector distancia, los ruteadores descubren la mejor ruta al destino basado en métricas.

FIGURA 2.9

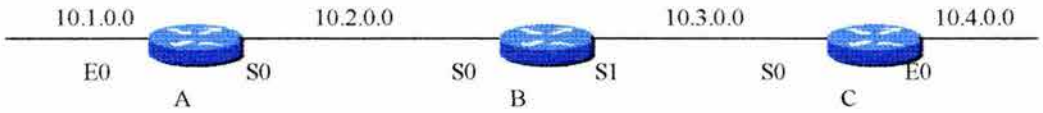


Tabla de Ruteo		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Tabla de Ruteo		
10.1.0.0	S0	0
10.2.0.0	S1	0
10.3.0.0	S1	1
10.4.0.0	S0	1

Tabla de Ruteo		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Por ejemplo, el ruteador A aprende acerca de las otras redes basandose en la información que recibe del ruteador B. Cada una de las entradas de red aprendidas del ruteador B es colocada en la tabla de ruteo del ruteador A y tiene un vector distancia acumulado para mostrar qué tan lejos está la red aprendida por la dirección dada.

2.2.3 CAMBIOS DE TOPOLOGIA DE VECTOR DISTANCIA

Como se mencionó anteriormente, las actualizaciones de tablas de ruteo comunican cambios en la topología. Como con el proceso de descubrimiento de red, las actualizaciones de cambio de topología viajan gradualmente de ruteador a ruteador.

Los algoritmos de vector distancia habilitan al ruteador para enviar la tabla de ruteo entera a cada uno de sus rutadores vecinos. Las tablas de ruteo de vector distancia incluyen información acerca del costo total de la ruta (definido por la métrica) y la dirección lógica del primer ruteador en la ruta a cada red conocida. En la figura 2.9, la métrica de cada ruta es mostrada en la tercera columna de la tabla de ruteo.

Cuando un ruteador recibe la actualización de un ruteador vecino, éste compara la actualización con su propia tabla de ruteo. Si aprende una mejor ruta (métrica más pequeña) a la red desde su vecino, el ruteador actualiza su propia tabla de ruteo. Para calcular una nueva métrica, el ruteador añade el costo para alcanzar su vecino al costo de la ruta reportada por el vecino, la nueva métrica es puesta en la tabla del ruteo del ruteador.

Típicamente, un ruteador envía actualizaciones por multicasting o por broadcasting a cada puerto configurado; pero otros métodos, tales como enviar la tabla sólo a un vecino preconfigurado, son empleados por algunos algoritmos de ruteo.
Multicasting es usado por RIPv2, OSPF y EIGRP. RIP e IGRP usan broadcasting.

2.2.4 PROBLEMA: LOOPS DE RUTEO

Los Loops de ruteo pueden ocurrir si la convergencia lenta de la red en una nueva configuración causa entradas de ruteo inconsistentes.

Tomemos la figura 2.9, si la red 10.4.0.0 falla, se inicia un loop de ruteo entre los ruteadores A, B y C. Los siguientes pasos, decriben el proceso del loop:

- Justo antes de que la red 10.4.0.0 falle, todos los ruteadores tienen un conocimiento consistente de la red y tablas de ruteo correctas, entonces se dice que la red ha convergido. Para este ejemplo, la función de costo es el conteo de saltos; entonces, el costo de cada enlace es 1. El ruteador C es directamente conectado a la red 10.4.0.0 con distancia de 0. El camino del ruteador A a la red 10.4.0.0 es a través del ruteador B con una cuenta de saltos de 2.
- Cuando la red 10.4.0.0 falla, el ruteador C detecta la falla y detienen los paquetes que salen por su interfaz E0. Sin embargo, el ruteador A todavía no ha recibido la notificación de la falla y aún cree que tiene acceso a la red 10.4.0.0 por el ruteador B. La tabla de ruteo del ruteador A refleja una ruta a la red 10.4.0.0 con una cuenta de saltos de 2.
- Como la tabla de ruteo del ruteador B indica la ruta a la red 10.4.0.0, el ruteador C cree que ahora tiene una ruta viable a dicha red por el ruteador B. El ruteador C actualiza su tabla de ruteo para reflejar una ruta a la red 10.4.0.0 con una cuenta de saltos de 2.
- El ruteador A recibe la nueva tabla de ruteo del ruteador B, detecta el vec tor distancia modificado a la red 10.4.0.0 y vuelve a calcular su propio vector distanacia a la red 10.4.0.0 como 3.

Como los ruteadores A, B y C concluyen que la mejor ruta es a través de cada una de ellos, los paquetes destinados a la red 10.4.0.0 continuan saltando entre los tres ruteadores.

2.2.5 SINTOMA: CUENTA A INFINITO

Las actualizaciones inválidas acerca de la red 10.4.0.0 continúan en loop y la cuenta de saltos se incrementa cada vez que el paquete de actualización pasa a través de otro ruteador. Este proceso de continuar incrementando los saltos se llama Cuenta a Infinito.

2.2.6 SOLUCION: DEFINIENDO UN MAXIMO

Las contramedidas del conteo a infinito es que los protocolos de vector distancia definen a infinito como algún número máximo. Un máximo puede ser definido por alguna métrica de ruteo incluyendo cuenta de saltos.

Con esto, el protocolo de ruteo permite el loop de ruteo hasta que la métrica excede el máximo valor permitido. Una vez que el valor de la métrica permitido excede el máximo, la red 10.4.0.0 es considerada inalcanzable (haciendo referencia a la figura 2.9). Los

ruteadores deben asignar ésta como inalcanzable en sus tablas de ruteo, deteniendo la circulación de la información de la actualización.

Definiendo un máximo, los algoritmos de ruteo de vector distancia se corrigen así mismos en respuesta a la información de ruteo incorrecta, aunque no inmediatamente. Un loop puede ocurrir por algun periodo finito de tiempo hasta que el valor máximo de la métrica es excedido.

Un concepto relacionado a esto es el parámetro Time to Live (TTL) que es un paquete que decrese cada que el ruteador procesa el paquete. Cuando TTL es igual a 0, el ruteador descarta el paquete sin enviarlo otra vez. Un paquete atrapado en un loop es removido cuando su TTL expira. IP usa un contador TTL para detener el problema de cuenta a infinito.

2.2.7 SOLUCION: SPLIT HORIZON

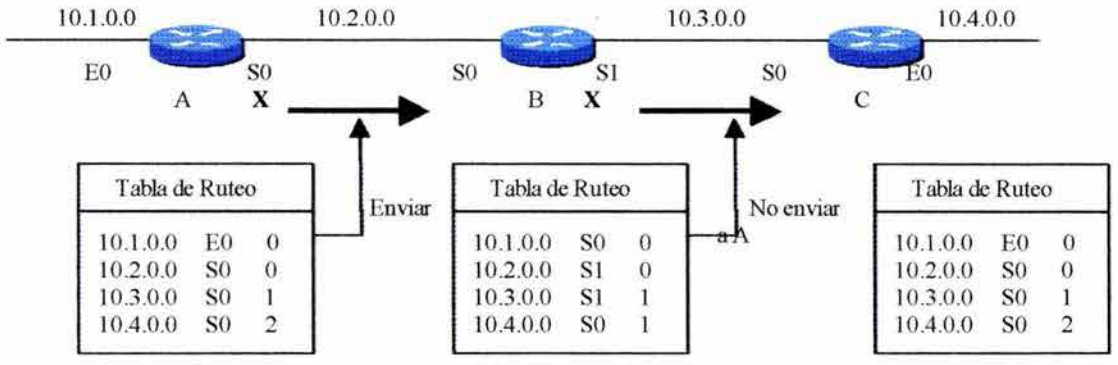
Un camino para eliminar los loops de ruteo y la velocidad de convergencia es por una técnica que se llama Split Horizon. La lógica detrás de Split Horizon es que nunca es útil para enviar información acerca de una ruta en dirección de donde vino originalmente.

En la fugura 2.10 por ejemplo, el ruteador aprende que la red 10.4.0.0 está caída por los siguientes pasos:

- El ruteador B tiene acceso a la red 10.4.0.0 por el ruteador C. No tiene ningún sentido anunciar al ruteador C que el ruteador B tienen acceso a la red 10.4.0.0 a través de él, porque este ruteador siempre tendrá la mejor información acerca de 10.4.0.0.
- Dado que el ruteador B pasa el envío de su ruta a la red 10.4.0.0 al ruteador A, no tienen sentido para el ruteador A avisar de su distancia desde la red 10.4.0.0 al ruteador A.
- No teniendo una ruta alternativa a la red 10.4.0.0, el ruteador B concluye que la red 10.4.0.0 es inaccesible.

En esta forma sencilla, simplemente el Split Horizon no permite que ninguna información de actualización fluya fuera de las mismas interfaces a las que llegó.

FIGURA 2.10



2.2.8 SOLUCION: POISON REVERSE

Poison Reverse es una variación del Split Horizon. Poison Reverse tiende a eliminar los loops de ruteo causados por actualizaciones inconsistentes. Con esta técnica, un ruteador que descubre una ruta inaccesible fija una entrada a la tabla que mantiene el estado de red consistente mientras que otros ruteadores gradualmente convergen correctamente en un cambio de topología. Poison Reverse es utilizado con los Hold-Down Timers, que son explicados más tarde. Poison Reverse es una solución para los loops largos. Por ejemplo, tomando las figuras anteriores, cuando la red 10.4.0.0 se cae, el ruteador C puede remover la conexión a la red 10.4.0.0 registrando una entrada a la tabla de ruteo para que la conexión tenga un costo infinito (ser inalcanzable). Por remover la ruta a la red 10.4.0.0, el ruteador C no es susceptible a otras actualizaciones incorrectas acerca de la red 10.4.0.0 desde los ruteadores vecinos que pueden demandar tener una ruta valida alterna.

Cuando una actualización muestra una métrica para una ruta inexistente, hay un loop. La ruta debe ser removida. Actualmente una ruta es removida si la métrica crece más que un factor de 1.1, porque cambios en las métricas pequeñas pueden ocurrir debido a cambios en la ocupación de un canal. Esta regla es sólo necesaria para eliminar los loops muy grandes. Los loops pequeños puden ser prevenidos por Split Horizon, Triggered Updates y Hold-Down Timers.

2.2.9 SOLUCION: HOLD DOWN TIMERS

Los Hold-Down Timers son usados para prevenir mensajes regulares de actualización inadecuada. Los Hold-Down Timers dicen a los ruteadores que lleven a cabo algunos cambios que puedan afectar a las rutas por algún periodo de tiempo. El tiempo de periodo Hold-Down es calculado para ser mayor al periodo de tiempo necesario para la actualización de la red entera con un cambio en el ruteo.

Los Hold-Down Timers trabajan como sigue:

- Cuando un ruteador recibe una actualización desde un ruteador vecino indicando que la red que era previamente accesible, ahora ya no lo es, el ruteador marca la ruta como inaccesible y empieza un Hold-Down Timer. Si el tiempo de un Hold-Down Timer expira una actualización es recibida desde el mismo ruteador vecino indicando que la red es otra vez accesible, el ruteador marca la red como accesible y remueve el Hold-Down Timer.
- Si una actualización llega desde otro ruteador vecino con una métrica mejor que la originalmente registrada, el ruteador marca la red como accesible y remueve el Hold-Down Timer.
- Si algún tiempo antes de que el Hold-Down Timer expire una actualización es recibida desde un ruteador vecino diferente con una métrica pobre, la actualización es ignorada.

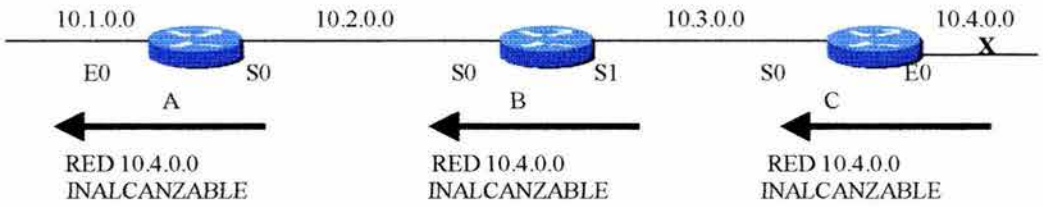
2.2.10 SOLUCION: TRIGGERED UPDATES

En los ejemplos anteriores de loops de ruteo, los loops fueron causados por información erronea, actualizaciones incosistentes, convergencia lenta y sincronización de actualizaciones. Si los ruteadores esperan por sus actualizaciones regularmente programadas, antes de notificar a sus ruteadores vecinos de catastrofes en la red, problemas serios pueden ocurrir.

Normalmente, nuevas tablas de ruteo son enviadas a cada uno de los rutadores vecinos en una base regular. Una Triggered Update es una actualización que es enviada inmediatamente en respuesta a algún cambio en la tabla de ruteo. El ruteador que detecta un cambio en la topología inmediatamente envía mensajes de actualización a los ruteadores adyacentes que, alternadamente, generan Tiggered Updates notificando a sus vecinos del cambio. Esta ola de actualizaciones se propagará a través de esa porción de red donde las rutas son conectadas a la ruta defectuosa.

En la figura 2.11, por ejemplo, el ruteador inmediatamente anuncia que la red 10.4.0.0 es inalcanzable. Sobre la recepción de esta información, el ruteador B anuncia a través de la interfaz S0 que la red está abajo. A su vez el ruteador envía una actualización fuera de la interfaz E0.

FIGURA 2.11



Las actualizaciones deben ser suficientes si se puede garantizar que la ola de actualizaciones es alcanzada por cada ruteador inmediatamente. Sin embargo, existen dos problemas:

- Los paquetes que contienen el mensaje de actualización pueden ser descartados por el enlace en la red.
- Los Triggered Update no suceden instantáneamente. Es posible que un ruteador que no haya recibido todavía un Tiggered Update, publicará una actualización regular en el tiempo incorrecto causando una ruta mala a ser insertada en un ruteador vecino que ya haya recibido un Triggered Update.

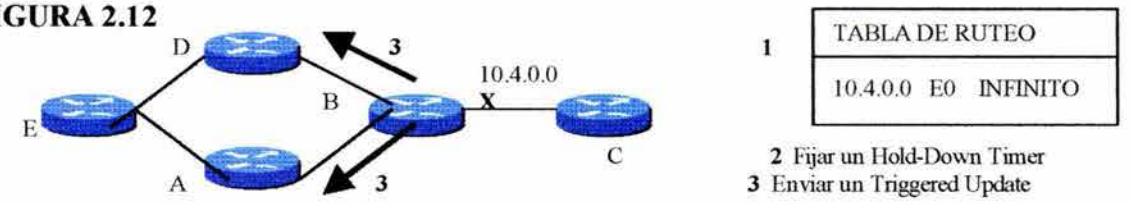
Un acoplamiento de Trigger Updates con Hold-Down Timers es diseñando para solucionar estos problemas. La regla Hold-Down dice que cuando una ruta es removida,

una nueva ruta al mismo destino no sería aceptada por cierto periodo de tiempo. Así, el Triggered Update tiene tiempo para propagarse en al red.

2.2.11 IMPLEMENTACION DE SOLUCIONES EN MULTIPLES RUTAS

Las soluciones individuales discutidas hasta ahora trabajan unidas para prevenir los loops de ruteo en un diseño de red complejo. En este escenario los ruteadores tienen múltiples rutas a cada una. Es importante considerar el diseño de la figura 2.12, que muestra que cada ruteador A, D y E tienen dos rutas a la red 10.4.0.0.

FIGURA 2.12



Cuando la red 10.4.0.0 falla, los siguientes pasos deben ocurrir:

- Ruta removida: Tan pronto como el ruteador B detecta la falla de la red 10.4.0.0, el ruteador B remueve la ruta indicando una cuenta de salto infinito a esa red.
- Fija in Hold-Down Timer: Una vez que el ruteador B remueve la ruta, éste fija un Hold Down Timer.
- Enviar un Triggered Update: El ruteador B también envía un Triggered Update a los ruteadores A y D indicando que la red 10.4.0.0 está "posiblemente" caída. La nueva información de la ruta se propaga por el resto de la red fijando un Hold-Down Timer y Triggered Updates. Los ruteadores D y A reciben el Triggered Update y fija sus propios Hold-Down Timers para suprimir algunos cambios en la ruta por un periodo de tiempo específico. Los ruteadores D y A, alternadamente, envían un Triggered Update al ruteador E indicando que la red 10.4.0.0 no es accesible.

Finalmente el ruteador E recibe el Triggered Update acerca del estado de la red 10.4.0.0 desde los rutadores D y A. El ruteador E entonces fija sus Hold-Down Timers y espera hasta que uno de los siguientes eventos ocurra:

- El Hold-Down Timer expira. En este caso, el ruteador E sabe que la red 10.4.0.0 está disponible.
- Otra actualización es recibida indicando que el estado de la red no ha cambiado. En este caso, el rutador E actualiza sus tablas con la nueva información.
- Otra actualización es recibida indicando una nueva ruta con una mejor métrica. En este caso, el ruteador E actiualiza sus tablas con la nueva información.

A continución se explicarán los protocolos de ruteo de vector distancia.

2.3 ROUTING INFORMATION PROTOCOL (RIP)

RIP es un protocolo de vector distancia para trabajar con redes de tamaño pequeño o mediano. RIP es de uso extenso como protocolo de ruteo que fuera formalmente definido por RFC 1080. RIP Versión 2, definido por RFC 2453, agrega algunas características adicionales y funcionalidades.

Algunas características utilizando RIP, especialmente en redes pequeñas, son que hay pequeños gastos en términos de ancho de banda y tiempo de configuración y administración. RIP también es fácil de implantar.

Los ruteadores que corren RIP pueden participar como dispositivos pasivos y activos. Un dispositivo en modo activo publicaría sus rutas, mientras que un dispositivo en modo pasivo oirá los anuncios de los dispositivos en modo activo. Por obvias razones, los ruteadores son dispositivos en modo activo, mientras que los hosts a menudo corren en modo pasivo cuando corren RIP.

RIP es utilizado para transportar información acerca de rutas o destinos. RIP confía en el acceso a la información acerca de sus redes directamente conectadas. Un dispositivo RIP activo logra esto por la publicación periodica de su información de ruteo. La información que usa RIP para la construcción de esas actualizaciones es tomada de la tabla de ruteo (o de la base de datos de RIP). La tabla de ruteo contiene una entrada para cada destino que es alcanzable en el sistema. Cada entrada tiene la siguiente información:

- Dirección IP del destino.
- Una métrica que representa el costo total para conseguir un datagrama del host al destino.
- La dirección IP del próximo ruteador a lo largo de la ruta la destino.
- Los temporizadores asociados con el ruteador.
- La bandera de cambio de ruta que indica la información acerca de que la ruta ha cambiado recientemente.

Lo siguiente es un ejemplo de una tabla de ruteo RIP:

DESTINO	PROXIMO SALTO	DISTANCIA	TEMPORIZADOR	BANDERA
RED A	RUTEADOR 1	3	11	X, Y
RED B	RUTEADOR 2	5	12	X, Y
RED C	RUTEADOR 1	2	13	X, Y

RIP mantiene solo la mejor ruta a un destino. Para evitar que la información de ruteo oscile entre rutas de costo igual, el RFC especifica que las actualizaciones de los próximos saltos deben ser usadas sólo si la métrica reportada es menos que la ruta instalada actualmente.

Los cambios de topologías de red pueden causar cambios en rutas. Esos cambios pueden resultar en una nueva ruta conviertiendose en la mejor ruta a un detino en particular. Cuando ocurren cambios en una topología de red, ellos son reflejados en mensajes de actualización de ruteo. Por ejemplo, cuando un ruteador detecta que una conexión a otro ruteador está fallando, vuelva a calcular esas rutas y envía mensajes de actualización de ruteo. Cada rutedor recibe un mensaje de actualización de ruteo que incluye una actualización de cambio y la propaga.

2.3.1 METRICA DE RIP

RIP utiliza una sola métrica, cuenta de saltos, para medir la distancia entre la red fuente y la red destino. Cada salto en este camino tiene asignado un valor de cuenta de saltos que usualmente en RIP es 1. Cuando un ruteador recibe una actualización de ruteo que contiene una entrada de red destino nueva o cambiada, el ruteador añade el 1 al valor de la métrica indicada en la actualización y la incorpora a la red en la tabla de ruteo. La dirección IP del emisor es usada como el próximo salto. Este método para incrementar la métrica de ruteo teóricamente proveerá de información libre de loops en un ambiente perfectamente estable, pero cuando la topología cambia o cuando las redes se vuelven inaccesibles, puede conducir a dos problemas básicos hechos por los algoritmos de vector distancia: lenta convergencia y cuenta a infinito.

La información de ruteo acerca de cambios en la topología se propaga lentamente a través de la red debido a inconsistencias en las tablas de ruteo. Limitando el número de saltos en la red ayuda a mejorar el problema de convergencia y también permite prevenir los loops de ruteo. RIP está limitado a las redes donde el camino o la ruta más larga son de 15 saltos. Con RIP, si un ruteador recibe una actualización de ruteo que contenga una entrada nueva o un cambio de entrada y si aumenta la métrica en 1, la métrica es 16. La red destino es considerada inalcanzable. En otras palabras, 16 es equivalente a infinito en una red RIP. Si una red llegara a ser completamente inaccesible, entonces los ruteadores podrían contar a infinito.

2.3.2 TEMPORIZADORES DE RIP

RIP también utiliza temporizadores para evaluar su desempeño. Todos los ruteadores que utiliza RIP envían un mensaje de actualización a todos sus vecinos aproximadamente cada 30 segundos. El RFC especifica que las publicaciones deben ser aleatorias de arriba de +/- 5 segundos para prevenir sincronizacion de las actualizaciones de ruteo.

Si un ruteador vecino no ha respondido en 180 segundos, se asume que este ruteador no está disponible o que la red conectada o el ruteador es unitilizable y es marcado como

inválido. El vecino es inalcanzable por el envío de un mensaje normal de actualización con métrica a infinito, entonces la ruta es colocada en estado de "caído" con una distancia de 16 y se mantiene en la tabla de ruteo.

Los temporizadores actuales usados para lograr las tareas anteriores son:

- Routing-update timer
- Route-Invalid timer
- Route-hold-down timer
- Route-flush timer

El RIP **Routing-update timer** es generalmente fijo en 30 segundos garantizando que cada ruteador envía una tabla completa de su tabla de ruteo a todos sus vecinos. El **Route-invalid timer** determina en cuánto tiempo debe expirar sin que un ruteador oiga acerca de una ruta en particular antes de que la ruta sea considerarda inválida. Cuando una ruta es marcada inválida, los rutadores vecinos son notificados de este hecho. Esta notificación debe ocurrir antes de que expire el **Route-flush timer.** Cuando el **Route-flush timer** expira, la ruta es removida de la tabla de ruteo. Los valores típicos para esos temporizadores son 180 segundos para el temporizador **Route-hold-down timer** y para el **Route-flush timer** es 240 segundos.

2.3.3 CARACTERISTICAS DE ESTABILIDAD

Para ajustarse a rápidos cambios de topologías de red, RIP especifica numerosas características de estabilidad que son comunes para algunos protocolos de ruteo. RIP implanta el mecanismo Split Horizon con Poison Reverse y Hold-Down para prevenir información de ruteo incorrecta. Split Horizon previene que mensajes incorrectos sean propagados no anunciando rutas sobre una interfaz que el ruteador se está usando para alcanzar las rutas. Poison Reverse operan por la publicación de rutas que no son alcanzados por una métrica de infinito de regreso a la fuente de la ruta. Hold-Down es un método para marcar rutas inválidas.

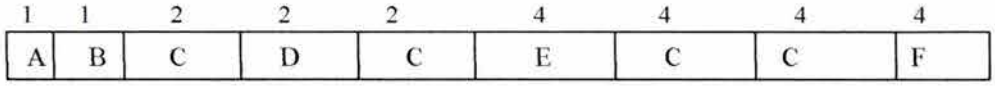
Las actualizaciones Triggered también son una caracteríatica de convergencia y estabilidad.

2.3.4 FORMATO DE PAQUETE DE RIP

RIP es un formato basado en User Datagram Protocol (UDP)[22]. Cada ruteador que utiliza RIP tiene un proceso de ruteo que envía y recibe datagramas en el puerto UDP número 520, puerto de RIP. Todas las comunicaciones para el proceso RIP para el ruteador usan este puerto. El tráfico RIPv1 es enviado como un broadcast a la dirección IP 255.255.255.255 por default.

[22] Es un protocolo simple que intercambia datagramas si conocimiento o garantia de entrega, requiriendo que el procesamiento de errores y retransmisión sea manejado por otros protocolos.

El siguiente es el formato de paquete para la versión original de RIP, definido en RFC 1058.



A=Comando (solicitud o respuesta)
B=Numero de versión
C= Zero
D= Identificador de familia de dirección
E= Dirección
F= Métrica

El campo Comando indica si el paquete es una solicitud o es una respuesta. La solicitud pregunta al ruteador para enviar todo o una parte de su tabla de ruteo. La respuesta puede ser un mensaje de actualización no solicitada o una respuesta a la solicitud. Múltiples paquetes RIP son utilizados para contener información de larga tablas de ruteo.

El número de Versión especifica la versión de RIP usada. Este comando puede señalar potencialmente versiones incompatibles.

El campo Zero no es utilizado.

El Identificador de Familia de Dirección (AFI) especifica la familia de direcciones utilizada. RIP está diseñado para tener información de ruteo para varios protocolos diferentes. Cada entrada tiene un AFI para indicar el tipo de direcciones que es especificado. El AFI para IP es 2.

La Métrica indica el número de saltos hacia el destino. Este valor es entre 1 y 15.

El formato de paquete RIPv1 no distingue entre diferentes tipos de direcciones. Campos que son etiquetados "direcciones" pueden contener algo de lo siguiente:

- Direcciones de Host
- Números de subred
- Número de red
- Zero (default)

2.3.5 RIP VERSION 2

Fue recreado como una funcionalidad adicional al RIP original y también tiene algunas mejoras. RIPv2 usa la misma base de algoritmos que la versión original, pero soporta etiquetas de rutas externas, máscaras de subred, direcciones al próximo salto y autenticación.

2.3.5.1 ETIQUETAS DE RUTA EXTERNA

RIPv2 incluye un campo llamado Route Tag, el cual es un atributo asignado a una ruta que debe ser publicada con otra ruta. Esto provee una mecanisnmo para separar rutas internas RIP desde rutas RIP externas, las cuales deben ser importadas desde un Exterior Gateway Protocol (EGP)

2.3.5.2 MASCARA DE SUBRED

RIPv2 permite el uso de la variable de máscara de subred en la red. En RIPv1 hay una ambigüedad subred/host porque los nodos no conocen máscaras de subred; entonces, analizando las direcciones, pueden ser ambiguas. En RIPv2 hay un campo de máscaras de subred, el cual es aplicado a las máscaras de subred para rendir la porción de red de la dirección. Si el campo es cero la máscara de red no es aplicada.

2.3.5.3 DIRECCIONES DEL PROXIMO SALTO

RIPv2 soporta direcciones de próximo salto; esta disposición es para optimización de rutas en un ambiente que usa múltiples protocolos de ruteo. Por ejemplo, si RIPv2 corre en una red con Enhance Interior Gateway Protocol (EIGRP)[23] y un ruteador corre ambos protocolos, entonces el ruteador podría indicar si un salto mejor que ese mismo existe para el destino. El campo de direcciones del próximo salto es un campo consultivo y si la información proveida es ingnorada, otra ruta podría tomarla.

2.3.5.4 AUTENTIFICACION

RIPv2 soporta mecanismos de autenticación, el cual es una función por mensaje. Con RIPv2 hay un solo campo de dos octetos disponible en el encabezado de mensaje y desde que dos octetos no son suficientes, el esquema de autenticación usa el espacio de una entrada de la tabla de ruteo.

Para identificar si la entrada contiene autenticación, checa si el AFI de la primera entrada es 0xFFFF. Si es verdad, puede haber un máximo de 24 entradas. El AFI o 0xFFFF no debería ser usado si la autenticación no es usada.

El tipo de password para RIPv2 es un simple password.

2.3.5.5 MULTICASTING

Los paquetes RIPv2 pueden ser multicast en lugar de broadcast. La dirección multicast es 224.0.0.9. Multicasting reduce la carga en los hosts que no soportan protocolos de ruteo y también permite que los ruteadores RIPv2 compartan información que ruteadores RIPv1 no pueden.

---

[23] Protocolo de ruteo híbrido (de Vector distancia y de estado de enlace): Será explicado más adelante.

2.3.6 FORMATO DE PAQUETE DE RIPv2

Command	Version	Unused	AFI	Route Tag	IP Address	Subnet Mask	Next Hop	Metric

Version: Especifica la versión RIP usado.

Unused: Valor fijado en cero.

Route Tag: Provee un método para distiguir entre rutas internas aprendidas por RIP y rutas externas que fueron aprendidas desde otros rutadores.

IP Address: Especifica la dirección IP de la entrada.

Subnet Mask: Contiene la máscara de subred para la entrada.

2.4 INTERIOR GATEWAY ROUTING PROTOCOL (IGRP)

IGRP es un protocolo de vector distancia que usa una combinación de métricas como retardo, ancho de banda, confiabilidad y carga que son los factores en la toma de decisiones en ruteo.

IGRP provee un amplio rango para sus métricas. Fiabilidad y carga, por ejemplo, toma cualquier valor entre 1 y 255; ancho de banda puede tomar valores reflejando velocidades desde 1,200bps hasta 10 Giga bits por segundo, mientras que el retardo puede tomar valores de 1 a 2 a la 24ava. potencia. Amplios rangos de métricas permiten la configuración satisfactoria en redes con una amplia variedad de características de desempeño. Lo más importante, los componentes de la métrica son combinados en un algoritmo. Todos los administradores de red pueden influenciar en la selección de rutas de manera intuitiva.

Para proveer flexibilidad adicional IGRP permite el ruteo multidireccional; líneas duales de igual ancho de banda pueden correr en una sola frecuencia de tráfico con intercambio automático a la segunda línea si la primera línea está caída. También múltiples rutas pueden ser usadas incluso si las métricas son diferentes. Por ejemplo, si una ruta es tres veces mejor que otra porque la métrica es tres veces menor, la mejor ruta puede ser tres veces más usada.

2.4.1 TEMPORIZADORES DE IGRP

IGRP mantiene un número de temporizadores y variables conteniendo intervalos de tiempo. Esos temporizadores incluyen un Update Timer, un Invalid Timer, un Hold-Down Timer y un Flush Timer. El Update Timer especifica qué tan frecuentemente los mensajes de actualización de ruteo deben ser enviados. En IGRP este valor es de 90 segundos. El

invalid Timer especifica qué tanto el ruteador debe esperar, en ausencia de mensajes de actualización de ruteo acerca de una ruta específica, antes de declarar la ruta inválida. El IGRP por defecto para esta variable es tres veces el periodo de actualización. La variable Hold-Timer especifica el periodo Hold-Down. El IGRP por defecto para esta variable es tres veces el periodo update timer más 10 segundos.

2.4.2 RUTEO DE ESTADO DE ENLACE

El segundo algoritmo básico usado en ruteo es el algoritmo de estado de enlace.

Los algoritmos de ruteo de estado de enlace -también conocidos como algoritmos Shortest Path First (SPF)- mantienen una compleja base de datos de información de topología, mientras que los algoritmos de vector distancia tienen entradas para distintas redes y un valor de métrica para alcanzar esas redes, pero no tienen el conocimiento de ruteadores distantes. Los algoritmos de ruteo de estado de enlace mantienen un amplio conocimiento de los ruteadores distantes y la manera en la que se interconectan. Ejemplo de protocolos de estado de enlace son NLSP, OSPF e IS-IS.

El ruteo de estado de enlace utiliza los Link-State Packets (LSP), una base de datos topológica, el algoritmo SPF, el resultante árbol SPF y finalmente, una tabla de ruteo de rutas y puertos a cada red para el envio de información.

2.4.3 DESCUBRIMIENTO DE LA RED ESTADO DE ENALCE

Los mecanismos de descubrimiento de red de estado de enlace son usados para crear una vista de la red entera. Todos los ruteadores de estado de enlace comparten esta vista común de la red.

El descubrimiento de red para el ruteo de estado de enlace utiliza los siguientes procesos:

- Los ruteadores aprenden de sus vecinos, es decir, otros ruteadores que están en redes directamente conectadas a ellas.
- Los ruteadores transmiten LSPs sobre la red. El LSP contiene información acerca de la red a la cual los ruteadores están conectados.
- Después, los ruteadores construyen su base de datos topológica constituida de todos LSPs de la red.
- El algoritmo SPF calcula el alcance de la red determinado la ruta más corta a cada red en el protocolo de red de estado de enlace. El árbol SPF expresa las rutas del ruteador a todos los destinos.
- El ruteador lista sus mejores rutas y puerto al destino en su tabla de ruteo.

2.4.4 CAMBIOS DE TOPOLOGIA DE ESTADO DE ENLACE

Los algoritmos de estado de enlace confían en los ruteadores teniendo una vista completa de la red. Siempre que una topología de estado de enlace cambia, los ruteadores que primero son enterados de este cambio envían información a otros ruteadores o a un ruteador designado, el cual todos los demás ruteadores pueden utilizar para actualizaciones. Esta acción exige la propagación de la información de ruteo común a todos los ruteadores de la red. Para alcanzar la convergencia, cada ruteador debe hacer lo siguiente:

- Saber de sus vecinos; nombre del vecino, si el vecino está funcionando o no y el costo del enlace al vecino.
- Construyen un LSP de la lista los nombres y costos de los enlaces de sus ruteadores vecinos. Esta información incluye nuevos vecinos, cambios en los costos de enlaces y enlaces a los vecinos que no están funcionando.
- Envía este LSP a todos los ruteadores.
- Cuando se recibe el LSP, se registra en la base de datos; entonces puede almacenar el LSP recientemente generado de otro ruteador.
- Utiliza los datos LSP acumulados para construir un mapa completo de la topología de la red.

Cada vez que un LSP hace un cambio en la base de datos de estado de enlace, el algoritmo vuelve a calcular las mejores rutas y actualiza la tabla de ruteo. Después cada ruteador toma el cambio de la topología para determinar la mejor ruta a usar para el paquete.

Diferente de los algoritmos de vector distancia, los algoritmos de estado de enlace se corrigen a sí mismos. Un loop es terminado por un algoritmo de estado de enlace tan pronto como la base de datos de la tabla de ruteo se actualice.

2.4.5 PREOCUPACIONES DE ESTADO DE ENLACE

Ningún protocolo de ruteo es perfecto. Los administradores de red necesitan tener en mente dos principales preocupaciones de ruteo de estado de enlace:

- Requerimientos de procesamiento y memoria.
- Requerimientos de ancho de banda.

Correr protocolos de estado de enlace, en la mayoría de las situaciones, requiere que los ruteadores utilicen mayor procesamiento y mayor memoria. Los administradores de red deben garantizar que los ruteadores selectos son capaces de proveer esos recursos de ruteo.

Los ruteadores no pierden de vista a sus vecinos ni a las redes que ellos alcanzan a través de otros nodos de ruteo. Para ruteo de estado de enlace, la memoria debe manejar la información de varias publicaciones de estado de enlace, árbol de topología y la tabla de ruteo.

La complejidad de procesamiento para calcular la ruta más corta es proporcional al número de enlaces de la red a los ruteadores.

Otra causa a considerar es el ancho de banda consumido por la inundación de paquete de estado de enlace inicial. Durante el proceso de descubrimiento inicial, todos los ruteadores utilizan un protocolo de estado de enlace y envían LSPs a todos los demás ruteadores.

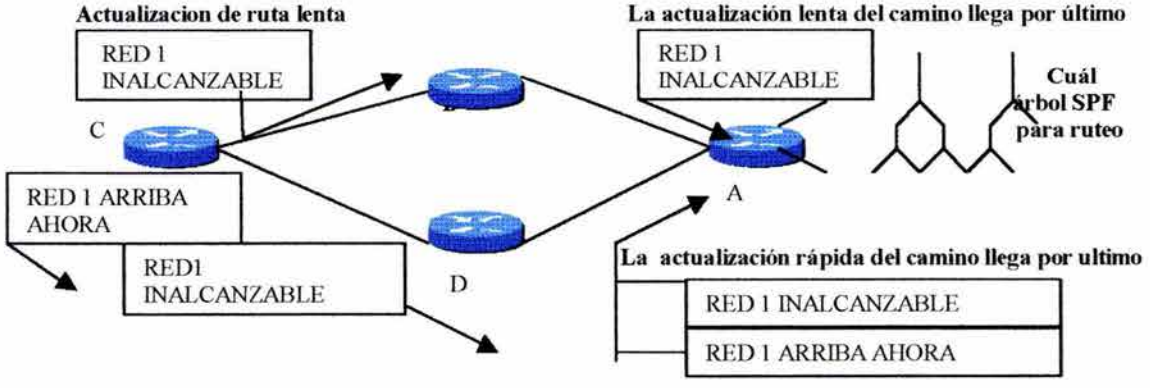
2.4.6 PROBLEMA: ACTUALIZACIONES DE ESTADO DE ENLACE

El aspecto más critico y complejo de ruteo de estado de enlace es estar seguros de que todos los ruteadores obtendrán todos los LSP necesarios. Los ruteadores con diferentes conjuntos de LSP calcularán rutas en una topología de datos diferente. Entonces, las rutas llegan a ser inalcanzables como resultado de este desacuerdo en ruteadores acerca del enlace. La figura 2.13 provee un ejemplo de la información de rutas consistentes.

Considerar la siguiente secuencia de eventos en la figura 2.13:

- Suponer que la red 1 entre los ruteadores C y D está "caída". Como se discutió anteriormente, ambos ruteadores construyen un LSP para reflejar el status inalcanzable.
- Después, la red 1 se vuelve a levantar; otro LSP reflejando este cambio de topología es necesario.
- Si el mensaje de actualización original "Red 1 Inalcanzable" del ruteador C utiliza una ruta lenta, esto puede llegar al ruteador A después que el LSP "Red 1 arriba Ahora" del ruteador D.
- Sin la sincronización de LSP, el ruteador A entra en un dilema acerca del árbol SPF a construir: si usa una de estas rutas con o sin red 1. ¿Cuál es la ruta más recientemente reportada como inalcanzable?

FIGURA 2.13



Si la distribución de LSP a todos los ruteadores no se sincroniza correctamente, el ruteo de estado de enlace puede resultar en rutas inválidas.

Utilizando los protocolos de estado de enlace en redes grandes puede intensificar el problema de distribución de LSP.

Por ejemplo, si una parte de la red funciona primero con otras partes funcionando más tarde, como a menudo ocurre, entonces cuando una red está en proceso de crecer, la orden de enviar y recibir LSP puede variar. Esta variación puede alterar y deteriorar la convergencia. Los ruteadores pueden aprender acerca de diferentes versiones de topología antes que construyan su árbol SPF y sus tablas de ruteo.

También en redes grandes, hay más probabilidad que haya una variación de la velocidad de transmisión en diferentes partes de la red. Eventualmente, una partición puede dividir la red en partes de actualización rápida y partes de actualización lenta. Entonces, los administradores de red deben localizar las averías para restaurar una conectividad aceptable.

Con actualizaciones defectuosas, los LSP pueden multiplicarse y propagarse a través de la red y consumir más y más ancho de banda.

2.4.7 SOLUCION: MECANISMOS DE ESTADO DE ENLACE

El ruteo de enlace de datos tiene varias técnicas para prevenir o corregir problemas potenciales de requerimientos de recursos y distribución de LSP:

- Un administrador de red puede reducir la distribución periódica de LSP de modo que las actualizaciones sólo ocurren después de cierta duración. Reduciendo el rango de actualizaciones periódicas no interfiere con actualizaciones Triggered de LSP por topología de red.
- Actualizaciones LSP pueden ir a un grupo Multicast en lugar de inundar a todos los ruteadores. En una LAN interconectada se puede usar uno o más ruteadores designados como un depósito de transmisiones LSP. Otros ruteadores pueden utilizar esos ruteadores designados como unas fuentes especializada de topología de datos consistente.
- En redes grandes, se puede instalar la jerarquía completa en diferentes áreas. Un ruteador en un área del dominio jerárquico no necesita almacenar y procesar LSP de otros ruteadores no localizados en la misma área.

2.4.8 COMPARANDO RUTEO DE VECTOR DISTANCIA CON RUTEO DE ESTADO DE ENLACE

Las principales diferencias pueden ser resumidas como sigue:

- Ruteo de vector distancia consigue todos los datos topológicos desde la perspectiva de recibir desde el proceso de información de la tabla de ruteo de sus vecinos. El

ruteo de estado de enlace obtiene una amplia vista de la topología de la red entera por acumulación de LSP.

- El ruteo de vector distancia determina la mejor ruta añadiendo el valor de la métrica en cada ruta. Minetras la métrica sea más larga, más largo es el camino a la red. Mientras la métrica sea más corta, el camino más corto a la red. Para ruteo de estado de enlace, cada ruteador trabaja simultáneamente su propio camino más corto al destino.
- Con la mayoría de los protocolos de vector distancia, las actualizaciones para cambios en la topología son actualizaciones periódicas de tablas de ruteo. Las tablas de ruteo enteras pasan de un ruteador a otro que usualmente resulta en una convergencia más lenta que el ruteo de estado de enlace. Con los protocolos de estado de enlace las actualizaciones son usualmente Triggered por cambios en la topología. Relativamente pequeños LSP son pasados a todos los ruteadores o a un grupo multicast de ruteadores, usualmente resulta en una convergencia más rápida.

2.4.9 RUTEO HIBRIDO

Una tercera parte de protocolos de ruteo resulta de la combinación de los aspectos de los protocolos de vector distancia y protocolos de estado de enlace. Esta tercera parte es llamada Híbrido Balanceado.

El protocolo de ruteo híbrido balanceado utiliza vectores de distancia con métricas más exactas para determinar las mejores rutas al destino. Sin embargo, difiere de los protocolos de vector distancia porque utiliza actualizaciones Triggered.

El tipo de ruteo híbrido balanceado converge relativamente, como los protocolos de estado de enlace; sin embargo, difiere de esos protocolos al acentuar la economía en el uso de recursos tales como ancho de banda y memoria.

Ejemplos de protocolos de ruteo híbrido balanceado son Intermediate System-to-Intermediate System y Enhanced Interior Gateway Routing Protocol (EIGRP).

2.5 OPEN SHORTEST PATH FIRST (OSPF)

OSPF es un protocolo de ruteo de estado de enlace que llama para el envío de Link-State Adversitisements (LSA) para todos los otros ruteadores en la misma área jerárquica.

Como un protocolo de estado de enlace, OSPF contrasta con RIP e IGRP, los cuales son protocolos de ruteo de vector distancia.

A diferencia de RIP, OSPF puede operar en una jerarquía. La entidad más grande en la jerarquía es el Autonomous System (AS), el cual es una colección de redes bajo una administración común que comparte una estrategia de ruteo.

Un Autonomous System puede ser dividido en un número de áreas, los cuales son grupos de redes contiguos y hosts asociados. Los ruteadores con múltiples interfaces pueden participar en múltiples áreas. Esos ruteadores son llamados *Area Border Routers* y mantienen separadas las bases de datos lógicas para cada área.

Una base de datos topológica es esencialmente una vista total de redes en relación con los ruteadores. Las bases de datos topológicas contienen la información de LSA recibidos de todos los ruteadores en la misma área. Como los ruteadores en la misma área comparten la misma información, ellos tienen bases de datos topológicas idénticas.

El término *Dominio* algunas veces es usado para describir una porción de red en la cual todos los ruteadores tienen bases de datos topológicas idénticas. Dominio es frecuentemente alternativamente con AS.

Una topología de área es invisible a entidades fuera del área. Manteniendo las topologías dentro de áreas separadas, OSPF pasa menos tráfico de ruteo que si el AS no fuera particionado.

El área particionado crea dos diferentes tipos de ruteo OSPF dependiendo de si la fuente y el destino están en la misma o en áreas diferentes. *Intra-area routing* ocurre cuando la fuente y el destino están en la misma área. *Inter-area routing* ocurre cuando la fuente y el destino están en diferentes áreas.

Un *OSPF Backbone* es el responsable de distribuir información de ruteo entre áreas. Esto consiste de todos los Area Border Routers, redes no entermente contenidas en un área y sus ruteadores adjuntos.

El mismo Backbone es un área, entonces todos los ruteadores Backbone utilizan los mismos procedimientos y algoritmos para mantener la información de ruteo que cualquier ruteador de área. La topología de Backbone es invisible a todos los ruteadores Intra-area, como son topologías de áreas individuales al Backbone.

Las áreas pueden ser definidas de tal manera que el Backbone no sea contiguo. En este caso, la conectividad de Backbone debe ser restaurado a través de enlaces virtuales. Los enlaces virtuales son configurados entre algunos ruteadores que comparten un enlace al área de no Backbone como si fueran enlaces directos.

2.5.1 ALGORITMO OSPF

El algoritmo de ruteo SPF es la base de las operaciones de ruteo. Cuando un ruteador SPF se acciona, se inicializa su estructura de datos de protocolo de ruteo y entonces espera indicaciones desde los protocolos de las capa inferiores de que su interfaz esta en función.

Después de que el ruteador está seguro de que sus interfaces funcionan, éste utiliza el protocolo "Hello" de OSPF para adquirir vecinos, los cuales son ruteadores con interfaces a una red común. El ruteador envía los paquetes "Hello" a sus vecinos.

En redes multiacceso (redes que soportan más de dos ruteadores) el protocolo "Hello" elige un *Designated Router* y un *Designated Router* de respaldo. Entre otras cosas, es el responsable de generar LSA para la red multiacceso. Los *Designated Routers* reducen el tráfico de la red y el tamaño de la base de datos topológica.

Cuando las bases de datos de estado de enlace de dos ruteadores vecinos son sincronizados, se dice que los ruteadores son adyacentes. En redes multiacceso el *Designated Router* determina cuáles ruteadores deben ser adyacentes. Las bases de datos topológicas son sincronizadas entre pares de ruteadores adyacentes. Las adyacencias controlan la distribución de paquetes de protocolos de ruteo, los cuales son enviados y recibidos sólo en la adyacencia.

Cada ruteador periódicamente envía un LSA para proveer la información de las adyacencias del ruteador o información a otros cuando el estado del ruteador cambia. Comparando las adyacencias establecidas a estados de enlaces, los ruteadores que fallan pueden ser detectados rápidamente y la topología de red alterada apropiadamente. Desde la base de datos topológica generada de LSA, cada ruteador calcula un algoritmo SPF.

2.5.2 FORMATO DE PAQUETE OSPF

Todos los paquetes OSPF empezan con 24 bytes de encabezado.

1	1	2	4	4	2	2	8	Variable
Version Number	Type	Packet Length	Router ID	Area ID	Cheksum	Authentication Type	Auttheticacion	Data

- Versión Number: Identifica la versión de OSPF utilizada.
- Type: Identifica el paquete OSPF como una de las siguientes:
  1. Hello: Establece y mantiene relaciones entre vecinos.
  2. Descripción de bases de datos: Describe el contenido de la base de datos topológica. Esos mensajes son intercambiados cuando una adyacencia es inicializada.
  3. Solicitud Link-State: Piezas de solicitud de bases de datos topológicas de ruteadores vecinos. Estos mensajes son intercambiados después de que el ruteador descubre que partes de su base de datos topológica son obsoletas.
  4. Actualización Link-State: Responde un paquete de solicitud Link- State. Estos mensajes son utilizados para la dispersión regular de LSA. Varios LSA pueden ser incluidos en un simple paquete de actualización Link-State.
- Packet Length: Especifica la longitud del paquete, incluyendo el encabezado OSPF en Bytes.
- Router ID: Identifica la fuente del paquete.
- Area ID: Identifica el área al cual el paquete pertenece. Todos los paquetes OSPF están asociados con una simple área.

- Checksum: Checa el paquete entero por si hay algún daño.
- Authentication Type: Contiene el tipo de autenticación. Todos los protocolos OSPF son autenticados
- Autenticación: Contiene información de autenticación.
- Data: Contiene la información encapsulada.

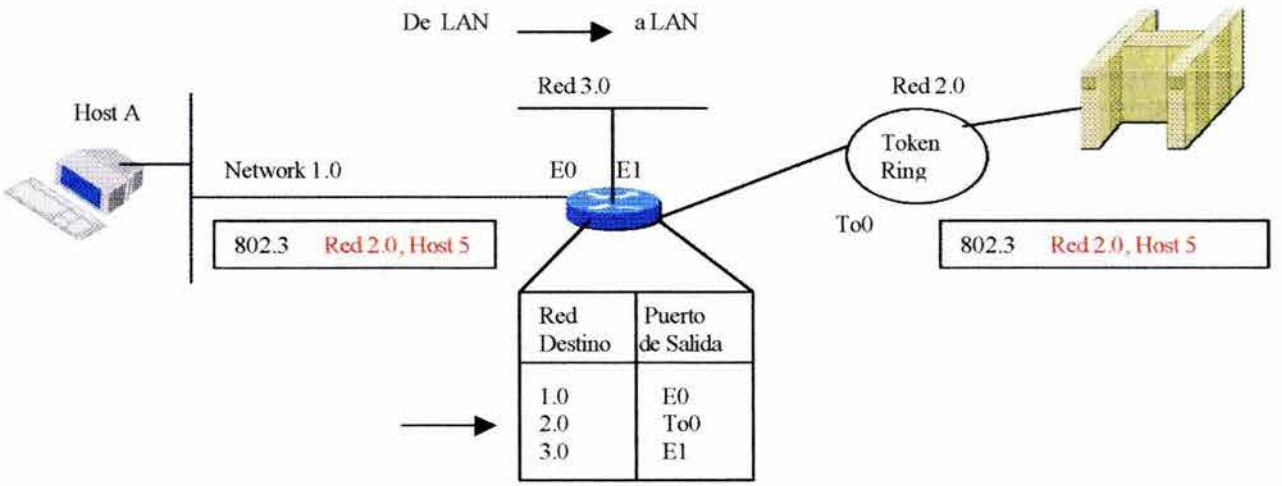
2.6 PROCESOS BÁSICOS DE RUTEO

Si una red utiliza mecanismos de ruteo de vector distancia o de enlace de datos, los ruteadores deben realizar las mismas funciones básicas de ruteo. Los ruteadores deben ser capaces de manejar paquetes encapsulados en diferentes frames de bajos niveles sin cambiar el direccionamiento de capa 3 de los paquetes.

2.7 RUTEO LAN-TO-LAN

La figura 2.14 muestra un ejemplo de la interconexión de la capa de red en ruteo LAN-to LAN. En este ejemplo el tráfico del paquete desde el nodo A en la red Ethernet 1.0, necesita una ruta al host 5 en la red Token Ring 2.0. Los hosts LAN dependen del ruteador y de su direccionamiento de red consistente para encontrar la mejor ruta.

FIGURA 2.14



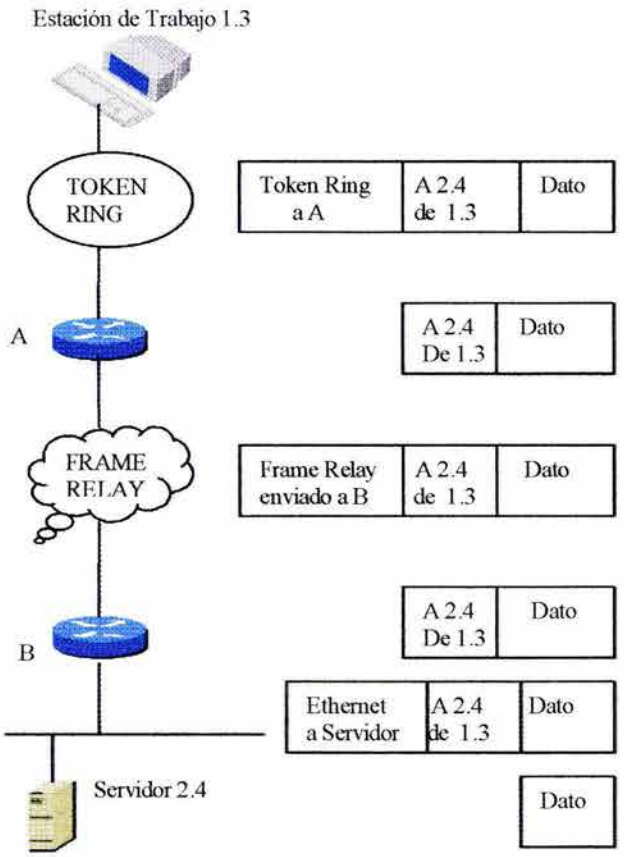
Cuando el ruteador revisa las entradas de su tabla de ruteo descubre que la mejor ruta a la red 2.0 usa el puerto de salida To0, la interfaz a la red LAN Token Ring.

Aunque el Framing de capas inferiores debe cambiar mientras que el ruteador cambia el tráfico del paquete de la red Ehternet 1.0 a la red Token Ring 2.0, el direccionamiento de capas es el mismo.

2.8 RUTEO LAN-TO-WAN

Conforme las redes crecen, la ruta que toma el paquete puede encontrar varios puntos de retardo y una variedad de tipos de enlace de datos más allá de la red. Por ejemplo, en la figura 2.15, un paquete de la estación de trabajo 1.3 debe atravesar tres enlaces de datos para alcanzar al servidor de archivos 2.4.

FIGURA 2.15



El ruteo es como sigue:

- La estación de trabajo envía un paquete al servidor encapsulando en un frame Token Ring al ruteador A en la capa de enlace de datos y el servidor en la capa de red.
- Cuando el ruteador recibe el frame, éste remueve el paquete del frame Token Ring y lo encapsula en un frame de Frame Relay y lo envía al ruteador B.
- El ruteador B remueve el paquete del frame de Frame Relay y envía el paquete al servidor en un nuevo frame Ethernet.

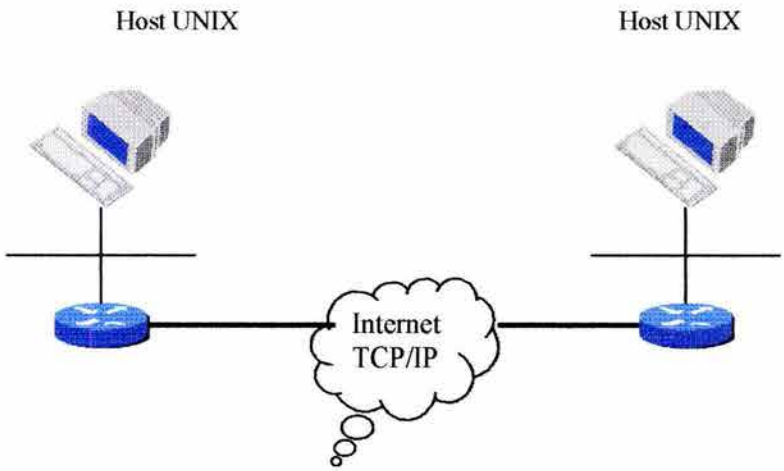
- Cuando el servidor recibe el frame Ethernet, lo extrae y pasa el paquete al proceso apropiado cuando de capas superiores.

CAPITULO 3

DESCRIPCION DE TCP/IP

El conjunto de protocolos TCP/IP (Transmisión Control Protocol/Internet Protocol) fue desarrollado como parte de una investigación hecha por la Defense Advanced Research Projects Agency (DARPA). Esto fue originalmente desarrollado para proveer comunicación entre dispositivos conectados a través de DARPA. Ahora TCP/IP es el protocolo estándar para comunicaciones de redes y sirve como protocolo de transporte para Internet habilitando a millones de computadoras para que se comuniquen globalmente. Originalmente, TCP/IP fue incluido con el Berkeley Software Distribution de UNIX para conectar hosts UNIX que fueron remotos de cada unos de ellos, como lo muestra la figura 3.1

FIGURA 3.1



A mediados de la década de los 70s, DARPA estableció una red de *paquetes switcheados*[24] para proveer comunicación entre las instituciones de investigación de los Estados Unidos. DARPA y otras organizaciones de gobierno entendieron el potencial de la tecnología de *paquetes switcheados* y era el principio justo para hacer frente al problema que virtualmente ahora tiene las compañías: la manera en la que se pueda establecer comunicación entre diferentes sistemas. Las redes de *paquetes switcheados* habilitan a las compañías a conectarse a la nube de Interred para conseguir información de un nodo a otro sin una conexión directa o un enlace entre los sitios.

[24] Un método de comunicación en el cual los paquetes de longitud variable son ruteados individualmente entre hosts.

ESTA TESIS NO SALE
DE LA BIBLIOTECA

3.1 CAPAS DEL PROTOCOLO TCP/IP

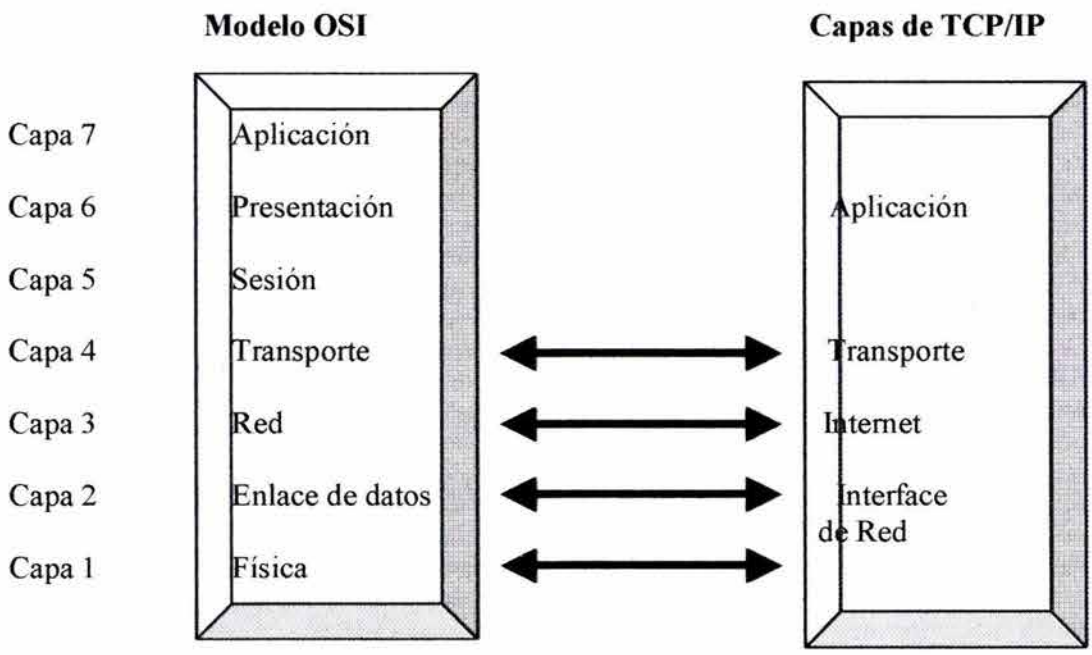
Los protocolos de Internet TCP/IP pueden ser utilizados para comunicarse a través de un conjunto de redes interconectadas. El conjunto de protocolos de Internet TCP/IP incluye no sólo especificaciones de capa 3 y 4 (tal como IP y TCP), sino también especificaciones para aplicaciones comunes tales como e-mail, acceso remoto y transferencia de archivos.

El modelo del protocolo TCP/IP mapea de cerca al modelo OSI en las capas inferiores. Todos los protocolos físicos y de enlace de datos estándares son soportados. El modelo TCP/IP consiste sólo de 4 capas:

- Capa de Aplicación: Define la funcionalidad de las capas superiores incluidas las capas de presentación y sesión del modelo OSI. Esta capa incluye soporte para un componente de comunicación de una aplicación, formato de código y conversión y establecimiento y mantenimiento de una sesión entre aplicaciones.
- Capa de Transporte: Define funcionalidad de transporte orientada a conexión y no orientada a conexión.
- Capa de Internet: Define la funcionalidad de interred para protocolos de ruteo.
- Capa de Interfaz de Red: Define las propiedades de estado de enlace y métodos de acceso al medio.

Las 4 capas del protocolo TCP/IP se muestra en la figura 3.2.

FIGURA 3.2

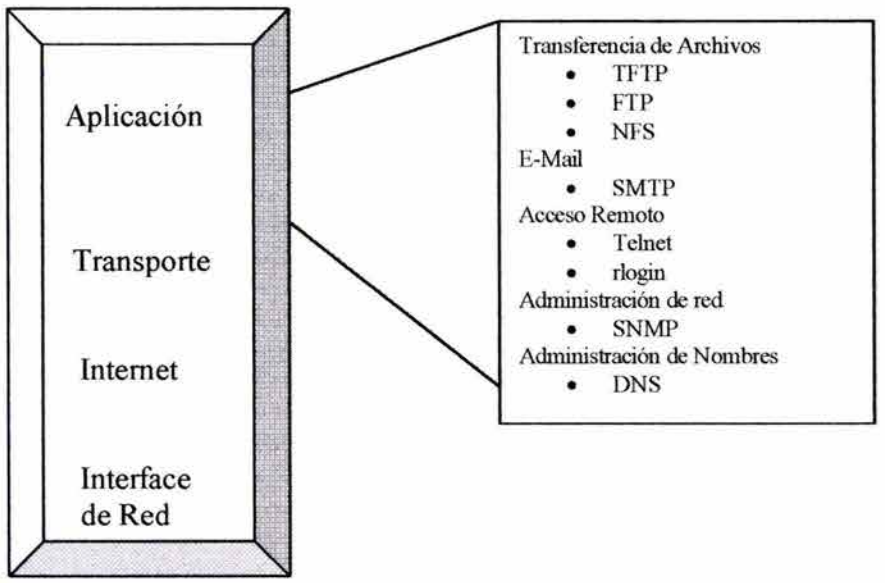


Un mensaje puede ser transferido en una secuencia de datagramas los cuales son reensamblados en el sitio de recepción. El término *paquete* y *datagrama* están muy cerca de ser intercambiables. Sin embargo, un *datagrama* es una unidad de dato, mientras que un *paquete* es una entidad física que aparece en una red. En la mayoría de los casos un paquete contiene datagramas.

3.2 DESCRIPCION DE CAPA DE APLICACIÓN

Los protocolos de aplicación existen para transferencia de archivos, acceso remoto, e-mail y administración de nombres. La administración de red también es soportada por al capa de aplicaciones como muestra la figura 3.3.

FIGURA 3.3



Algunas de esas aplicaciones pueden residir en el ruteador o en un dispositivo de host. Por ejemplo, TFTP y Telnet son aplicaciones que pueden ser usadas para accesar y configurar un ruteador. Si un ruteador soporta SNMP, el ruteador puede ser administrado por otros dispositivos SNMP con suficientes permisos. Finalmente habilita al ruteador para responder solicitudes de DNS.

3.3 DESCRPCION DE CAPA DE TRANSPORTE

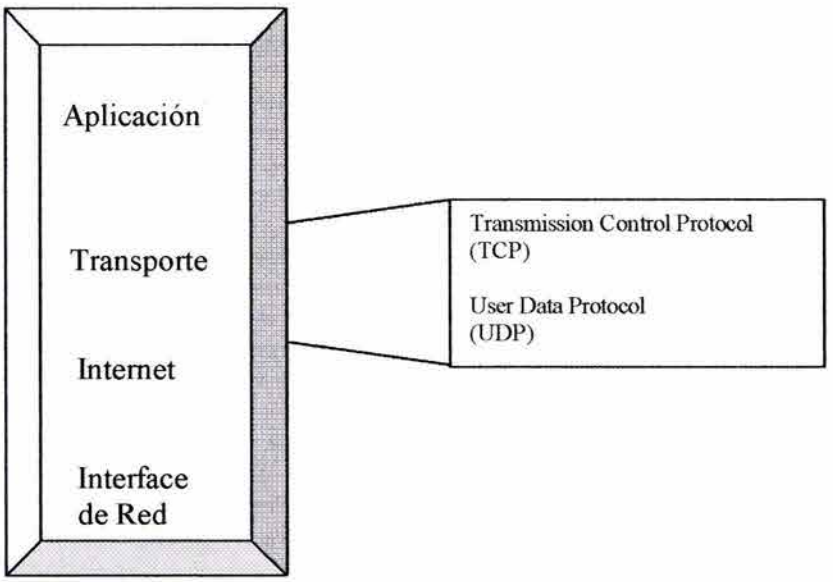
La capa de transporte desempeña varias funciones:

- Flujo de control provisto por ventanas deslizantes.
- Confiabilidad provista por secuencia de número y reconocimientos.

Dos protocolos son provistos en la capa de transporte: TCP y UDP (ver figura 3.4):

- TCP es un protocolo orientado a conexión. Es el responsable de cortar los mensajes en segmentos y reensamblarlos en la estación destino, reenviar algo que no fue recibido.
- UDP es un protocolo no orientado a conexión. Como se han eliminado todos los mecanismos de reconocimiento, UDP es rápido y eficiente. UDP no divide los datos en piezas.

FIGURA 3.4



Típicamente, las conexiones TCP son lentas para establecerse pero garantizan entrega de la información. UDP; por otro lado, no garantiza la entrega de la información. Si los paquetes son perdidos en una comunicación UDP, las capas superiores deben tener temporizadores en lugar de reintentar la temporización.

3.3.1 FORMATO DE SEGMENTO TCP

La figura 3.5 muestra el formato de un segmento TCP

FIGURA 3.5

#Bits 16	16	32	32	4	6	6
Source Port	Dest. Port	Sequence Number	Acknowledgement Number	HLEN	Reserved	Code Bits

ESTA TESIS NO SALE DE LA BIBLIOTECA

#Bits 16	16	16	0 to 32	
Window	Check sum	Urgent	Option	Data

Las definiciones en los campos en el segmento TCP incluyen lo siguiente:

- Source Port: Numero de puerto fuente.
- Destination Port: Numero de puerto destino.
- Sequence Number: Posición en la secuencia del byte de la fuente del dato en el segmento usado para establecer confiabilidad.
- Acknowledgement Number: El próximo octeto TCP esperado, utilizado para establecer confiabilidad.
- HLEN: Numero de palabras de 32 bits en el encabezado. Indica en dónde empeza el dato.
- Reserved: Fijo en cero.
- Code bits: Funciones de control (tales como SYN, para comienzo y FIN para termanción de una sesión).
- Cheksum: Calcula el checksum del encabezado y campo de datos, verifica que el datagrama llegue intacto.
- Urgent Pointer: Indica el final de un dato urgente.
- Option: Tamaño máximo del segmento TCP.
- Data: Dato de protocolo de capas superiores.

3.3.2 NÚMEROS DE PUERTO

TCP y UDP utilizan números de puerto o *sockets* para pasar información de capas superiores. Los números de puertos son usados para no perder de vista diferentes conversaciones a través de la red al mismo tiempo.

Las conversaciones que no involucran una aplicación con un número de puerto conocido son asignadas a números de puertos aleatorios elegidos de un rango específico. Esos números de segmento son usados como direcciones fuente y destino del segmento TCP.

Algunos puertos son reservados en TCP y UDP pero algunas aplicaciones no lo soportan. Los números de puertos tienen asignados los siguientes rangos:

- Números debajo de 256 para aplicaciones públicas.
- Números desde 256 a 1023 son asignados a compañias para aplicaciones vendibles.
- Números sobre 1023 son asignados dinámicamente por el host de aplicaciones.

En número de puerto TCP combinado con otra información es lo que los desarrolladores de UNIX llaman *Socket*.

3.4 DESCRIPCION DE CAPA DE INTERNET

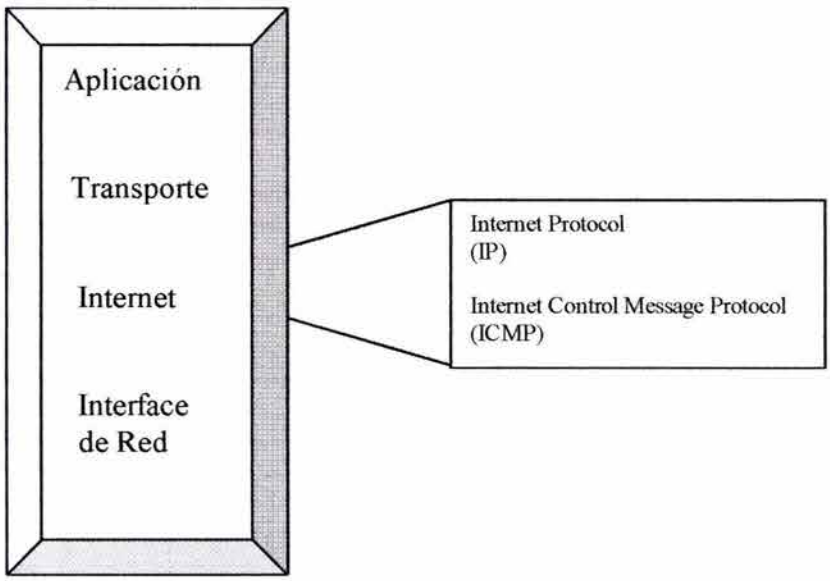
La capa de Internet corresponde a la capa de red del modelo OSI. Cada capa es responsable de obtener paquetes por una red utilizando direccionamiento de software.

Como muestra la figura 3.6, dos protocolos operan en la capa de Internet, los cuales corresponden a la capa de red del modelo OSI:

- IP, el cual es un protocolo no orientado a conexión. Este no ve el contenido de los datagramas, en lugar de eso, busca el camino para enviar el datagrama al destino.
- Internet Control Message Protocol (ICMP), el cual provee control y capacidades de mensajes.

Hay que notar que los protocolos de ruteo son considerados como protocolos de capa de administración que soporta la capa de red.

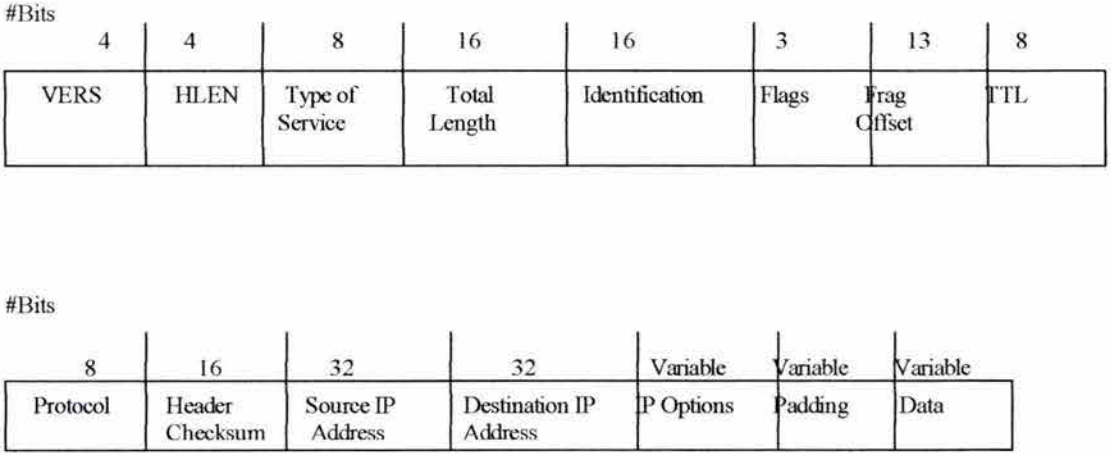
FIGURA 3.6



3.4.1 DATAGRAMA IP

La figura 3.7 muestra el formato de un datagrama IP. Los datagramas IP contienen un encabezado IP y un dato y son rodedados por el encabezado de capa MAC.

FIGURA 3.7



Las definiciones de los campos en este datagrama IP son:

- VERS: Numero de versión, la actual versión es IP versión 4; la próxima generación de IP (llamada IPv6) es IP versión 6[25].
- HLEN: Encabezado de palabras de 32 bits; indica dónde empieza el encabezado de transporte.
- Type of Service: La manera en que el datagrama debe ser manejado; especifica la confiabilidad, procedencia, retardo y parámetros de rango de transferencias.
- Total Length: El largo total, incluye encabezado y dato.
- Identification, Flags, Flag Offset: Provee fragmentación y reensamble de datagramas que permiten diferentes tamaños de frame en la red.
- TTL (Time To Live): Cada estación debe decrementar este número por uno o por el número de segundos que se manejan en el paquete. Cuando el contador alcanza cero, el TTL expira y el paquete es desechado.
- Protocol: Identifica el protocolo de capas superiores (capa 4) que debe recibir el datagrama. Aunque la mayoría del tráfico IP usa TCP, hay otros protocolos que pueden usar IP.
- Header Checksum: Checa la integridad del encabezado.
- Source and Destination IP Address: Direcciones IP de 32 bits que identifica el dispositivo fuente y final involucrado en la comunicación.
- IP Options: Pruebas de red, Debugging, seguridad y otros.

[25] Incluye soporte para flujo ID en el encabezado de paquete, el cual puede ser usado para identificar los flujos de información.

3.4.2 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

El ICMP es implementado por todos los hosts TCP/IP. Los mensajes ICMP son cargados en el datagrama IP y usa innumerables tipos de mensajes definidos. La siguiente lista muestra algunos de los más comunes y útiles tipos de mensajes de ICMP:

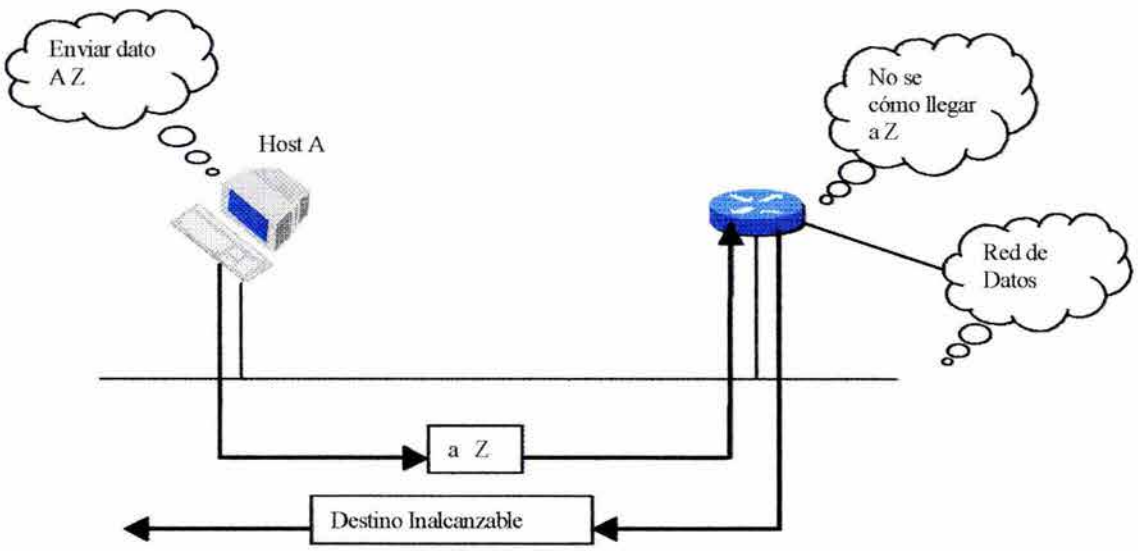
- Destination Unreachable: Reporta destino inalcanzable.
- Parameter Problem: Estructura de paquete IP defectuosa.
- Source Quench: Control de flujo.
- Redirect: Cambio de ruta.
- Echo: Prueba de confiabilidad.
- Echo Reply: Prueba de confiabilidad.
- Information Request: Obtiene una direccion de red.
- Information Reply: Obtiene una dirección de red.
- Address Mask Request: Obtiene una máscara de subred.

3.4.3 PROBANDO ICMP

Si un ruteador recibe un paquete que este es incapaz de entregar al último destino, el ruteador envía un mensaje de que el destino es inalcanzable a la fuente como muestra la figura 3.8. Este mensaje puede ser no entregado porque no hay ruta conocida al destino.

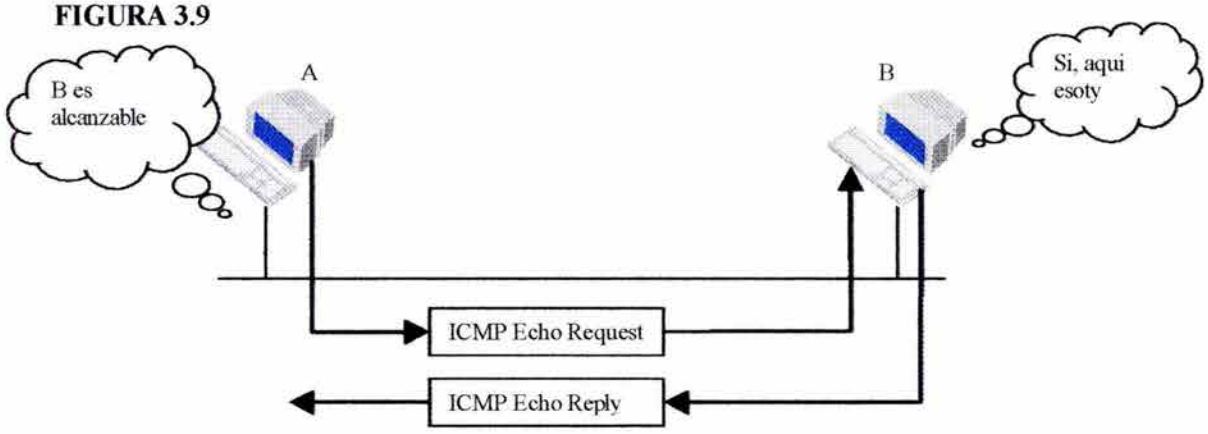
ICMP es más simple que UDP. ICMP utiliza números de puerto en su encabezado porque todos los mensajes de red son interpretados por el software de la red misma; por lo tanto, los números de puerto no son necesitados para determinar el destino de un mensaje.

FIGURA 3.8



Un *Echo Replay* es una respuesta exitosa del comando *PING*; sin embargo, los mensajes ICMP, tales como Inalcanzables o Timeouts indican que la solicitud *PING* no pudo alcanzar el destino. La figura 3.9 muestra el host A enviando un *Echo Request* al host B. Despés de recibir el host B el *Echo Request* este envía un *Echo Replay*.

FIGURA 3.9

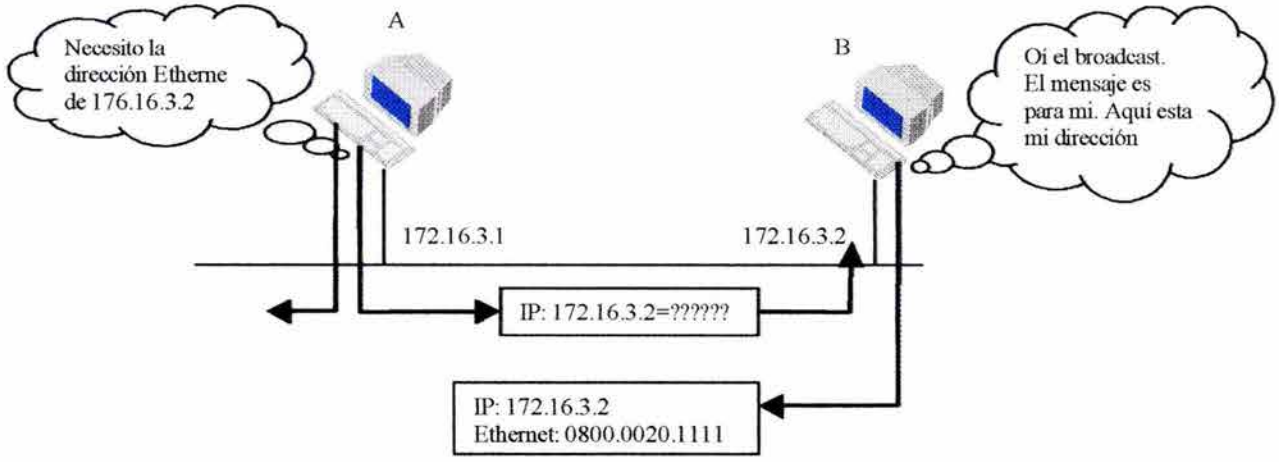


Otro comando que utiliza ICMP es el comando *Traceroute*. *Traceroute* provee una lista de los ruteadores a lo largo de la ruta entre dos dispositivos.

3.4.4 ADDRESS RESOLUTION PROTOCOL

Address Resolution Protocol (ARP) es utilizado para resolver o mapear una dirección IP a una dirección MAC para permitir la comunicación en un medio multiacceso como lo es Ethernet. Para determinar una dirección destino para un datagrama, la tabla ARP cache es revisada. Si la dirección no está en la tabla, ARP envía un broadcast para localizar la estación destino, como en la figura 3.10.

FIGURA 3.10



El término *Local ARP* se refiere a la resolución de una dirección cuando el host solicitador y el host destino comparten el mismo medio. En el caso de un paquete destinado a un dispositivo de otra red, el host local hará un ARP sólo para la dirección MAC del ruteador local.

3.4.5 REVERSE ARP

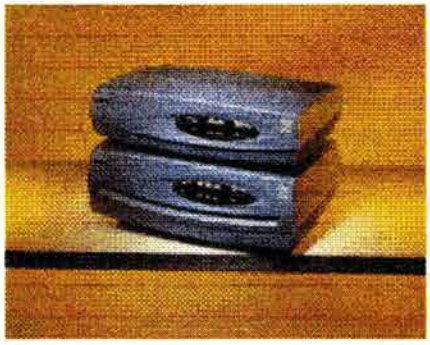
Reverse ARP (RARP) es utilizado para obtener una dirección IP utilizando un broadcast RARP. RARP confia en la presencia de un servidor RARP con una tabla que contiene información usada para responder esas solicitudes.

CAPITULO 4

RUTEADORES COMERCIALES

En esta sección se describen las características más importantes de los ruteadores más vendidos para soluciones de pequeñas y medianas empresas.

4.1 CISCO 1700 SERIES



La serie Cisco 1700 de ruteadores de acceso modulares son diseñados para proveer de una plataforma de voz, datos y video para pequeñas y mediana empresas, pequeños corporativos y sucursales. Estos ruteadores ofrecen acceso a red de alta velocidad, cracteristicas de seguridad y plataforma multiservicios. El ruteador de acceso Cisco 1710 trabaja con modems de banda ancha existentes para proveer de un ruteo avanzado y seguridad. El ruteador de acceso modular Cisco 1720 provee de acceso a datos de alto desempeño.
El ruteador de acceso modular Cisco 1751 optimiza el tráfico de voz y datos.

4.1.1 CARACTERISTICAS CLAVES

- Soporta cuatro interfaces seriales o dos ISDN BRI; una conexión LAN Fast Ethernet (10/100Mbps); un puerto Auxiliar (AUX) para conexiones de Dial-up o conexiones asíncronas de baja velocidad (arriba de 112.5 kbps).
- Flexibilidad: la serie 1700 soporta un conjunto de tarjetas WAN y tarjetas de voz que son compartidas con la serie 1600 (sólo WAN), 2600 y 3600.
- Dispositivo integrado: La serie Cisco 1700 combina ruteo WAN, VPN[26] y acceso multiservicio en un simple dispositivo.
- Slots de expansión: Soporta un módulo opcional VPN para encriptación IPSec 3DES (módulo VPN estándar en ruteador Cisco 1710).
- Seguridad Integrada: La serie 1700 soporta control de acceso por filtrado de firewall dinámico, detección de negación de servicios y prevención, bloqueo de Java, Intrusión Detection System (IDS) y encriptación.
- Soporte a VLAN (sólo Cisco1710 y 1751).

[26] VPN (Virtual Private Network). Una red que habilita tráfico IP para viajar con seguridad sobre una red pública TCP/IP por encriptación.

4.2 CISCO 2500 SERIES

La serie Cisco 2500 de ruteadores, la serie más popular del mundo para oficinas sucursales, provee una gran variedad de modelos para satisfacer un amplio rango de necesidades de red. Estos ruteadores tienen configuraciones fijas con al menos dos de las siguientes interfaces: Ethernet, Token Ring, Serial síncrono, Serial Asíncrono, ISDN BRI y puertos de concentrador 10BaseT.
Dos modelos modulares también están disponibles.

4.2.1 CARACTERISTICAS CLAVE

- Proveen una tecnología con un amplio conjunto de Cisco IOS Software.
- Ruteadores configurables con Cisco Configmaker, una herramienta de configuración fácil de utilizar.
- Con CiscoWorks se permite la instalación remota y mantenimiento desde una locación.

4.2.2 ESPECIFICACIONES

SERIE CISCO 2500 (TODOS LOS MODELOS)

CARACTERISTICA	ESPACIFICACION
Velocidad de procesador (Tipo)	20Mhz (68030)
Memoria Flash	Banco dual de 8MB (default) 16MB (max)
Memoria DRAM	4 MB actualizable a 8 o 16MB
Fuente de Poder	AC, con DC opcoonal o RSP

SERIE CISCO 2500 (RUTEADORES LAN SIMPLES)

CARACTERISTICA	CISCO 2501	CISCO 2502	CISCO 2503	CISCO 2504
Puertos LAN Fijos	1 Puerto Ethernet	1 Puerto Token Ring	1 Puerto Ethernet	1 Puerto Token Ring
Puerto WAN Fijos	2 Puertos Seriales Sincronos	2 Puertos Seriales Sincronos	2 Puertos Seriales Sincronos 1 Puerto ISDN PRI (S/T)	2 Puertos Seriales Sincronos 1 Puerto ISDN BRI (S/T)
Slots	No	No	No	No

SERIE CISCO 2500 (COMBINACIONES RUTEADOR/CONCENTRADOR)

CARACTERISTICA	CISCO 2505	CISCO 2507	CISCO 2516
Puertos LAN Fijos	8 Puertos Ethernet	16 Puertos Ethernet	14 Puertos Ethernet
Puerto WAN Fijos	2 Puertos Seriales Sincronos	2 Puertos Seriales Sincronos	2 Puertos Seriales Sincronos 1 Puerto ISDN BRI (S/T)
Slots	No	No	No

SERIE CISCO 2500 (SERVIDORES DE ACCESO)

CARACTERISTICA	CISCO 2509	AS 2509-RJ	CISCO 2511	AS 2511-RJ	CISCO 2512
Puertos LAN Fijos	1 Puerto Ethernet	1 Puerto Ethernet	1 Puerto Ethernet	1 Puerto Ethernet	1 Puerto Token Ring
PuertoS WAN Fijos	2 Puertos Seriales Sincronos 8 Puertos Seriales Asincronos	1 Puertos Seriales Sincronos 8 Puertos Seriales Asincronos	2 Puertos Seriales Sincronos 16 Puertos Seriales Asincronos	1 Puertos Seriales Sincronos 16 Puertos Seriales Asincronos	2 Puertos Seriales Sincronos 16 Puertos Seriales Asincronos
Slots	No	No	No	No	No

SERIE CISCO 2500 (RUTEADORES DE ALTA DENSIDAD)

CARACTERISTICA	CISCO 2520	CISCO 2521	CISCO 2522	CISCO 2523
Puertos LAN Fijos	1 Puerto Ethernet	1 Puerto Token Ring	1 Puerto Ethernet	1 Puerto Token Ring
Puertos WAN Fijos	2 Puertos Seriales Sincronos de Alta Velocidad 1 Puerto ISDN BRI (S/T) 2 Puertos Seriales Sinc/Asinc de baja velocidad	Lo mismo que Cisco 2520	2 Puertos Seriales Sincronos 1 Puerto ISDN BRI (S/T) 8Puertos Seriales Sinc/Asinc	Lo mismo que Cisco 2522
Slots	No	No	No	No

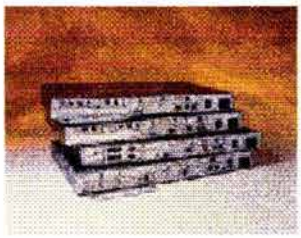
SERIE CISCO 2500 (RUTEADORES LAN DUALES)

CARACTERISTICA	CISCO 2513	CISCO 2514	CISCO 2515
Puertos LAN Fijos	1 Puerto Ethernet 1 Puerto Token Ring	2 Puertos Ethernet	2 Puertos Token Ring
Puertos WAN Fijos	2 Puertos Serial Sincrono	2 Puertos Serial Sincrono	2 Puertos Serial Sincrono
Slots	No	No	No

SERIE CISCO 2500 (RUTEADORES LAN SIMPLES, CONFIGURACION MODULAR)

CARACTERISTICA	CISCO 2524	CISCO 2525
Puertos LAN Fijos	1 Puerto Ethernet	1 Puerto Token Ring
Puertos WAN Fijos	No	No
Modulos LAN	No	No
Modulos WAN	1 Puerto ISDN BRI (S/T) 1 Puerto ISDN BRI (U) 1 Puerto CSU/DSU T1/T1 Fraccional 1 Puerto Serial Sincrono	Lo mismo que el Cisco 2524

4.3 CISCO 2600 SERIES



Cisco Systems extiende la versatilidad, la integración y el poder a las oficinas sucursales con la serie Cisco 2600.

La arquitectura modular de la serie Cisco 2600 provee la versatilidad necesaria para adaptarse a los cambios de tecnología de red tales como nuevos servicios y aplicaciones que llegan a estar disponibles. Utilizando un poderoso procesador RISC la serie Cisco 2600 soporta calidad de servicio (QoS) avanzada, seguridad y características de integración requeridas hoy en día. Por la integración de funciones de dispositivos separados en una simple unidad, los ruteadores de la serie Cisco 2600 reduce la complejidad de la administración de redes remotas. La serie Cisco 2600 comparte las interfaces modulares con los ruteadores de las series Cisco 1600, 1700 y 3600, ofreciendo un solución de costo-efectivo, tales como acceso Internet/Intranet, integración de servicio voz/datos, acceso VPN, VLAN y administración de ancho de banda.

4.3.1 CARACTERISTICAS CLAVE

- Protección de Inversión/Versatilidad. Las interfaces modulares permiten habilitar miles de soluciones y facil migración a futuros requerimientos de red.
- Integración/Flexibilidad. Bajos costos de propiedad y mejora de la administración remota, proporcionado redes integradas que combinan CSU/DSU, multiplexores, modems, gateways de voz/datos, Firewalls, VPN, encriptación y dispositivos de compresión.
- Redes Multiservicio (Voz/Datos). Reduce los costos de teléfonos/fax entre oficinas. El tráfico de voz es encapsulado y digitalizado en paquete Frame Relay o en paquetes IP, consolidando el tráfico de datos.

4.3.2 ESPECIFICACIONES

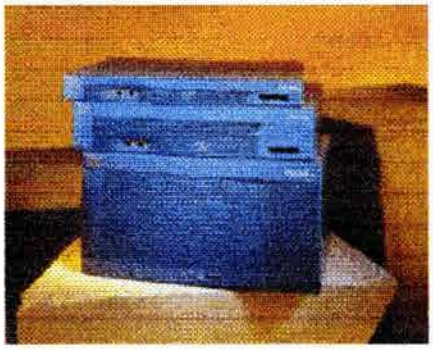
CARACT.	CISCO 2610	CISCO 2611	CISCO 2612	CISCO 2613	CISCO 2620	CISCO 2621
Puertos LAN Fijos	1Pto.Ethernet	2Ptos. Ethernet				
Puertos WAN Fijos	Puerto AUX	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Slots NM[27]	1	1	1	1	1	1
Slots Interfaz WAN	2	2	2	2	2	2
Advance Integration Slots (AIM)	1	1	1	1	1	1
Tarjeta de interfaz WAN	1 Pto. ISDN BRI (S/T) 1 Pto. ISDN BRI (U) 1 Pto. T1/T1 Fraccional 1 y 2 Ptos. Seriales Sinc. Alta velocidad 2 Ptos. Seriales Sinc./Asinc. De baja velocidad	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Tarjetas de voz Multiflex	1 y 2 Ptos. T1/T1 Fracc. con DSU/CSU 1 Pto. E1 30 Canales de voz	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610

[27] NM = Network Module

	1 Pto. 60 canales de voz					
Modulos de Voz/Fax	1 o 2 Slots de voz 1 Pto. T1 24 Canales de voz 2 Ptos. T1 48 canales de voz 1 Ptos. E1 30 Canales de voz 1 Ptos. E1 60 canales de voz	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Tarjetas de voz	2 Ptos. de voz-FXS 2 Ptos. de voz E&M 2 Ptos. de voz FXO 2 Ptos de voz BRI	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Modulos LAN	1 - 4 Ptos. Ethernet 10BaseT	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Modulos WAN	4-8 Ptos. BRI (S/T) 4-8Ptos. BRI (U) 4-8 Ptos. Seriales Asin/Sin 16 y 32 Ptos. Seriales Asinc. 1 y 2 Ptos. T1/PRI 1 y 2 Ptos. E1/PRI Balanceado 1y 2 Ptos. E1/PRI No balanceado	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Modulos ATM	1 Pto. ATM-25 1 y 8 Ptos. T1 ATM IMA con CSU/DSU 1 y 8 Ptos. E1 ATM IMA	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Modulos de modem	8 y 16 Ptos. analogicos	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Modulos AIM	Data Compression	Lo mismo	Lo mismo 2610	Lo mismo	Lo mismo 2610	Lo mismo

	AIM (8Mbps)	2610		2610		2610
Velocidad de Procesador	40Mhz (RISC)	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	50Mhz (RISC)	50Mhz (RISC)
Memoria Flash	8MB (Default) 16MB (Max)	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610
Memoria DRAM	24MB(Default) 64 (Max)	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610	Lo mismo 2610

4.4 CISCO 3600 SERIES



La serie Cisco 3600 es una familia de plataformas de acceso modular y multifuncional para empresas pequeñas y medianas y proveedores de servicios de Internet. Con cerca de 70 opciones de interfaces modulares, la familia Cisco 3600 provee integración de voz y datos, VPNs y ruteo de datos multi protocolo. Utilizando módulos de voz/fax, el Cisco 3600 permite a los clientes consolidar el tráfico de voz, fax y datos en una sola red. El alto desempeño y la arquitectura modular protegen la inversión del cliente en una tecnología de red e integra las funciones de varios dispositivos en una sola solución administrable.

4.4.1 CARACTERISTICAS CLAVE

- Combina acceso Dial-in, servicios de ruteo avanzados de LAN TO LAN, conectividad ATM e integración multiservicio de voz, datos y video en una sola plataforma.
- Un diseño modular y escalable proporciona desempeño, escalabilidad, flexibilidad y proteccion de inversión.
- Disponibilidad de paquetes de modems PRI y BRI preconfigurados.
- Cisco IOS Software intergrado.

4.4.2 ESPECIFIACIONES

CARACT.	CISCO 3620	CISCO 3640	CISCO 3660
Puertos Fijos	No	No	1 o 2 Ptos. 10/100

Slots NM	2	4	6
Slots AIM	No	No	2
Modulos LAN/Combo	1 y 4 Ptos. 10BaseT 1 y 2 Ptos. 10BaseT, 2 Slosts WIC 1 Pto. 10BaseT, 1 Ptos. Token Ring, 2 Slots WIC 1 Pto. 100BaseFX 1 Pto. 10/100bTX, 1 Pto. Ch T1/ISDN PRI 1 Pto. 10/100bTX, 2 Pto. Ch T1/ISDN PRI 1 Pto. 10/100bTX, 1 Pto. Ch T1/ISDN PRI con CSU 1 Pto. 10/100BbTX, 2 Ptos. Ch T1/ISDN PRI con CSU 1 Pto. 10/100bTX, 1 Ptos. Ch E1/PRI No Balanceado 1 Pto. 10/100bTX, 2 Ptos. Ch E1/PRI No Balanceado 1 Pto. 10/100bTX, 1 Ptos. Ch E1/PRI Balanceado 1 Pto. 10/100bTX, 2 Ptos. Ch E1/PRI Balanceado 1 Pto. 10/100 Ethernet, 2 Slots WIC 2 Ptos. 10/100 Ethernet, 2 Slots WIC 1 Pto. 10/100 Ethernet,1 Ptos. Token Ring, 2 Slots WIC 2 Slots WIC	Lo mismo 3620	Lo mismo 3620
Modulos WAN	4 y 8 Ptos. BRI (S/T) 4 y 8 Ptos. BRI (U) con NT-1 4 Ptos. Seriales 4 y 8 Ptos. Seriales Asin/Sin 16 y 32 Ptos. Asincronos 1 y 2 Ptos. Ch T1/ISDN-PRI 1 y 2 Ptos. Ch T1/ISDN-PRI con CSU 1 Pto. Compresión HSSI	Lo mismo 3620	Lo mismo 3620
Modulos ATM	1 Pto. 25Mbps ATM 1 Pto. OC3 155Mbps ATM 4 y 8 Ptos. T1 ATM	Lo mismo 3620	Lo mismo 3620
Modulo de red Voz/Fax	1 o 2 Slots Voz/Fax 1 Pto. T1 24 Canales de voz 2 Ptos. T1 48 Canales de voz	Lo mismo 3620	Lo mismo 3620

	1 Pto. E1 30 Canales de voz 2 Ptos. E1 60 Canales de voz		
Modulos WIC	1 Pto. ISDN BRI (S/T) 1 Pto. ISDN BRI (U) 1 Pto. Sincrono Serial 1 Pto. CSU/DSU 56kbps 1 Pto. T1/FT1 CSU/DSU	Lo mismo 3620	Lo mismo 3620
Tarjetas de Interfaz Voz/WAN Multiflex	1 Pto. RJ-48 Troncal Multiflex-T1 2 Ptos. RJ-48 Troncal Multiflex T1 1 Pto. RJ-48 Troncal Multiflex-E1 2 Ptos. RJ-48 Troncal Multiflex E1	Lo mismo 3620	Lo mismo 3620
Modulos VIC	2 Ptos. de voz-FXS 2 Ptos. de voz E&M 2 Ptos. de voz FXO 2 Ptos de voz BRI	Lo mismo 3620	Lo mismo 3620
Modulos Modem	6, 12, 18, 24, 30 Ptos. de modem digital 8 o 16 Ptos. de modem anlogico	Lo mismo 3620	Lo mismo 3620
Velocidad de Procesador (tipo)	80Mhz (IDT R4700 RISC)	100Mhz (IDT R4700 RISC)	55Mhz (QED RM5271 RISC)
Memoria Flash	8MB (Default) 32MB (Max)	Lo mismo 3620	8MB (Default) 64MB (Max)
Memoria DRAM	32MB (Default) 64MB (Max)	32MB (default) 128MB (Max)	32MB (Default) 256MB (Max)

CAPITULO 5

TAREAS PRELIMINARES EN UN RUTEADOR

Este capítulo discute los principios básicos de arranque, modos de comando y comandos de estado de un ruteador. Se podrá desarrollar un modelo de ruteador basado en componentes que son configurables.

5.1 INICIALIZANDO UN RUTEADOR

Esta sección cubre los componentes del ruteador que juegan un papel en el proceso de configuración. Examina las rutinas de inicialización de un ruteador. Conocer los componentes que son involucrados en el proceso de configuración provee de una mejor comprensión de la manera en que el ruteador almacena y utiliza sus comandos de configuración.

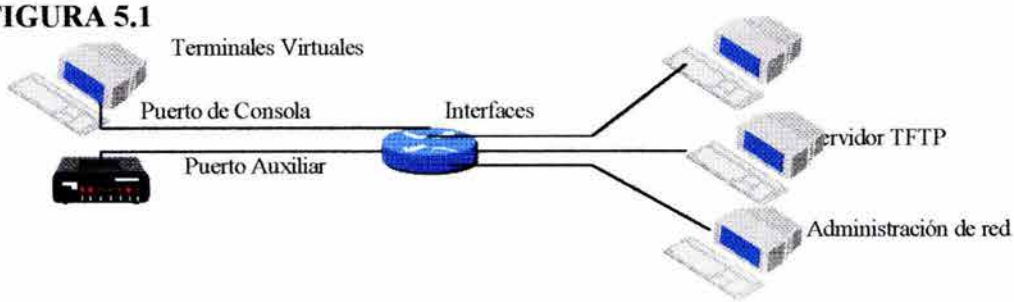
5.1.1 FUENTES DE CONFIGURACION EXTERNAS

El ruteador puede ser configurado desde varias locaciones como se muestra en la figura 5.1.

- Puerto de consola: Sobre la instalación inicial, se puede configurar el ruteador desde una terminal de consola, la cual es conectada al ruteador por un puerto serial.
- Puerto Auxiliar: También se puede configurar un ruteador desde el puerto auxiliar.
- Terminales virtuales: Se puede configurar un ruteador desde terminales virtuales después que el ruteador es conectado en la red.
- TFTP[28] Server: También se puede hacer una descarga de la configuración desde un servidor TFTP en la red. Un servidor TFTP puede ser una estacion UNIX o un PC que actúe como deposito de archivos. Se pueden mantener los archivos de configuración en un servidor TFTP y después hacer la descarga al ruteador.
- Estación de Administración de red: Se puede configurar un ruteador desde un sistema remoto corriendo un software de Administración de red.

[28] Trivial File Transfer Protocol: Protocolo de transferencia de arcHivos muy sencillo que carece de seguridad. TFTP ejecuta las mismas tareas que el FTP pero usa un protocolo de transporte diferente.

FIGURA 5.1



Para enviar y recibir información de configuración de una terminal virtual, un servidor TFTP o una estación de administración, el ruteador debe ser configurado para soportar tráfico IP.

5.1.2 COMPONENTES INTERNOS DE CONFIGURACIÓN

La arquitectura del ruteador soporta componentes que juegan un papel muy importante en el proceso de inicialización:

- RAM/DRAM (Random Access Memory/Dynamic Random Access Memory): Es el componente de almacenamiento temporal del ruteador. RAM también es llamada *Working Storage* y contiene información dinámica de la configuración.
- NVRAM (Non-volatile RAM): Contiene una copia de respaldo de la configuración. Si el ruteador es apagado por un periodo de tiempo, la copia de respaldo de la configuración habilita al ruteador para volver a operar sin necesidad de ser reconfigurado.
- Memoria Flash: La memoria es una clase especial de memoria borrable y programable de sólo lectura. Esta memoria contiene una copia del IOS (Interworking Operative System)[29].
  La memoria flash tiene una estructura que habilita el almacenamiento de múltiples copia de IOS permitiendo cargar un nuevo nivel de sistema operativo en cada ruteador en la red y entonces, en cierto tiempo conveniente, actualizar toda la red a ese nuevo nivel.
- ROM: Contiene un programa de inicialización *Bootstrap* y un sistema pequeño de monitoreo que puede ser usado para recuperación en alguna catástrofe.
- Interfaces: Son conexiones de red a través de las cuales los paquetes entran y salen del ruteador. Las interfaces soportadas están disponibles para Token Ring, Ethernet, Fast Ethernet, Gigabit Ethernet. Adicionalmente hay soporte para ISDN BRI[30], ATM y otras conexiones fisicas.
- Puertos auxiliares: El IOS permite al puerto auxiliar ser usado en ruteo asíncrono como interfaz de red.

---

[29] Sistema Operativo de red del ruteador.

[30] El ISDN BRI *Basic Rate Interface* ofrece dos canales *B* y un canal *D (2B+D)*. El canal *B* opera a 64Kbps y lleva datos del usuario; el canal *D* opera a 16 Kbps y lleva informacion de control y señalización.

5.1.3 DESCRIPCION DEL SISTEMA DE INICIALIZACION

Las rutinas de inicialización para el IOS software tienen el objetivo de empezar las operaciones del ruteador.
Para tener éxito, las rutinas de inicialización deben desempeñar tres tareas:

- Revisa el hardware y revisa un POST (Power on self test).
- Encontrar y cargar la imagen del IOS Software. La imagen es el dato que el ruteador utiliza para su sistema operativo.
- Encontrar y aplicar la información de la configuración del ruteador. Esta información incluye declaraciones acerca de los atributos específicos del ruteador, funciones de protocolo y direcciones de interfaces.

Primero el ruteador debe estar seguro que el hardware fue aprobado. Durante el POST, el ruteador ejecuta diagnósticos desde la ROM a todos los módulos. Esos diagnósticos verifican la operación básica del CPU, memoria y circuitos de interfaz.

Después de verificar las funciones del hardware, el ruteador procede con la inicialización del software. Algunas rutinas de inicialización actúan como operadores de retraso que son capaces de realizar la inicialización del ruteador debido a otras rutinas que no son capaces de hacerlo.

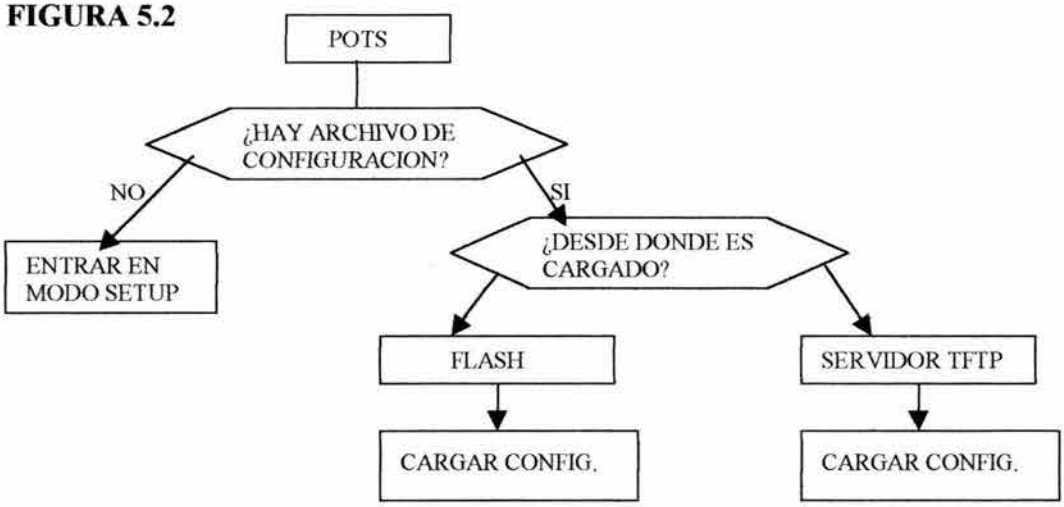
Lo siguiente en el proceso de inicialización, el ruteador busca su registro de configuración para determinar donde encuentra el IOS software. Si el ruteador no encuentra la imagen de su sistema válida o si la secuencia de inicialización fue interreumpida, el sistema entrará en el *Modo ROM Monitor* cada vez que el ruteador se enciende. Desde el modo ROM monitor también se puede inicializar el dispositivo o realizar pruebas de diagnóstico.

Después de que el IOS software ha sido cargado, el ruteador procurará cargar el archivo de configuración, si existe. Este archivo contiene toda la información de configuración básica que se especificó para un ruteador en particular. El archivo de configuración es almacenado en NVRAM; sin embargo, se puede configurar el ruteador para cargar el archivo de configuración de un servidor TFTP.

Si el archivo de configuración no existe, el ruteador invertirá para el *modo Setup*. El *modo Setup* es un diálogo interactivo que permite crear una configuración básica para el ruteador. Si el ruteador está configurado para cargar el software desde un servidor TFTP y el servidor no puede ser encontrado, el ruteador utiliza el archivo de configuración existente en NVRAM. Si el servidor TFTP está disponible, el ruteador cargará el archivo de configuración suplente almacenado en el servidor TFTP.

La figura 5.2 muestra la secuencia de inizializacion de un ruteador.

FIGURA 5.2



Un ruteador puede inicializar desde la ROM, Flash o del servidor TFTP. Después de que el ruteador ha completado el proceso de inicialización, empieza con las operaciones. En este punto se pueden construir nuevos parámetros de configuración o parámetros existentes. En cualquier caso, se puede acceder el ruteador con los comandos de interfaz de usuario.

5.2 ACCESANDO LA INTERFAZ DE USUARIO

Esta sección cubre la manera en que se puede manipular el IOS software desde la consola del ruteador. La consola del ruteador puede ser una estación de trabajo corriendo un paquete de emulación de terminal, como el Hyperterm, o un dispositivo remoto corriendo Telnet. Ambos métodos dan acceso a la interfaz de usuario del IOS software para entrar a los comandos de usuario.

5.2.1 MODOS DE RUTEADOR

La interfaz de usuario de IOS software provee acceso a modos de comando:

- Modo EXEC usuario: Interpreta los comandos que se escribe y realiza las operaciones correspondientes. EXEC tiene dos niveles de acceso comando: Modos usuario y Modo provilegiado.
  Después de que se entra en el ruteador, automáticamente se está en el modo usuario. En general, en el modo EXEC usuario contiene comandos no destructivos que permiten la conexión con dispositivos remotos, cambiar los parámetros de terminal en una base temporal, realizar pruebas básicas. El modo EXEC usuario es indicado por el nombre del dispositivo seguido del símbolo (>).
- Modo EXEC privilegiado: Fija los parámetros de operación. Los comandos privilegiados incluyen esos comandos contenidos en el modo EXEC usuario, así como el comando *Configure* a través del cual se puede accesar a los modos de comando restantes. El modo EXEC privilegiado también incluye comandos de prueba de alto nivel, tal como *Debug*. Para entrar al modo EXEC privilegiado,

teclear *Enable* en el prompt de EXEC usuario. El prompt de mode EXEC privilegiado consiste en el nombre del dispositivo seguido del símbolo (#). El modo EXEC privilegiado contiene comandos no destrictuvos y pueden ser protegidos con passwords.

- Modo de ROM Monitor: Ocurre si el ruteador no encuentra una imagen de sistema válida o si se interrumpio el proceso de inicialización. Permite configurar el ruteador.
- Modo Setup: Este es un modo de prompt interactivo en la consola que ayuda a los nuevos usuarios a crear una configuración básica. Se puede entrar en el modo Setup tecleando *Setup* en el prompt del modo EXEC privilegiado.
- Modo RXBOOT: Este es un modo especial al que se puede entrar alterando los parámetros de registro de configuración y reinicializando el ruteador. El modo RXBOOT provee al ruteador de un subconjunto de IOS software y ayuda al iniciarse el ruteador cuando no encuentra una imagen de IOS válida en la memoria Flash. El prompt de modo RXBOOT es el nombre del host seguido de <boot>.
- Modo de configuración global: Los comandos de configuración global se aplican a características que afectan al sistema entero. Se puede entrar al modo de configuración global tecleando *Configure* en el prompt del modo EXEC privilegiado. El modo de configuración es indicado por el nombre del dispositivo (config) seguido del símbolo (#).

5.2.2 ENTRANDO EN EL RUTEADOR

El intérprete de comando EXEC espera un intervalo de tiempo para comenzar la entrada. Si una entrada no es tecleada, el EXEC pausa la conexión y se debe entrar al ruteador otra vez. El intervalo fijo para que el ruteador espere por una entrada son 10 minutos. El comando *no-exec timeout* remueve la definición timeout.

5.2.3 UTILIZANDO PASSWORDS

El IOS software soporta una gran variedad de características de seguridad para controlar los accesos al ruteador. Este acceso puede ser controlado por uno o más de los siguientes:

- Un password de línea de acceso
- Un password de modo EXEC priviliegiado.
- Passwords encriptados.

Los passwords son fijados durante la configuración inicial en el modo *Setup* o con el comando *Enable password*. Si un password no es fijado en el modo *Enable* puede sólo ser accesado desde la consola del ruteador.

5.2.4 PASSWORDS DE LINEA INDIVIDUAL

Se debe tener asegurado el acceso al ruteador por la protección de líneas individuales por un password. Este nivel de seguridad requiere que los usuarios verifiquen autorización antes de poder accesar a alguna línea, incluyendo la línea de consola.

5.2.5 PASSWORDS DE MODO EXEC PRIVILEGIADO

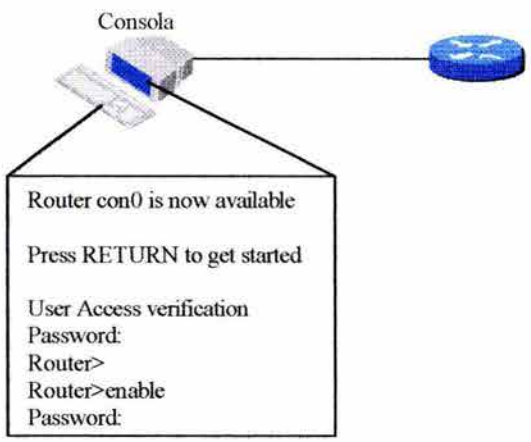
Se puede controlar el acceso de modo EXEC privilegiado asignando un password a este modo durante el Setup inicial del ruteador.

5.2.6 PASSWORD ENCRIPTADO

Cisco provee una característica que permite encriptar passwords. Si se utiliza esta característica, los passwords son almacenados en el ruteador en forma codificada y se enmascarán cuando se despliegan los parámetros de configuración del ruteador. Esta encriptación es habilitada usando el comando *Service-password ecryption.*

Se puede configura un ruteador para que haga una revision de usuario, como muestra la figura 5.3:

FIGURA 5.3



5.2.7 LISTA DE COMANDOS DE MODO USUARIO

Una vez que estemos en modo EXEC usuario se pueden desplegar todos los comandos disponibles tecleando el signo de interrogación (?) en el prompt de modo EXEC usuario como muestra la figura 5.4.

La pantalla despliega 22 líneas en un tiempo. El *–More–*al final del despliegue indica que múltiples pantallas son disponibles. Para desplegar las próximas líneas presionar *Return*. Presionar cualquier otra tecla para regresar al prompt de EXEC usuario.

FIGURA 5.4

```
Router>?
Exec commands:
access-enable     Create a temporary Access-list entry
atmsig            Execute Atm Signalling Commands
clear             Reset functions
cd                Change current device
connect           Open a terminal connection
dir               List files on given device
disable           Turn off privileged commands
disconnect        Disconnect an existing network connection
enable            Turn on privileged commands
--More--
```

5.2.8 LISTA DE COMANDOS DEL MODO PRIVILEGIADO

En el modo EXEC privilegiado también se pueden desplegar los comandos tecleando el signo de interrogación (?) en el prompt de modo EXEC privilegiado como muestra la figura 5.5.

FIGURA 5.5

```
Router#?
Exec commands:
access-enable     Create a temporary Access-list entry
access-template   Create a temporary Access-list entry
bfe               For manual emergency modes settings
clear             Reset functions
clock             Manage the system clock
configure         Enter configuration Mode
connect           Open a terminal connection
copy              Copy configuration or image data
debug             Debugging functions
disable           Turn off privileged commands
disconnect        Disconnect an existing network connection
enable            Turn on privileged commands
erase             Erase flash or configuration memory
exit              Exit from EXEC
help              Description of interactive help system
lat               Open a lat connection
lock              Lock the terminal
login             Log in as a particular user
logout            Exit from the EXEC
mbranch           Trace multicast route down tree branch
--More--
```

5.2.9 AYUDA DE CONTEXTO

Si se conoce un comando pero no se está seguro de la sintáxis completa el IOS software soporta Ayuda de Contexto. Esta característica permite obtener una lista de palabras claves y argumentos asociados con el comando específico. Los modos EXEC usuario y privilegiado soportan ayuda de contexto.

Se pueden abreviar comandos y palabras clave a un número de carateres que permiten una abreviación única. Por ejemplo, se puede abreviar el comando *clock* a *clo*.

Utilizando la ayuda del contexto, el espacio antes del símbolo (?) es significante. Para obtener la lista de comandos que empiecen con una lista de caracteres en particular, escribir los caracteres seguido inmediatamente del símbolo (?). No incluir espacio.

5.2.10 UTILIZANDO COMANDOS ENHANCED EDITING

La interfaz de usuario incluye el modo Enhenced Editing que provee un conjunto de funciones claves de edición. Esta característica permite alterar o corregir comandos largos o complejos sin tener que reescribirlos. Aunque el modo Enhanced Editing es automáticamente habilitado con el release[31] del software existente se puede deshabilitar escribiendo *terminal no editing* en el prompt de mode EXEC usuario.

El conjunto de comando edición provee una característica de movimiento en sentido horizontal para comandos que se extienden más allá de una simple línea de pantalla. Cuando el cursor se mueve diez espacios a la izquierda no se pueden ver los primeros diez caracteres de la línea pero se puede regresar y revisar la sintáxis en el comienzo del comando. Las siguientes combinaciones ayudan a automatizar el scrolling de líneas largas:

- <Ctrl> <A> Mover al inicio de la línea de comando.
- <Ctrl> <E> Mover al final de la línea de comando.
- <Esc> <B> Mover al inicio de la palabra anterior.
- <Ctrl> <F> Mover adelante un caractér.
- <Ctrl> <B> Mover atrás un caractér.
- <Esc> <F> Mover adalante una palabra.

5.2.11 REVISANDO LA HISTORIA DE COMANDO

La interfaz de usuario provee de una historia o un registro de los comandos que se han utilizado. Esta característica es particularmente útil para recordar los comandos largos o complejos. Con esta característica de historia de comandos se pueden completar las siguientes tareas:

---

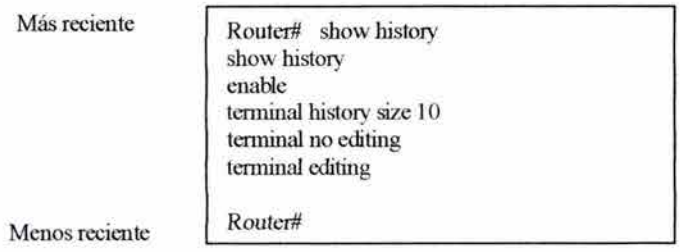
[31] Así se le llama a la version del IOS software

- Fijar el tamaño de buffer de historia de comando
- Recordar comandos
- Desabiliatar la característica de historia de comandos.

Para ver los parámetros de la historia existente, teclear *show history* en el prompt de modo EXEC privilegiado, como muestra la figura 5.6.

Por defecto, el comando *history* es habilitado y el sistema graba diez líneas de comando en este buffer history. Para cambiar el número de líneas de comando el sistema graba durante la sesión terminal existente, usar el comando *terminal history size*.

FIGURA 5.6



Lo siguiente son combianciones para automatizar el movimiento a través de la historia del comando:

- <Ctrl> <P> o Flecha *Arriba*: último comando recordado.
- <Ctrl> <N> o Flecha *Abajo*: El más reciente comando recordado.
- <Tab>: Terminación de la entrada.

5.3 EXAMINANDO EL ESTADO DEL RUTEADOR

Esta sección cubre los comandos básicos que se pueden usar para determinar el estado del ruteador. Esos comandos ayudarán a obtener información vital necesaria para operaciones de monitoreo y troubleshooting.

Los comandos de estado del ruteador son:

- Show version: Despliega la configuración de sistema de hardware, la versión del software, nombre y fuentes de archivos de configuración e imágenes de inicialización.
- Show processes: Despliega información acerca de los procesos activos.
- Show protocols: Despliega los protocolos. Este protocolo muestra el estado de algún protocolo de capa 3 configurado.

- Show memory: Muestra estadisticas acerca de la memoria, incluyendo memoria libre.
- Show ip route: Despliega las entradas en la tabla de ruteo.
- Show flash: Muestra información acerca del dispositivo de memoria flash.
- Show running-config (write term en el Cisco IOS Release 10.2 o nuevos): Despliega los parámetros de configuración activa.
- Show startup-config (show config en el Cisco IOS Release 10.2 o nuevos): Despliega el archivo de configuración de respaldo.
- Show interfaces: Despliega las estadísticas de todas las configuraciones del ruteador.

Las secciones siguientes examinan varios de esos comandos a más detalle.

5.3.1 COMANDO SHOW VERSION

El comando *show version* despliega la versión del IOS que corre en el ruteador como muestra en la figura 5.7.

FIGURA 5.7

```
Router# show version

IOS ™ 2500 Software (C2500-JS-L), Version 11.2 (6),. RELEASE SOFTWARE (fcl)
Copyrigth © 1986-1997 by cisco systems, Inc.
Compiled Tue 06-MAY-97 16:17 by Kuong
Image text-base: 0x0303ED8C, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2 (8a), RELEASE SOFTWARE
ROM: 2500-XBOOT Bootstrap Software, Versión 10.1 (1), RELEASE SOFTWARE

Router uptime is 1 week, 3 days, 32 minutes
Systemm restarted by reload
System image file is "c2500-js-1", booted via tftp from171.69.1.129

--More--
```

Esta información es importante para saber cuándo hacer una actualización del software en los ruteadores.

Este comando no sólo muestra la versión de software de los ruteadores sino también muestra estadísticas del tiempo en que ha estado funcionando el sistema, el nombre del archivo de imagen del sistema y el lugar de donde fue originado el archivo de sistema. Cada vez que la versión del IOS software es revisado o actualizado, un número de revisión

es aplicado a la versión. Este número de revisión aparece en paréntesis seguido del número de versión.

5.3.2 COMANDOS SHOW STARTUP-CONFIG Y SHOW RUNNING-CONFIG

Los commandos *show statup-config* y *show running-config* (mostrados en la figura 5.8) están entre los commandos más usados en el IOS software.

FIGURA 5.8

```
Router#     show startup-config
Using 1108 out of 130048 bytes
!
version 11.2
!
hostname router
                --More--
```

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

Current configuration
!
version 11.2
                --More--
```

El comando *show startup-config* permite al administrador de red ver el tamaño de la imagen y comenzar los comandos de configuración que el ruteador usará la próxima vez que inicialice. Este archivo de respaldo es guardado en memoria cuando el ruteador es inicializado y contiene toda la información especificada acerca de las interfaces de ruteador.

El comando *show running-config* despliega la información de la configuración de la memoria terminal. Se puede saber que se está corriendo la configuración cuando aparece en la pantalla la frase *current configuration*. Se pueden hacer cambios en la configuración que se está corriendo; sin embargo, esos cambios se perderán cuando el ruteador se apague. Para guardar los cambios de configuración se debe copiar el archivo de configuración de inicializacón almacenado en NVRAM. Para realizar esa copia utilizar el comando *copy running-config starup-config.*

En Cisco IOS Release 10.2 o nuevos, el comando *write terminal* muestra la configuración y el comando *show config* muestra la configuración de inicio.

5.3.3 COMANDO SHOW INTERFACES

El comando *show interfaces* despliega los parámetros configurables y estadísticas en tiempo real relacionadas con las interfaces del ruteador. Este comando es muy útil en la determinación de la actividad y el ambiente de una interfaz física o verificación de cambios que se le han hecho a las interfaces.

Un conjunto de estadísticas se pueden obtener del comando *show interfaces*:

- Estado de la interfaz.
- Tamaño del MTU.
- Dirección Internet para la interfaz.
- Dirección MAC para la tarjeta LAN.
- Tipo de encapsulación.
- Número de paquetes recibidos.
- Numero de errores en paquetes de entrada/salida.
- Número de colisiones detectadas.

Este comando es extremadamente útil en ayuda a determinar el estado del ruteador y su historia operacional.

Examinar la figura 5.9. La línea superior dice que la línea de protocolo está funcionando. Unas pocas líneas abajo, se muestra la dirección Internet y debajo hay ciertas métricas: BW, que es el ancho de banda; DLY, es retardo y más abajo está HDLC, que es el protocolo de encapsulación por defecto para líneas seriales en el ruteador.

FIGURA 5.9

```
Router# show interfaces
Serial0 is up, line protocol is up
Hardware is MK5025
Internet address is 183.8.64.129, subnet mask is 255.255.255.128
MTU 1500bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 9/255
Encapsulation HDLC, loopback not set, keppalive set (10 sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops: input queue 0/75, 0 drops
Five minute input rate 1000 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 0 no buffer
        331885 packets input, 6400237 bytes, 0 no buffer
        Received 230457 broadcast, 0 runts, 0 giants
        3 input errors, 3 CRC, 0 frame, 0 overrn, 0 ignored, o abort
        0 input erros, 0 collisions, 8 interfaces resets, 0 restarts
        45 carrier transitions
```

Un *runt*[32] es un paquete que es muy pequeño para ser legal y un *giant*[33] es un paquete muy grande.

[32] Si el frame es más corto de 64 bytes.
[33] Si el Frame es más largo de 1518 bytes.

5.3.4 COMANDO SHOW PROTOCOLOS

El uso del comando *show protocol* es para desplegar los protocolos configurados en el ruteador, como muestra la figura 5.10. Este comando muestra un estado global y específico de interfaces de algunos protocolos configurados de capa 3 como IP, DECNet, IPX y Apple Talk.

FIGURA 5.10

```
Router# show protocols
Global values:
   Internet Protocol routing is enabled
DECnet routing is enabled
XNS routing is enabled
Vines routing is enables
Appletalk routing is enabled
Novell routing is enabled
--More—
Ethernet0 is up, line protocol is up
Internet address is 183.8.128.2, subnet mask is 255.255.255.128
DECnet cost is 5
XNS address is 3010.aa00.0400.0284
CLNS enabled
Vines metric is 32
Appletalk address is 3012.93, zone 1 d-e0
Novell address is 3010.a00.0400.0284
--More--
```

Los ruteadores dividen la información del archivo de configuración en configuración global y configuración de interfaz. La configuración global dice el tipo del tráfico que el ruteador es capaz de pasar. La configuración de interfaz ofrece más información detallada de configuración tales como direcciones de protocolos.

CAPITULO 6

CONFIGURANDO UN RUTEADOR

Este capítulo cubre la carga del archivo de configuración, la configuración de interfaces, configuración de ruteo IP, configuración de ruteo IPX y Listas de Acceso. El capítulo presenta modos de configuración disponibles para usuario privilegiado así como también los comandos para entrar y realizar cambios.

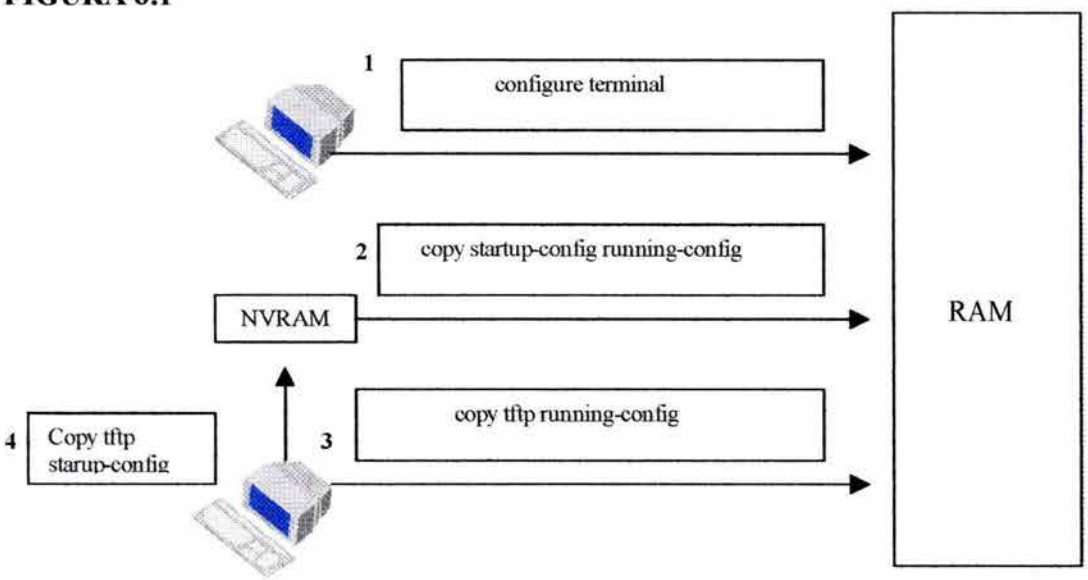
En la mayor parte de este capítulo se asume que el archivo de configuración ya existe. Sin embargo, se revisa el uso del modo *Setup* para crear o cambiar un archivo de configuración.

6.1 CARGANDO ARCHIVOS DE CONFIGURACIÓN

Como las variables de configuración afectan a todo el ruteador, se debe estar en modo de configuración global antes de crear, cargar o alterar algúna información de configuración existente. Para entar al modo de configuración global, introducir el comando *Configure* en el modo EXEC privilegiado.

La información de la configuración del ruteador puede ser generada por varios medios, como muestra la figura 6.1. Los comandos de configuración pueden venir desde una terminal, la memoria no volátil (NVRAM) o un archivo almacenado en un servidor de red. El medio fijo es una terminal de consola.

FIGURA 6.1



Para el IOS Release 10.3 se puede especificar la fuente de los comandos de configuración directamente cuando se entra al modo de configuración global, escribiendo uno de los siguientes comandos:

- *configure terminal*: Ejecuta comandos de configuración desde una terminal.
- *copy tftp running-config*: Copia un archivo desde un servidor tftp a RAM.
- *copy tftp startup-conf*: Carga un archivo de configuracion de un servidor TFTP directamente a la NVRAM.
- *copy startup-config running-config*: Copia la información de configuración en NVRAM a RAM. El ruteador actúa como un comando compilador de comandos y lee el archivo de configuración línea por línea, sobrescribiendo sólo las líneas que ya existen en RAM. Si hay un conflicto entre dos conjuntos de parámetros, el ruteador deshabilitará los procesos.

6.1.1 CARGANDO ARCHIVOS DE CONFIGURACION DESDE UN SERVIDOR TFTP

Si se tiene una red la cual consiste de algunos ruteadores, se puede mantener la consistencia de los archivos de configuración y reducir la carga de trabajo usando una o dos configuraciones de respaldo. Utilizar un servidor de red para almacenar respaldos de archivos de configuración y ahorrar tiempo.

El siguiente ejemplo copia un archivo de configuración desde un servidor TFTP al ruteador (ver la figura 6.2).

Para extraer el archivo de configuración almacenado en un servidor TFTP, veamos los siguientes pasos:

- Entrar al modo de configuración con el comando *copy tftp running-config*.

FIGURA 6.2

```
Router# copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-conf]? P1R1.2
Configure using P1R1.2 from 131.108.2.151? [confirm] y
Booting P?1R1.2 from 131.108.2.155:!! [OK – 874/16000 bytes]
P1R1#
```

- Incorporar el tipo de archivo de configuración. El prompt da la opción de cargar uno o dos tipos de archivos de configuración desde el servidor. Esos tipos de archivos son:

    1. Host Configuration File: Este tipo de archivo de configuración contiene comandos que se aplica a un ruteador en particular.
    2. Network Configuration File: Este archivo de configuración contiene comandos que son aplicables a todos los ruteadores de la red.

- Escribir la dirección de red de Host remoto del cual se extraerá el archivo de configuración.
- Escribir el nombre del archivo de configuración o aceptar el número fijo.

6.2 TAREAS FUNDAMENTALES DE CONFIGURACIÓN

En esta sección se revisan los comandos de configuración que individualiza al ruteador. También se discuten los comandos que alteran las interfaces del ruteador.

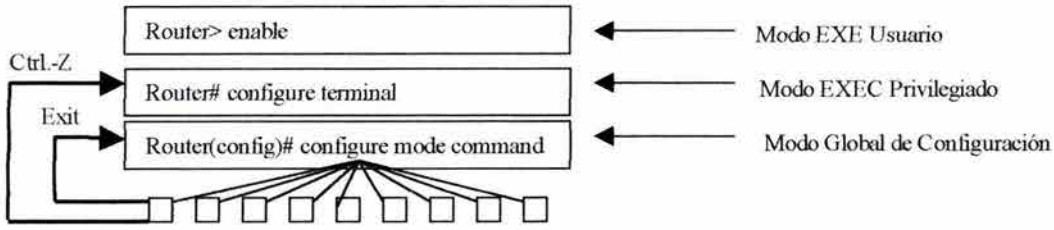
6.2.1 DESCRIPCION DE LOS MODOS DEL RUTEADOR

Escribir *configure terminal* para entrar al modo de configuración global. El modo de configuración global reconoce los comandos que afectan a todo el ruteador. Por ejemplo, el ruteador tiene un password habilitado y un nombre de host, esos comandos son aceptados en el modo de configuración global. También en el modo de configuración global, el ruteador reconoce comandos en línea. Algunos de esos comandos provocan que el ruteador entre en otros modos de configuración donde se reconocen comandos más complicados.

Un ejemplo de otro modo de configuración es el modo de configuración de interfaz. Se puede entrar en este modo especificando una interfaz en particular. Algunos comandos, tales como *ring-speed*, son apropiados para Token Ring pero no tendrían ningún sentido en una interfaz serial.

El prompt siempre identifica el modo operativo actual, incluyendo el modo global de configuración, como muestra la figura 6.3.

FIGURA 6.3



Modo Configuracion	Puerto de Ruteador
Interfaz	Router(config-if)#
Subinterface	Router(config-subif)#
Controlador	Router(config-controller)#
Linea	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-IPX-router)#
Route-map	Router(config-roter-map)#

Desde el modo de configuración global se puede tener acceso a modos específicos de configuración, incluyendo:

- Interface Mode: Soporta comandos que configuran operaciones en una base pre-interfaz.
- Subinterface Mode: Soporta comandos que configuran múltiples interfaces virtuales en una simple interfaz física.
- Controller Mode: Soporta comandos que configuran un T1/E1 canalizado.
- Line Mode: Soporta comandos que configuran la operación de una línea.
- Router Mode: Soporta comandos que configuran un protocolo de ruteo IP.
- IPX-Router Mode: Soporta comandos que configuran un protocolo de capa red red Novell.
- Route-Map Mode: Soporta comandos que configuran tablas de ruteo.

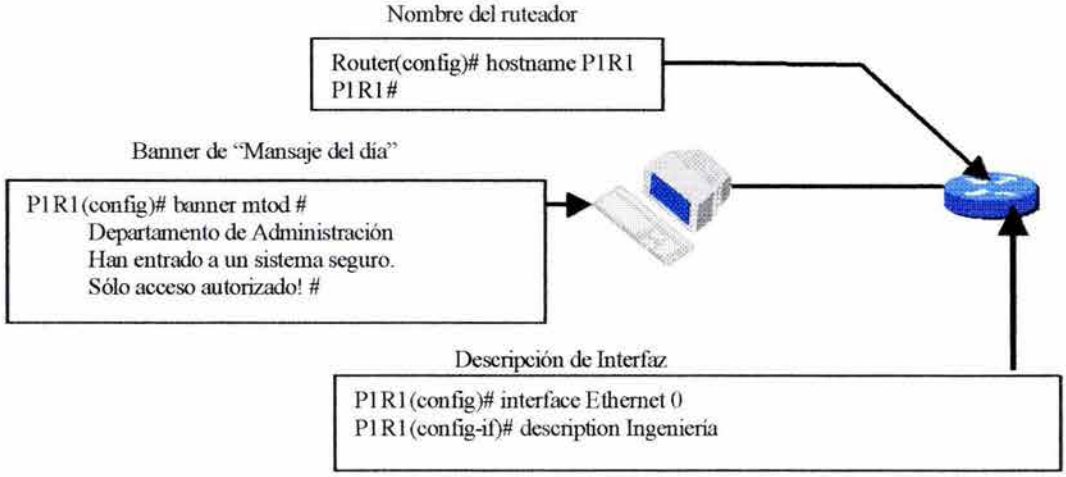
Si se escribe *Exit*, el ruteador regresará al nivel anterior. En general, introducir el comando *Exit* desde uno de los modos de configuración específicos, se regresará al modo de configuración global. Presionando Ctrl-Z, se deja el modo de configuración completamente y el ruteador regresa al modo EXEC privilegiado.

6.2.2 CONFIGURANDO LA IDENTIFICACION DEL RUTEADOR

Una de las primeras tareas a realizar en la configuración de un ruteador es darle un nombre. Nombrar al ruteador ayuda a una mejor administración de la red por una identificación única para cada ruteador en la red. El nombre del ruteador es considerado el nombre de host y es el nombre desplegado en el prompt del sistema. Si no hay un nombre

configurado, el nombre del ruteador por defecto es *Router*. En al figura 6.4, el nombre del ruteador es P1R1.

FIGURA 6.4



Se puede configurar un banner con un "mensaje del día" para ser desplegado en todas las terminales conectadas. Este banner es desplegado al entrar a la red. Cuando se introduce el comando *banner mtod*, sigue le comando con uno o dos espacios en blanco y un carácter delimitado, por ejemplo, el signo (#). Después se añade el texto banner y se termina con un carácter delimitado.

Algunos otros banners son disponibles incluyendo un *idle banner*, el cual se despliega en una terminal o consola cuando no está en uso. Algunas veces se utiliza el *idle banner* para desplegar el logo coporativo.

Se puede añadir una descripción a la interfaz para ayudar a recordar la información específica de esa interfaz. Esta descripción es solamente un comentario para ayudar a identificar la manera en que una interfaz está siendo utilizada.

La función *description* es fácil de implementar utilizando la sintaxis *descrition (string)*. Considerar el siguiente ejemplo:

P1R1(config-if)#descrption Network Lab, Tyler Building

6.2.3 CONFIGURACION DE PASSWORD

Se puede tener seguro el ruteador por un password para restringir el acceso. Los passwords pueden ser establecidos en líneas individuales y en el modo EXEC privilegiado.

El Password de consola está fijo independientemente de otros passwords de líneas, tales como passwords de terminales virtuales. Si la consola se encuentra en alguna oficina bajo llave no se necesitará password de consola, sólo con presionar *return* y se estará en modo

usuario. Sin embargo, si la consola no esta bajo llave se tendrá que poner un password en la línea de consola.

6.2.4 PASSWORD DE CONSOLA

Line console 0 login password xxxx establece un password de una conexión a la consola.

Line VTY 0 4 login password xxxx establece password de conexión para sesiones Telnet.

El comando *enable password* restringe el acceso al modo EXEC privilegiado.

6.2.5 PASSWORD DE TERMINAL VIRTUAL

El password de la terminal virtual debe ser fijo para soportar configuración remota. Telnet requiere de un password. Los números 0 y 4 son un rango, que son lineas de VTY de 0 a 4, la cual es igual a 4 líneas o es igual a 5 sesiones de Telnet.

El mismo password puede ser usado por las 5 sesiones. Sin embargo, se debe fijar un password de la terminal virtual para ser único. Esta configuración es a menudo usada en redes grandes con varios administradores de red.

6.2.6 PASSWORD DEL MODO EXEC PRIVILEGIADO

El ruteador tiene un *enable password*. Sea quien sea que tenga el password puede hacerle lo que quiera al ruteador.

Para proveer una capa adicional de seguridad, particularmente para passwords que cruzan la red y son almacenados en un servidor TFTP, se puede utilizar el comando *enable secret*. Ambos comandos, *enable password* y *enable secret* permiten establecer un password encriptado que los usuarios deben introducir para accesar del modo EXEC usuario al modo EXEC privilegiado, pero el comando *enable secret* ofrece una mejora del algoritmo de encriptación.

6.2.7 ENCRIPTACION DE PASSWORD

Los comandos pueden ser protegidos del desplegado a través del uso del comando *service password-encryption*. Para fijar la encriptación de passwords se debe introducir lo siguiente en el modo de configuración global:

Router(config)# service password-encryption

Si un password encriptado es perdido se debe borrar la configuración del ruteador y crear una nueva configuración en el modo Setup.

6.2.8 CONFIGURACION Y MANEJO DE UNA INTERFAZ

La función principal de un ruteador es trasmitir paquetes de un punto a otro. Para hacer esto, las características de interfaces por las cuales son recibidos y enviados los paquetes deben ser definidas. Esas características incluyen la dirección de puerto, el método de encapsulación del dato, tipo de medio y ancho de banda.

El modo de configuración de interfaz contiene comandos que modifican la operación de un puerto Ehternet, Token Ring, FDDI o Serial. Cuando se utiliza el comando *interface*, se debe definir el tipo de interfaz y el número. El número es asignado a cada interfaz por el fabricante y es utilizado para identificar cada interfaz, la cual es particularmente útil cuando se tienen múltiples interfaces del mismo tipo en un ruteador.

Un ejemplo de tipo de interfaz y número.

Router(config)# interface serial 0
Router(config)# interface Ethernet 1

Algunas series de ruteadores pueden aceptar múltiples tarjetas de interfaz con múltiples puertos en cada tarjeta. En este caso, el primer número es el número de la tarjeta o numero del slot. El segundo número es el número de puerto en la tarjeta. Por ejemplo, en la segunda tarjeta de interfaz, la primera interfaz Ethernet es especificada *ethernet 2/0*.

Se define una interfaz en los ruteadores Cisco por el número de slots y puertos:

Router(config)#interface ethernet 1/0

Para salir del modo de configuración de interfaz, introducir el comando *exit* en el prompt.

6.9 COMANDO SHOW INTERFACES

El comando *show interfaces* despliega todas las estadísticas de todas las interfaces en el ruteador, como muestra la figura 6.5.

FIGURA 6.5

```
Router#show interfaces
    Ethernet0 is up, line protocol is up
    Hardware is Lance, address is 0060.4740.c2b6 (bia 0060.4740.c4b6)
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
    Encapsulation ARPA, loopback no set, keepalive set (10 sec)
     ARP type: ARPA, ARP Tomeout 04:00:00
                                        *
                                        *
Serial1 is up, Line protocol is down
     Hardware is MK5025
     MTU 1500 bytes, BW 1544 Kbits, DLY 20000 usec, rely 255/255, load 9/255
     Encapsulation HDLC, loopback not set, keepalive set (10 sec)
                                        *
                                        *
```

Si se quiere una vista de las estadísticas para una interfaz específica, introducir el comando *show interfaces* seguido de la interfaz específica y el número de puerto. El siguiente ejemplo utiliza el comando *show interface* para desplegar estadísticas de la interfaz serial, puerto 1:

Router# show interfaz serial 1

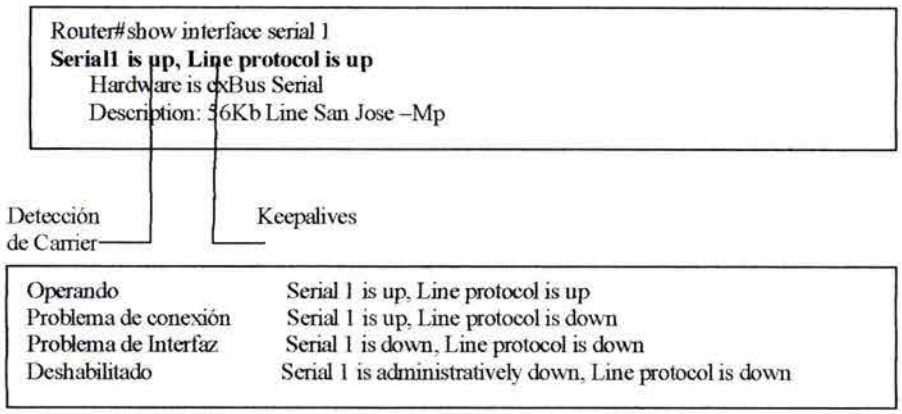
Si se utiliza el comando *show interfaces* en los ruteadores Cisco 3600, 7000 y 7200, sin argumentos slot/puerto, la información será desplegada para todos los tipos de interfaz que tenga el ruteador. Por ejemplo, si se escribe *show interfaces ethernet*, se recibirá información de todas las interfaces ethernet. Sólo el camino para especificar una interfaz en particular es añadiendo el tipo de slot/puerto.

En la figura 6.5, la primera línea dice que la interfaz está en funcionamiento. Más abajo están algunas características. Para la interfaz Ethernet, la dirección MAC de la tarjeta, el MTU y el ancho de banda. Para la interfaz serial, el ancho de banda fijo es un T1. En la siguiente línea está HDLC[34] que es el protocolo de encapsulación fijo para las interfaces seriales.

6.2.10 INTERPRETANDO EL ESTADO DE LA INTERFAZ

Uno de los elementos más importantes del comando *show interfaces*, es el despliegue y línea de estado del protocolo de enlace de datos. La figura 6.6 indica el despliegue de estado de la interfaz.

FIGURA 6.6



El primer parámetro ("Serial1 is up", en la figura 6.6) se refiera a la capa de hardware y esencialmente refleja si la interfaz está recibiendo la señal del carrier. El segundo parámetro

[34] High Level Data Link Control. Protocolo síncrono orientado a bit de la capa de enlace de datos.

("Line protocol is down", en la figura 6.6) se refiere a loa capa de enlace de datos. Este parámetro refleja si los keepalives del protocolo de enlace de datos están siendo recibidos.

Las siguientes combinaciones de parámetros son posibles:

- Si la interfaz y la línea de protocolo arriba, la conexión es operacional.
- Si la interfaz está arriba y la línea de protocolo está abajo, existen problemas de capa de enlace de datos como:

    1. No Keepalive.
    2. No rango de reloj.
    3. Conector incorrecto.
    4. Encapsulación incorrecta.

- Si la interfaz y la línea de protocolo están abajo, nunca se conectó el cable cuando se encendió el ruteador.
- Si la información dice "administratively down", se ha deshabilitado manulmente la interfaz.

6.2.11 CONFIGURANDO UNA LINEA SERIAL

Unas de las configuraciones de interfaces más comunes es una configuración serial. Una interfaz serial puede ser configurada desde la consola o por medio de una terminal virtual. La figura 6.7 muestra la manera de configurar una línea serial.

Los pasos para configurar una línea son los siguientes:

- Entrar al modo de configuración global. En este ejemplo se configura la interfaz serial desde la consola.
- Una vez que se está en el modo de configuración global se debe identificar una interfaz específica.
- Si se está configurando una interfaz que actúe como un dispositivo DCE[35]. Se debe especificar un rango de reloj en bits por segundo: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 o 4000000.

[35] Data Comunnicatios Equipment. Dispositivos y conexiones de redes de comunicaciones que abarcan el extremo de la red del usuario a la interfaz de la red. El DCE provee conexión física a la red, reenvia trafico y provee señales de reloj usadas para sincronizar la transmisión de datos.

FIGURA 6.7

Entrar el modo de configuración global	Router#configure term Router (config)#
Especificar Interfaz	Router(config)#interface serial 1 Router(config-if)#
Fijar Rango de reloj DCE (opcional)	Router(config-if)#clock rate 56000
Fijar ancho de banda (opcional)	Router(config-if)#bandwidth 56 Router(config-if)#exit Router(config)#exit Router#

- Escribir el ancho de banda deseado para la interfaz. El comando *bandwidth* reempleza el ancho de banda desplegado en el comando *show interfaces* y es utilizado por algunos protocolos de ruteo como IGRP.

Si se cambia la interfaz de DCE a DTE[36]. Utilizar el comando *no clock rate* para remover el reloj.

6.2.12 DETERMINADO EL ESTADO DE DTE/DCE

En conexiones seriales, un lado del enlace actúa como dispositivo DCE y el otro lado como dispositivo DTE. Por defecto, los ruteadores Cisco son dispositivos DTE pero se pueden configurar como dispositivos DCE.

Antes de que se empiece a configurar o alterar la interfaz serial, se debe determinar si la interfaz será DCE o DTE. El comando *show controllers serial* despliega la información específica del hardware de la interfaz, como muestra la figura 6.8.

[36] Data Terminal Equipment. Dispositivo que sirve como fuente de datos, destino o ambos. El DTE conecta una red de datos a través de un DCE.

FIGURA 6.8

```
Router#show controllers serial 1
HD unit 1, idb= 0xBFD3C, drive structure at 0xC39A0
buffer size 1524 HD unit 1, V.35 DCE cable, clock rate 56000
cpb = 0x83, eda = 0x800, cda = 0x830800
RX ring with 16 entries at 0x83800
00 bd_ptr=0x0800   pak=0x0C54F0   ds=0x836938   status=80 pak_sizes=22
01 bd_ptr=0x8014   pak=0x0C5158   ds=0x835BC8   status=80 pak_sizes=22
02 bd_ptr=0x0828   pak=0xC4F8C    ds=0x835510   status=80 pak_sizes=259
03 bd_ptr=0x083C   pak=0x0C4DC0   ds=0x834E58   status=80 pak_sizes=22
                                  *
                                  *
                                  *
```

Se puede desplegar información de todos los controladores, de un tipo de controlador o de un controlador específico. El comando *show controllers* despliega información de todos los controladores instalados en el ruteador. El comando *show controllers serial* despliega información de un tipo de interfaz. El comando *show controller serial 1* despliega información de un controlador específico.

6.2.13 VERIFICANDO LOS CAMBIOS

Tomarse un momento para verificar los cambios que se le han hecho a una interfaz puede garantizar que no se presenten errores durante el proceso de guardar los cambios. El comando *show interfaces* habilita una vista de la configuración y el estado de una interfaz. Por ejemplo, la figura 6.9 muestra la vista que arroja el comando *show interfaces serial 1*.

FIGURA 6.9

```
Router#show interfaces serial 1
Serial1 is up, line protocol is up
Hardware is MK5025
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 9/255
Encapsulation HDLC, loopback not set, keepalive set (10sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of "show interfaces" counters never
Output queue 0/40, 0 drops; input quere 0/75, 0 drops
Five minute input rate, 1000 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 0 packets/sec
331885 packets input, 62400237 bytes, 0 no buffer
Received 230457 broadcasts , 0 runts, 0 giants
3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
403591 packets ougtput, 66717279 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface reset, 0 restarts
45 carrier transitions
```

6.2.14 DANDO DE BAJA UNA INTERFAZ

Se puede deshabilitar una interfaz, por ejemplo, para realizar mantenimiento de hardware de una interfaz específica o de un segmento de red. También si existe un problema en un segmento de red en particular y si se necesita aislar ese segmento del resto de la red hasta que el problema sea detectado o reparado.

El comando *shutdown*, como muestra la figura 6.10, apaga la interfaz. Para que la interfaz vuelva a funcionar se usa el comando *no shutdown*.

FIGURA 6.10

```
Router#configure term
Router(config)#interfaces serial 1
Router(config-if)}#shutdown
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial1, changed state to down
%LINK-5-CHANGED: Interface Serial, changed state to administratively down
```

```
Router#configure term
Router(config)#interfaces serial 1
Router(config-if)}#shutdown
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial1, changed state to up
%LINK-3-UPTOWN: Interface Serial, changed state to up down
```

6.3 MANEJANDO EL AMBIENTE DE CONFIGURACIÓN

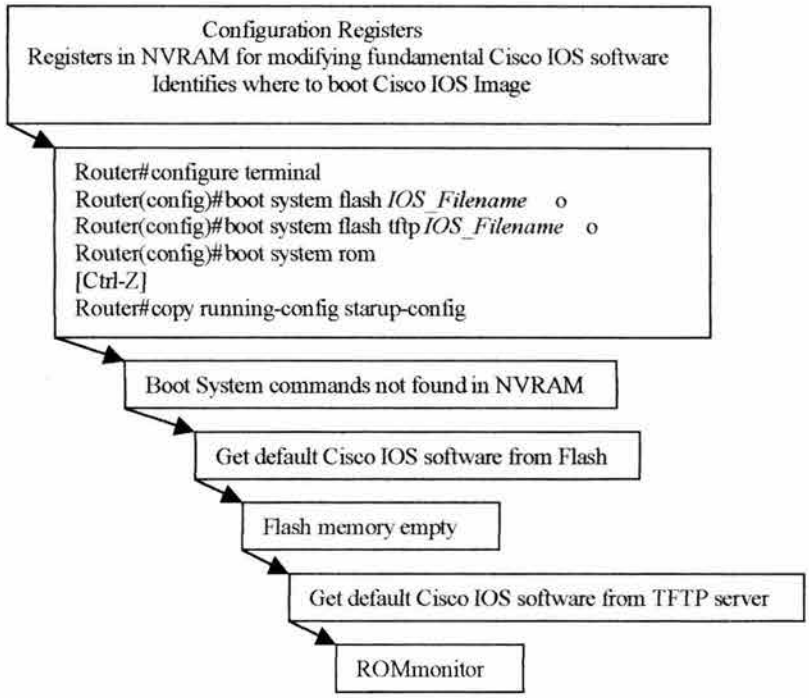
Esta sección discute las fuentes alternativas para el Cisco IOS y la manera en que el ruteador se direcciona para localizar el software y la manera para modificar el registro de configuración existente para encontrar una nueva localización para la imagen del sistema.

6.3.1 LOCALIZANDO EL CISCO IOS SOFTWARE

El campo de arranque del registro de configuraciones, determina si el ruteador carga una imagen de sistema operativo y si es así, el sitio de donde se obtiene la imagen. Se puede modificar el campo de arranque del registro de configuración para decirle al ruteador cómo debe cargar la imagen del sistema en el arranque. En lugar de utilizar una imagen de sistema y un archivo por defecto, se puede especificar una imagen de sistema en particular y un archivo de configuración localizados en otra parte de la red.

La fuente fija del Cisco IOS Software depende de la platarforma del hardware, pero comúnmente el ruteador ve los comandos de configuración guardados en NVRAM.

FIGURA 6.11



Si se especifica el comando *boot system* para definir las secuencias de fuentes, se pueden guardar esos estatutos en NVRAM con el comando *copy running-config* o con el comando *startup-config*. El ruteador utilizará la nueva secuencia durante el próximo arranque.

Si el comando *boot system* no es utilizado, el sistema tienen otras alternativas (figura 6.11). El ruteador busca el Cisco IOS software en la memoria Flash.

Si la mamoria Flash está vacia, el ruteador tratará otra alternativa. Utiliza el valor de registro de configuración para formar un nombre de archivo desde la cual pueda arrancar una imagen de sistema almacenado en un servidor de red.

Finalmente, si el ruteador agota todas las alternativas y no puede encontrar el Cisco IOS software, el ruteador entra en modo ROM Monitor.

6.3.2 DETERMINADO EL VALOR DE REGISTRO DE CONFIGURACIÓN ACTUAL

Antes de alterar el registro de configuración, se debe determinar la manera en que el ruteador carga la imagen. Utilizar el comando *show versión* para obtener el valor del registro de configuración como muestra la figura 6.12. La última línea que arroja el comando *show versión* contiene el valor de registro de configuración.

FIGURA 6.12

```
Router#show version

IOS ™ 2500 Software (c2500-JS-L), Version 11.2(6), RELEASE SOFTWARE (fcl)
Copyright © 1986-1997 by Cisco System, Inc.
Compiled Tue 06-May-97 16:17 by Kuong
Image text-base: 0x0303ED8C, data-base; 0x00001000

ROM: System Bootstrap, Version 5.2 (8a), RELEASE SOFTWARE
ROM: 3000 Bootstrap Software (IGS-RXBOOT), version 10.2 (8a),
RELEASE SOFTWARE (fcl)
Router uptime is 21 hours, 13 minutes
System restarted by reload
System Image file is "flash:c2500-js-1.112-6.bin", booted via flash
                                        *
                                        *
                                        *
Configuration register is 0x02102
```

Se puede cambiar el registro de configuración con el modo de configuración activo y el comando *config-register*. Introducir *configure terminal* en modo EXEC privilegiado para entrar al modo de configuración, como muestra la figura 6.13

FIGURA 6.13

```
Router#configure terminal
Router(config)#config-register
0x2102
[Ctrl-Z]
Router#reload
```

El registro de configuración es un registro de 16 bits. Los cuatro bits menos significativos forman el campo de arranque. Un número hexadecimal es utilizado como argumento para fijar el valor de registro de configuración. La siguiente tabla muestra opciones hexadecimales y sus significados.

Valor de Registro de Configuración	Significado
0x0	Utilización del modo ROM Monitor
0x1	Arranca automáticamente desde ROM
0x2 a 0xF	Examina NVRAM para comandos de sistema de arranque

Para cambiar el campo de arranque y dejar los otros bits fijos para sus valores por defecto, seguir los siguientes pasos:

- Fijar el campo de arranque en 0 para entrar automáticamente al modo ROM Monitor. El ruteador despliega el prompt *rommon>* en este modo.

- Fijar el campo de arranque en 1 para configurar el sistema para arrancar automáticamente de ROM. El ruteador despliega el prompt *Router(boot)>* en este modo.
- Fijar el campo de arranque en valores de 2 a F para configurar que el sistema utilize los comandos de sistema de arranque en NVRAM.

Utilizar el comando *show version* para verificar los cambios en el campo de arranque.

6.3.3 OPCIONES DE BOOT SYSTEM EN SOFTWARE

Como se mencionó anteriormente, se puede definir una secuencia que el ruteador pueda utilizar durante el arranque. La figura 3.14 muestra los comandos de boot system utilizados para especificar una secuencia para arrancar el Cisco IOS Software.

Los comandos de *boot system* en (figura 6.13) especifican que la imagen del Cisco IOS Software primero será cargada desde la memoria Flash, después de un servidor de red y finalmente de la ROM.

Cargado desde la memoria Flash, permite copiar una imagen de sistema sin cambiar la EEPROM[37].

La información almacenada en la memoria Flash no es vulnerable a las fallas de red que puedan ocurrir cuando se cargan las imágenes des sistema desde servidores de red.

FIGURA 6.13

Flash

```
Router#configure terminal
Router(config)#boot system flash c2500-js-1.1
[Ctrl-Z]
Router#copy running- config startup-config
```

Red

```
Router#configure terminal
Router(config)#boot system tftp test.exe 172.16.13.111
[Ctrl-Z]
Router#copy running- config startup-config
```

ROM

```
Router#configure terminal
Router(config)#boot system rom
[Ctrl-Z]
Router#copy running- config startup-config
```

[37] Electrically Erasble Programmale Read-Only Memory. Puede ser borrada usando señales eléctricas aplicadas en pines específicos.

En caso de que la memoria Flash llegara a ser corrupta, las entradas del sistema de arranque (en la figura 6.13) especifican que la carga de la imagen debe ser cargada desde un servidor de red. Finalmente, si la memoria Flash es corrupta y el servidor de red falla, para cargar la imagen se debe hacer desde ROM.

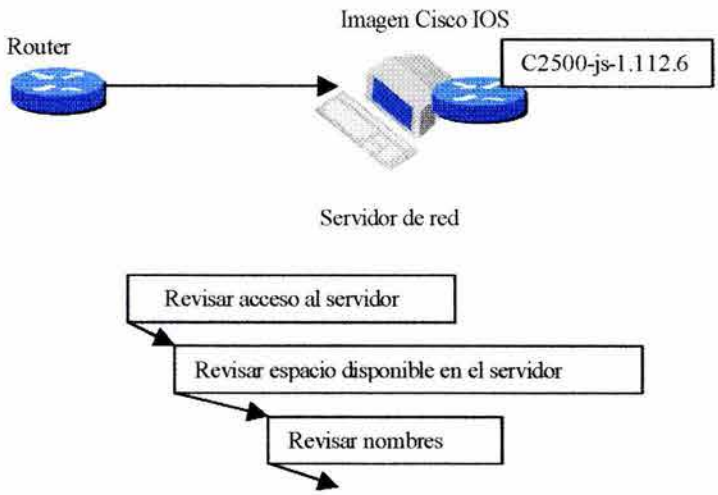
El comando *copy running-config startup-config* guarda la secuencia de comandos en NVRAM. El ruteador ejecutará los comandos *boot system* en el orden en el cual fueron integrados en el modo de configuración.

6.3.4 PREPARANDO UN RESPALDO DE IMAGEN DE SISTEMA

Se necesita tener una copia de respaldo de la imagen de sistema en caso de que la imagen en el ruteador sea corrupta.

Ruteadores geográficamente distribuidos necesitan una localización fuente o de respaldo para imágenes de sistema. Utilizar un servidor de red permite cargas y descargas de imágenes de sistemas y configuraciones sobre la red. El servidor de red puede ser otro ruteador, una estación de trabajo o un host de sistema, como muestra la figura 6.14.

FIGURA 6.14



Antes de copiar el software entre el servidor y la memoria Flash del ruteador, se debe de considerar lo siguiente:

- Estar seguros de que hay acceso al servidor de red.
- Verificar que el sevidor de red tenga suficiente espacio para la imagen de sistema.
- Revisar los requerimientos de nombres de archivos.

6.3.5 OBSERVANDO LA MEMORIA DISPONIBLE Y EL NOMBRE DEL ARCHIVO DE LA IMAGEN

El comando *show flash* es una herramienta importante para obtener información acerca de la memoria del ruteador y el nombre de la imagen (ver la figura 6.15)

FIGURA 6.15

```
Router#show flash

System flash directory:
Files          Length          Name/status
  1            7871172         c2500-js-1.112-6.bin

[7871236 bytes used, 517372 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Con el comando *show flash* se puede determinar lo siguiente:

- Cantidad total de memoria en le ruteador.
- Cantidad de memoria disponible.
- Nombre del archivo de imagen de Cisco IOS Software usado por el ruteador.

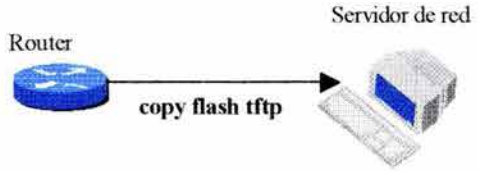
El nombre del archivo de la imagen de sistema contiene varias partes, cada una tiene su significado especifico:

- La primera parte de la imagen contiene la plataforma en la cual la imagen corre. En la figura 6.15 la plataforma es c2500.
- La segunda parte del nombre especifica capacidades especiales del archivo de imagen. Una letra o una serie de letras identifica las caracteristicas fijas soportadas en esta imagen. En la figura 6.15, la *j* indica que una imagen enterprise y la *s* significa que tiene capacidades extendidas.
- La tercera parte del nombre especifica dónde corre la imagen y si el acrchivo es comprimido. En la figura 6.15 el *1* indica que el archivo es relocalizado y no es comprimido.
- La cuarta parte indica el número de versión. En la figura 6.15 el número de versión es 11.2(6).
- La parte final del nombre es la extensión del archivo. La extensión *.bin* indica que este archivo es un archivo ejecutable binario.

6.3.6 CREANDO UN RESPALDO DE IMAGEN DE SOFTWARE

Se puede crear un archivo de imagen de software copiando el archivo de imagen desde el ruteador al servidor de red como, muestra la fugura 6.16.

FIGURA 6.16




```
Router#show flash

System flash directory:
Files          Length          Name/status
  1            7871172         c2500-js-1.112-6.bin

[7871236 bytes used, 517372 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
IP address of remote| host [255.255.255.255]? 172.16.13.111
filename to write on tftp server? C2500-js-1.112.-6
wrting c2500-js-1.112-6  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
successful tftp write.
Router#
```

Para copiar el archivo de imagen de sistema del ruteador al servidor de red, se utiliza el commando *copy flash* en el modo EXEC privilegiado.

Cuando se utiliza un servidor tftp:

Router#copy flash tftp

El comando *copy flash* también requiere de la dirección IP del host remoto y el archivo de imagen del sistema fuente y destino. El comando *copy flash* despliega el contenido de la memoria Flash incluyendo el nombre del archivo de imagen de sistema.

Parar el proceso de copiado, presionar las teclas CTRL+SHIFT.

6.3.7 ACTUALIZANDO LA IMAGEN DE SISTEMA DESDE LA RED

Se debe cargar un nuevo archivo de imagen de sistema en el ruteador si el archivo de imagen de sistema existente ha sido dañado o si se esté actualizando el sistema a una versión nueva. Se puede bajar una imagen usando el siguiente comando:

Router#copy tftp flash

El comando preguntará por la dirección IP del host remoto y el nombre fuente y destino del archivo de la imagen de sistema. Introducir el nombre de archivo correcto y apropiado de actualización de imagen como aparecen en el servidor de red. Ver figura 6.17.

FIGURA 6.17

```
Router#copy tftp flash
IP address or name of remote host [255.255.255.255]?172.16.13.11
Name of tftp filename to copy into flash []?c4500-js-l
copy c4500-js-1.112-6 from 172.16.13.111 into flash memory?[confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm]<Return>
Clearing and initializing flash memory (please wait) ###...##
Loading from 172.16.13.111:!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!! (text omitted) [OK – 324572/524212 bytes]
Verifying checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvv (text omitted)
Flash verification successful. Length = 1804637, checksum = 0xA5D3
```

Antes de realizar este procedimiento se debe estar seguro que se puede alcanzar el servidor TFTP y revisar la disponibilidad de la imagen de sistema adecuada. Se debe estar seguro de utilizar el comando *show flash* para ver el archivo y comparar su tamaño con el de archivo original en el servidor antes de cambiar los comandos de *boot system* y arrancar el ruteador en un nuevo nivel.

Después de confirmar las entradas, el procedimiento pregunta si se quiere borrar la memoria Flash. Borrar la memoria Flash genera espacio para la nueva imagen. Se puede realizar esta tarea si hay suficiente memoria Flash para soportar más de una imagen de sistema. Si no se tiene suficiente espacio disponible en la memoria Flash o si la memoria Flash nunca ha sido escrita, se requiere de una rutina de borrado antes de copiar la nueva imagen de sistema.

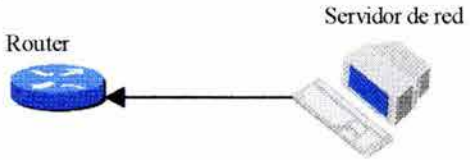
Como se muestra en la figura 6.17, cada exclamación (¡) significa que un segmento UDP se ha transmitido exitosamente. La serie de Vs indica que la verificación checksum de un segmento fue existosa.

Precaucion: Por un periodo de tiempo después de que la memoria Flash fue borrada y no se ha copiado la imagen de sistema, la situación es crítica. Algunos ruteadores que corren el Cisco IOS Software desde la memoria Flash, si se borra la memoria Flash de esos ruteadores, como la serie 2500, el ruteador dejará de funcionar.

6.3.8 SOBRESCRIBIENDO LA IMAGEN EXISTENTE

Si se hace una copia de una imagen sobre otra imagen que ya existe, el sistema notificará, como lo muestra la figura 6.18

FIGURA 6.18




```
Router#copy tftp flash
IP address or name of remote host [255.255.255.255]?172.16.13.11
Name of tftp filename to copy into flash []?c4500-js-l
File c4500-js-1.112-6 already exists; it will be invalidate!
copy c4500-js-1.112-6 from 172.16.13.111 into flash memory?[confirm] <Return>
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm]<Return>
Clearing and initializing flash memory (please wait) ###...##
Loading from 172.16.13.111:!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!! (text omitted) [OK – 324572/524212 bytes]
Verifying checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvv (text omitted)
Flash verification successful. Length = 1204637, checksum = 0x95D9
```

El archivo existente es borrado cuando se copie un nuevo archivo en la memoria Flash. La primera copia del archivo aún reside en la memoria Flash pero no se puede utilizar a favor de la nueva versión y será listada con la etiqueta [deleted] al utilizar el comando *show flash*.

Si más de un archivo del mismo nombre es copiado en la memoria Flash, sin importar el caso, el último archivo copiado será el archivo válido. Si se aborta el proceso de copiado del archivo más nuevo es marcado como *Deleted* porque el archivo entero no fue copiado y no es válido. En este caso, el archivo original aún reside en la memoria Flash y esta en uso.

6.3.9 CREANDO O CAMBIANDO UNA CONFIGURACION UTILIZANDO EL COMANDO SETUP

Si el dispositivo es un ruteador nuevo o los contenidos de la NVRAM son corruptos en ruteador no puede encontrar la información de la configuración necesaria para arrancar. En cualquiera de esos casos, el modo de ruteador entra en el modo de SETUP y empieza la configuración. Se puede forzar la entrada al modo SETUP con el comando *setup* en el modo EXEC privilegiado.

El propósito principal de este modo SETUP es dar la configuración mínima, la cual se realiza a través del programa System Configfuration Dialog.

La primera cosa que pregunta el programa System Configuration Dialog es si se quiere continuar con el programa, como lo muestra la figura 6.19.

FIGURA 6.19

```
Router#setup

        -- System Configuration Dialog --

At any point you may enter a question mark "?" for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets "[]"


Continue with configuration dialog? [yes/no]:    yes

First, would you like to see the current interface summary? [yes]:     no
```

Se puede salir del programa escribiendo NO en el prompt. Para empezar un proceso inicial de configuración, escribir YES. Presionando Ctrl-C se termina le proceso.

Para algunos de los prompts en el programa System Configuration Dialog del comando *setup*, las respuestas por defecto aparecen en corchetes ([]) después de la pregunta. Presionando RETURN permite utilizar las respuestas por defecto.

6.3.10 PARAMETROS DEL MODO SETUP GLOBAL

Si se decide continuar con el programa System Configuration Dialog, primero se deben fijar los parámetros globales para el ruteador.

El primer parámetro global permite definir el nombre del ruteador. Este nombre estará presente en todos los modos de configuración. En la configuración inicial el nombre del ruteador por defecto es mostrado entre corchete asi *[Router]*, como lo muestra la figura 6.20.

Los siguientes parámetros globales muestran la manera en que se fijan varios passwords utilizados en el ruteador. Esos parámetros están donde se define un password secreto. Cuando se introduce una cadena de caracteres de un password, los caracteres son procesados por encriptación propiedad de Cisco. Este proceso mejora la seguridad de password. Se recomienda utilizar diferentes passwords y mantener un nivel de seguridad mejorado.

FIGURA 6.20

```
Configuring global parameters:

    Enter host name [Router]: P1R1

The enable secret is a one-way cryptographic secret used
Instead of the enable password when it exists.

    Enter enable secret [<Use current secret>]:

    Enter enable password [sanfran]:
% Please choose a password that is different from the enable secret
    Enter enable password [sanfran]: cisco
    Enter virtual terminal password [sanjose]:
    Configure SNMP Network Management? [no]:
    Configure IP? [yes]:
        Configure IGRP routing? [yes]:
          Your IGRP autonomous system number [1]:
                                        *
                                        *
                                        *
```

6.3.11 PARAMETROS DEL MODO SETUP DE INTERFAZ

Después de haber configurado los parámetros globales, continuamos con la configuración de los parámetros de cada interfaz instalada, como lo muestra la figura 6.21.

FIGURA 6.21

```
Configuring interfaces parameters:

Configuring interface TokenRing0
    Is this interface in use? [no]:

Configuring interface Serial0
    Is this interface in use? [yes]:
Configure IP on this interface? [yes]:
Configure IP unnumbered on this interface?: [no]:
    IP address for this interface: 172.16.97.97
    Number of bits in subnet field [0]:
    Class B network is 172.16.0.0, 0 subnet bits: mask is 255.255.0.0
Configure Novell on this interface? [yes]: no

Configuring interface Serial1:
    Is this interface in use? [yes]: no
```

Si se elige una interfaz no configurada, el System Configuration Dialog pasará los prompts subsecuentes relacionados con esa interfaz. Si se elige configurar una interfaz,

introducir los valores de cada configuración en cada prompt. Se puede configurar cada protocolo que se habilitó en la sección global para cada interfaz. Se puede observar que algunas interfaces se pueden habilitar para múltiple protocolos, mientras que otros pueden estar corriendo con un solo protocolo.

Para un ainterfaz serial (Serial0), el sistema busca una dirección IP para este puerto y si está configurada con IP unnumbered[38].

Usualmente la razón para usar IP unnumbered es para conservar direcciones IP. Esto puede ser innecesario al utilizar una dirección IP explícita para un enlace serial que conecta con otra interfaz serial.

6.3.12 REVISANDO EL SCRIPT DEL MODO SETUP

Cuando se completan los cambios, el comando *setup* muestra una escritura de las configuraciones que fueron creadas durante la sesión de *setup*. Ver figura 6.22.

FIGURA 6.22

```
The following command configuration script was created:

Hostname P1R1
enable secret 5 $1$g722$dg2UV
enable password sanfran
line vty 0 4
     password sanfran
     snmp-server community
!
ip routing
no decnet routing
no xns routing
novell routing
no apollo routing
appletalk routing
no clns routing
no vines
no bridge
no mop enable
--More--
```

```
Interface TokenRing0
   Shutdown
    !
    interface serial0
    ip address 172.16.97.97 255.255.0.0

    interface serial1
    shutdown
!
router igrp 200
network 172.16.0.0
!
end

Use this configuratiobn? [yes]:  yes
[OK]
Use the enable mode "configure" command  to modify this
configuration
```

El Script permite una vista de los cambios antes de que sean guardados en NVRAM.

Los comandos son divididos en secciones globales y de interfaz. Notar en la figura 6.22 que las interfaces *TokenRing0* y *Serial1* están dadas de baja. Para utilizar estas interfaces se debe entrar en el modo de configuración de interfaz y escribir *no shutdown* para habilitar

[38] La interfaz IP UNNUMBERED toma prestada una dirección IP de otra interfaz ya configurada en el ruteador, de tal modo que hay conservación de direcciones.

esas interfaces. Si esas interfaces nunca han sido configuradas, se debe utilizar el comando *configure* e introducir los valores apropiados para hacer esas interfaces operacionales.

Al final, el *setup* preguntará si se quiere utilizar esa configuración; si se escribe"yes" el archivo de configuración es cargado en el almacén de funcionamiento y una copia es almacenada en la memoria de respaldo de NVRAM. Este es el tiempo en que el ruteador almacenará automáticamente una configuración en NVRAM.

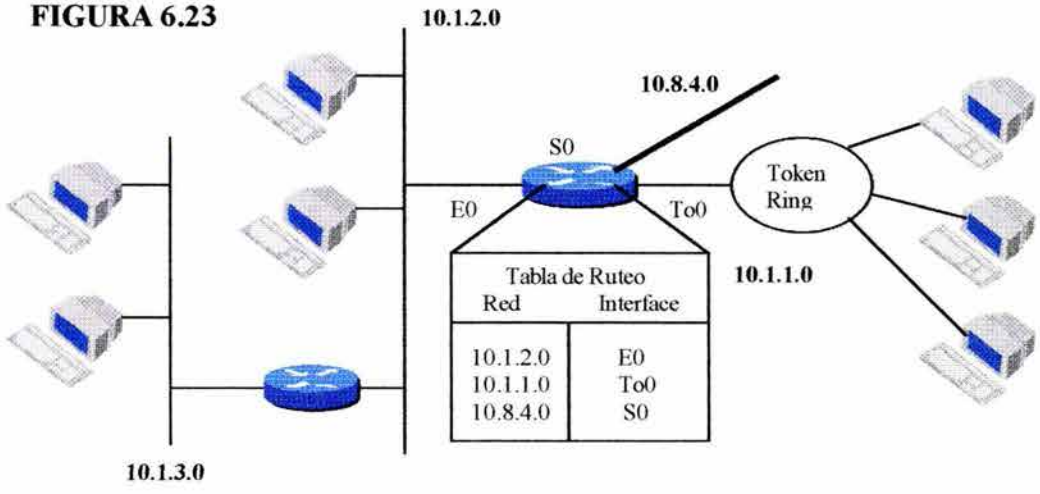
6.4 MECANISMOS BASICOS Y COMANDOS DE RUTEO IP

Esta sección introduce el concepto de ruteo IP y comandos requeridos para crear rutas y tablas de ruteo.

6.4.1 CREANDO UNA TABLA DE RUTEO IP INICIAL

Los dispositivos se comunican unos con otros por medio de rutas. Una ruta es un camino en el cual un dispositivo envia y el otro dispositivo recibe. Las rutas pueden ser manualmente configuradas por el administrador; los dispositivos pueden enviar pruebas para descubrir la manera en que se puede obtener un destino; o los dispositivos pueden recibir actualizaciones acerca de los ruteadores que están disponibles. Una vez que el dispositivo obtiene información acerca de una ruta, el dispositivo almacena la información de la ruta en una tabla de ruteo, como muestra la figura 6.23.

FIGURA 6.23



Si el dispositivo está en la misma red que el dispositivo que envía, el dispositivo que envía simplemente transmite el datagrama directamente al destino. Cuando el destino no está en la misma red local, el dispositivo que envía transmite el datagrama al ruteador. Para

enviar el datagrama, primero el ruteador debe saber qué ruteadores están conectados a la red local.

Basado en la red mostrada en la figura 6.23, un paquete destinado a la red 10.1.3.0 podrá ser caido. Cuando un ruteador empieza a funcionar, conoce sólo acerca de las redes que están conectadas directamente a sus interfaces. Cada conexión del ruteador a la red es configurada con una dirección IP y una máscara, las cuales son asociadas a las interfaces del ruteador. El Cisco IOS Software aprende acerca de estas direcciones IP y su máscara correspondiente desde la entrada de la información de configuración, tal como un administrador de red.

6.4.2 ENTENDIENDO LA MANERA EN QUE EL RUTEO IP APRENDE DESTINOS

Los ruteadores aprenden rutas o destinos por tres modos:

- Rutas estáticas: Manualmente definidas por el administrador de red como una sola ruta el destino; útil para controlar seguridad y reducir el tráfico.
- Rutas por defecto: Manualmente definidas por el administrador de red como una ruta a tomar cuando una ruta al destino no se conoce.
- Rutas aprendidas dinámicamente: Los ruteadores aprenden las rutas o destinos por recepción de actualizaciones periódicas de otros ruteadores.

El ruteo IP es automáticamernte habilitado en el Cisco IOS Software. Para deshabilitar el ruteo se debe introducir el siguiente comando en el modo de configuración global:

Router(config)# no ip routing

Cuando el ruteo IP está deshabilitado, el ruteador actuará como un host IP para paquetes IP. Para volver a habilitar el ruteo IP se debe introducir el siguiente comando en el modo de configuración global:

Router(config)#ip routing

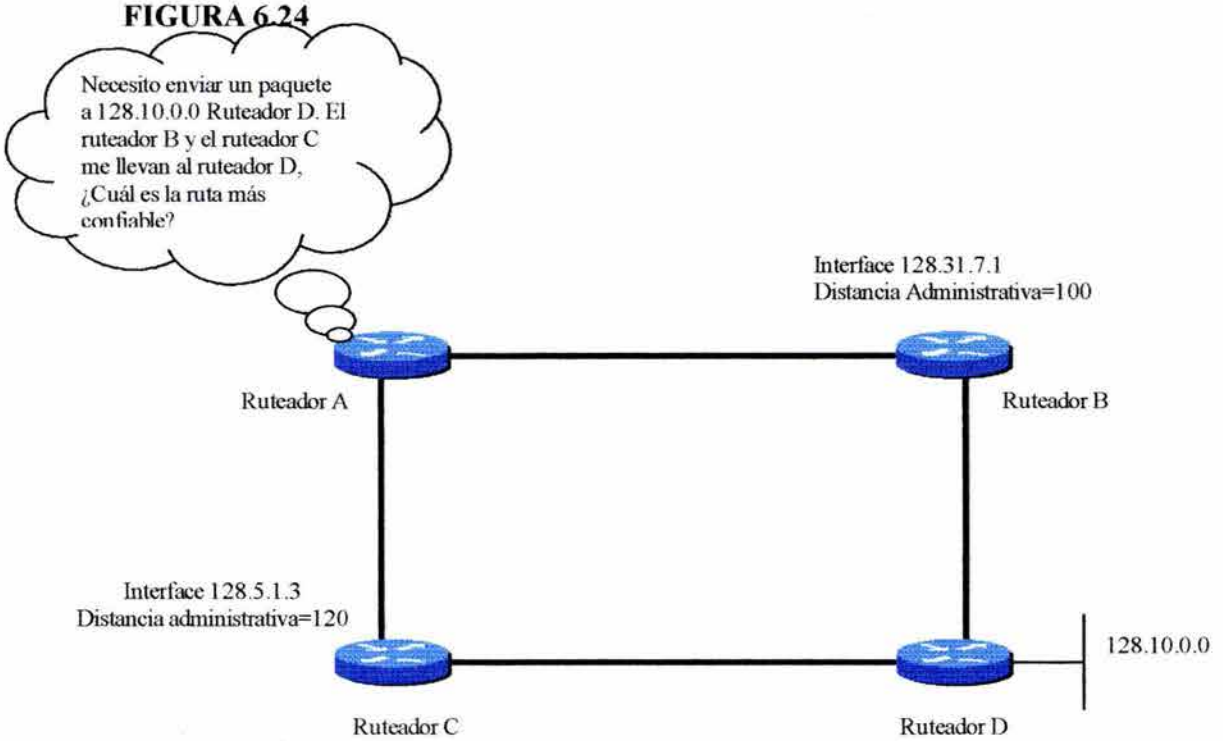
6.4.3 ESPECIFICANDO VALORES DE DISTANCIA ADMINISTRATIVA

Una distancia administrativa es un rango de confianza de la fuente de la información de ruteo, tal como un ruteador individual o un grupo de ruteadores. Una distancia administrativa es un entero de 0 a 255. En general, el valor más alto es el valor de confianza más bajo. Una distancia administrativa de 255 no puede ser del todo confiable y debe ser ignorada.

Especificar los valores de la distancia administrativa habilita al Cisco IOS Software para discriminar entre fuentes de información de ruteo, como lo muestra la figura 6.24. Para

obtener la red 128.10.0.0, el ruteador A elegirá enviar el paquete al ruteador B porque el ruteador B tiene la distancia administrativa menor que el ruteador C.

FIGURA 6.24



El software siempre selecciona la ruta cuyo protocolo de ruteo tiene la distancia administrativa menor.

La siguiente tabla muestra las distancias administrativas por defecto de algunas fuentes de información de ruteo.

FUENTE DE RUTEO	DISTANCIA POR DEFECTO
Interfaz conectada	0
Ruta estática	1
IGRP	100
RIP	120
Desconocido	255

Si un ruteador tiene los protocolos IGRP y RIP habilitados, el Cisco IOS Software utilizará información derivada de IGRP porque la distancia administrativa por defecto de IGRP es menor que la distancia administrativa de RIP e ignora la información derivada de RIP. Sin embargo, si se pierde la información derivada de IGRP, el software utiliza la información derivada de RIP hasta que la información derivada de IGRP aparezca.

6.4.4 CONFIGURADO RUTAS ESTATICAS

Las rutas estáticas son rutas definidas por el usuario que causan movimiento de paquetes de una fuente a un destino por un camino en particular. Las rutas estáticas son importantes cuando el Cisco IOS Software no puede construir una ruta a un destino. Los ruteadores pueden sólo enviar paquetes a rutas conocidas y si el ruteador no puede aprender dinámicamente una ruta, la entrada estática puede ser utilizada para habilitar al ruteador para enviar un paquete. Las rutas estáticas también pueden ser para especificar un *gateway* para el cual todos los paquetes ruteables son enviados. Este *gateway*, el cual es un ruteador, es utilizado como última alternativa para manipular el paquete.

El ruteo dinámico es típicamente preferido porque el ruteo estático puede ser poco manejable en una red compleja porque el administrador debe hacer algunos cambios manuales. En redes pequeñas y sencillas, sin embargo, el ruteo estático proporciona precisión y control sobre la red sin mucho trabajo.

Para configurar una ruta estática, se debe introducir el comando *ip route* en el modo de configuración global. Una ruta estática permite configuración manual de una tabla de ruteo.
Para completar los parámetros del comando *ip route*, está lo siguiente:

ip route red [máscara] {dirección|interfaz} [distancia] [*permanente*]

donde los parámetros tiene los siguentes significados:

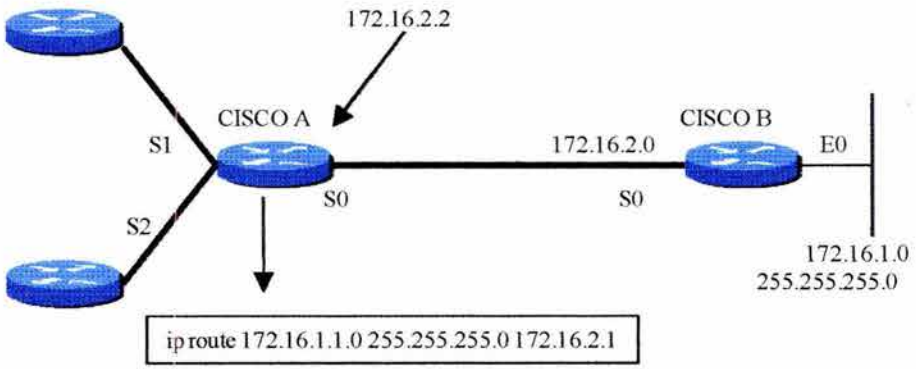
- Red: Red destino o subred.
- Máscara: Máscara de subred.
- Dirección: Dirección del siguiente ruteador.
- Interfaz: Nombre de la interfaz usada para obtener la red destino.
- Distancia: Distancia administrativa
- Permanente (opcional): Especifica que la ruta no será removida si la interfaz se cae.

Si la máscara es omitida en el comando *ip route*, el ruteador asume que puede usar la máscara por defecto. La figura 6.25 provee un ejemplo de ruta estática basada en el siguiente comando *ip route*:

Router(config)# *ip route* 172.16.1.0 255.255.255.0 172.16.2.1

En este ejemplo el commando *ip route* identifica una ruta estática; 172.16.2.1 es la dirección IP del próximo ruteador.

FIGURA 6.25



La asignación de una ruta estática para alcanzar un *área stub* es apropiada para el ruteador Cisco A porque hay solo un camino para alcanzar esa red. Un *área stub* es una que sólo tiene una conexión a otra red. Si una red se conecta a más de una red y permite tráfico a través de ésta, esa red es llamada *Transit Network*.

La asignación de una ruta estática del ruteador Cisco B a la nube de redes también es posible. Sin embargo, la asignación de una ruta estática es requerida para cada destino de red. Asi que una ruta por defecto es más apropiada.

IMPORTANTE:

Se puede tener más de un protocolo de ruteo IP operando en el mismo ruteador al mismo tiempo. Cada ruta es distinguida por la ruta administrativa. El número más bajo es la mejor ruta. Esto básicamente es una medición en la manera en la cual se considera una ruta como buena.

6.4.5 CONFIGURANDO RUTEADORES POR DEFECTO

Los ruteadores no pueden conocer las rutas hacia otras redes. Para establecer un ruteador por defecto, se debe de entrar en el modo de configuración:

Router(config)#*ip default-network* número-de-red

donde el número de red es igual a la dirección IP de la red o el número de subred definida por defecto.

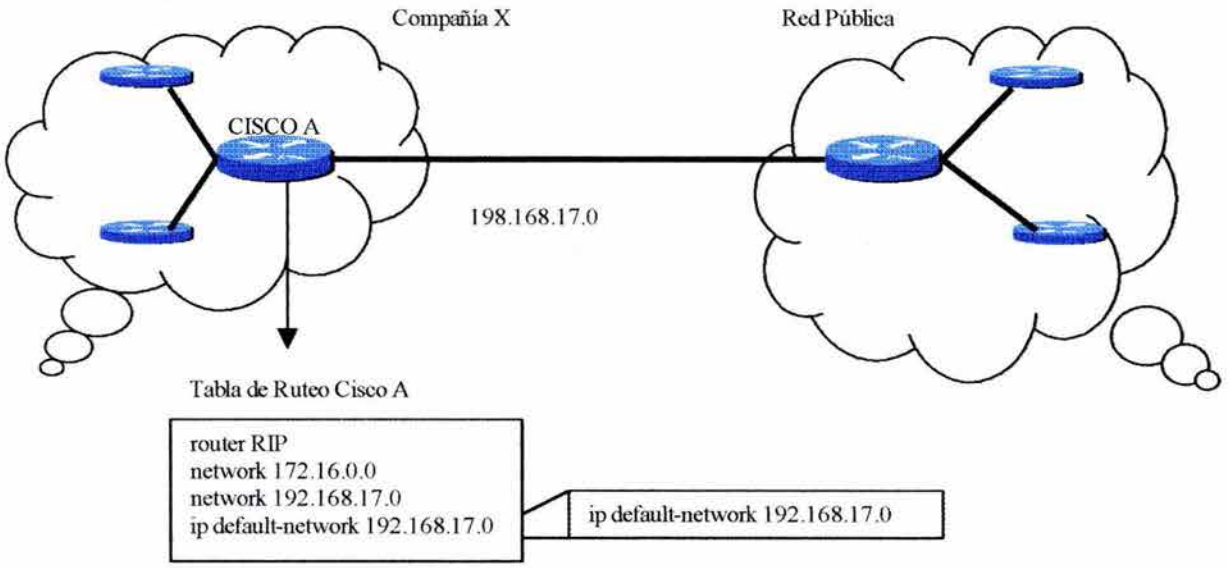
Cuando una entrada para un destino no existe en la tabla de ruteo, el paquete es enviado a una red por defecto, así que la red por defecto debe existir en la tabla de ruteo. Un beneficio de las rutas por defecto es que pueden reducir el tamaño de la tabla de ruteo.

Se debe utilizar el número de red por defecto cuando se necesita una ruta pero cuando se tiene sólo información parcial del destino. Como el ruteador no tiene un completo conocimiento de todos las redes destinos, puede utilizar un número de red por defecto para indicar la dirección a tomar por números de redes desconocidos. Además de las direcciones IP, el IP Routing Information Protocol (RIP) utiliza 0.0.0.0 como ruta por defecto.

En el ejemplo mostrado en la figura 6.26, en el comando global *ip default-network* 192.168.17.0 define la red de Clase B 192.168.17.0 como una ruta destino para paquetes que no tienen una entrada de ruta en la tabla de ruteo.

Para prevenir actualizaciones indeseadas desde la red pública, la compañía X podría instalar un Firewall en el ruteador A. Para agrupar esas redes que compartirán la estrategia de ruteo de la compañía X, el ruteador A podría implementar un número de sistema autónomo.

FIGURA 6.26



6.4.6 AGRUPANDO EN SISTEMAS AUTÓNOMOS

En la figura 6.26 podemos ver cómo la compañía X utiliza un ruteador por defecto a la red pública. Cómo se mencionó antes se pueden agrupar los ruteadores en un *sistema autónomo*. Un *sistema autónomo* es un conjunto de ruteadores y redes bajo la misma administración. Un *sistema autónomo* puede consistir de un ruteador conectado directamente a una red LAN o a Internet o puede ser una red corporativa que conecta varias redes locales a un backbone corporativo.

El *sistema autónomo* presenta una vista consistente de ruteo al mundo externo. Para un ruteador que pertenezca a un sistema autónomo, todos los ruteadores en ese sistema deben estar:

- Interconectados.
- Deben correr el mismo protocolo de ruteo.
- Deben ser asignados al mismo número de sistema autónomo.

Network Information Center (InterNIC) un único *sistema autónomo* para las empresas. Este *sistema autónomo* es un número de 16 bits. Un protocolo de ruteo como IGRP requiere que se especifique el número único de *sistema autónomo* asignado en la configuración. InterNIC asignará un número de sistema autónomo **si y sólo si** la organización utilizará un Protocolo de Ruteo Exterior, tal como Border Gateway Protocol (BGP).

6.4.7 UTILIZANDO PROTOCOLOS DE RUTEO INTERIOR Y EXTERIOR

El criterio de diseño para un protocolo de ruteo interior requiere de encontrar la mejor ruta a través de la red, en otras palabras, la métrica y la manera en que esa métrica es utilizada en los elementos más importantes en un protocolo de ruteo interior.

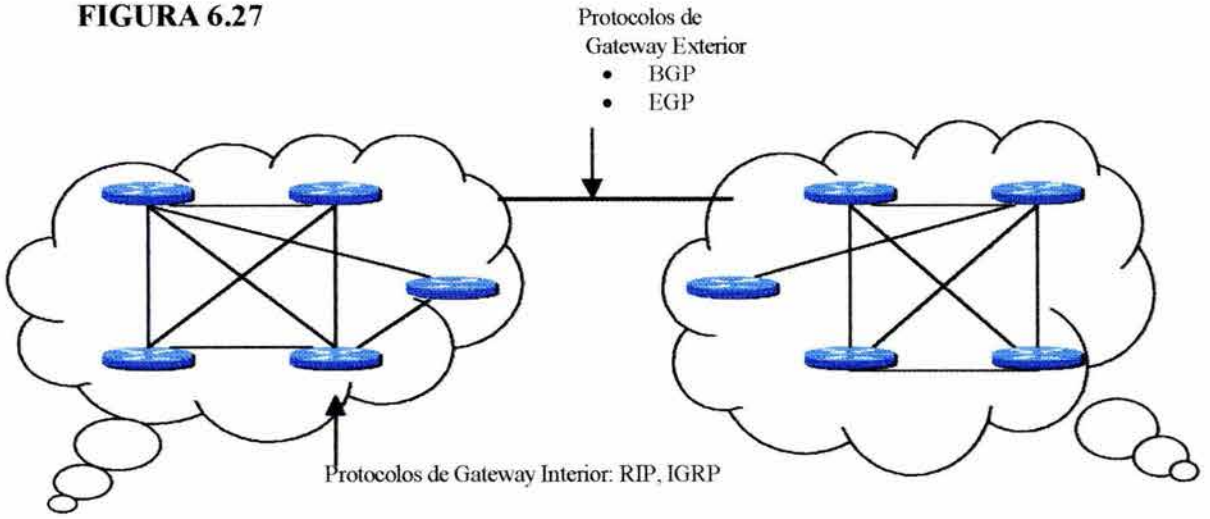
Los protocolos exteriores son utilizados para intercambiar información de ruteo entre redes que no comparten alguna administración en común. Los protocolos de gateway exteriores requeren de los siguientes tres conjuntos de información antes de empezar el ruteo:

- Una lista de los ruteadores vecinos o servidores de acceso con los cuales se pueda intercambiar información de ruteo.
- Una lista de redes para publicarse como alcanzable.
- Un número de *sistema autónomo* para el ruteador local.

Como lo mustra la figura 6.27, los protocolos de gateway exteriores son:

- Border Gateway Protocol (BGP)
- Exterior Gateway Protocol (EGP)

FIGURA 6.27



Un protocolo de ruteo exterior debe de aislar los *sistemas autónomos*. Básicamente otro *sistema autónomo* es manejado por otro personal. Como no se tiene el control sobre la manera en que la red es configurada, se necesita proteger la red de errores que pueden ocurrir por una mala configuración.

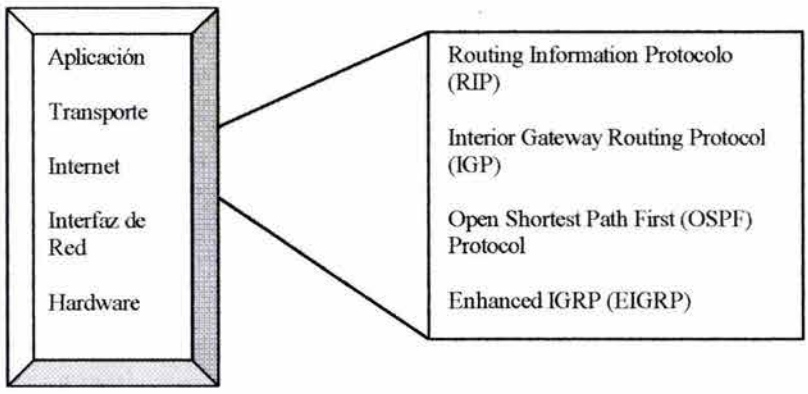
6.4.7.1 PROBLEMAS DE PROTOCOLO DE RUTEO

El problema más común que podría ocurrir es el *loop de ruteo* o problema de convergencia. Este problema podrá ser propagado en la red como alguna actualización especificando cambios en la métrica. Por lo tanto, el protocolo de ruteo exterior está tentado a eliminar esta conexión a la red.

6.4.7.2 PROTOCOLOS DE RUTEO INTERIOR

En la capa de Internet del conjunto de protocolos TCP/IP, como lo muestra la figura 6.28, un ruteador puede utilizar un protocolo de ruteo IP para lograr el ruteo a través de la implantación de un algoritmo de ruteo específico.

FIGURA 6.28



Los protocolos interiores son utilizados para redes de ruteo que están bajo una misma administración. Los protocolos de gateway interior deben ser especificados con una lista asociada de redes antes de empezar las actividades de ruteo. Un proceso de ruteo escucha actualizaciones de otros ruteadores en esas redes y sus broadcasts de su misma información de ruteo en esas mismas redes. El Cisco IOS Software soporta los siguientes protocolos de ruteo interior:

- Rountig Information Protocol (RIP)
- Internet Gateway Routing Protocol (IGRP)
- Enhanced IGRP (EIGRP)
- Open Shortest Path First (OSPF)
- Intermediate System- to- Intermediate System (IS-IS)

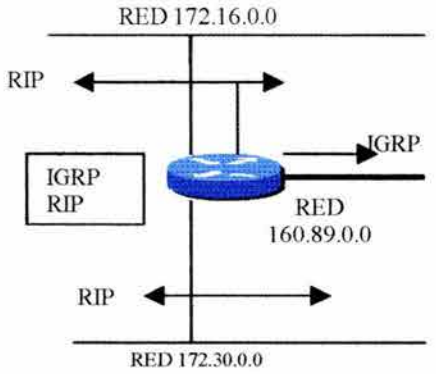
6.4.8 COMPLETANDO LAS TAREAS DE CONFIGURACION DE RUTEO IP

La selección de IP como protocolo de ruteo involucra la configuración de parámetros globales y de interfaz. Los parámetros globales incluyen:

- Seleccionar un protocolo de ruteo (ver figura 6.29).
- Asignar números de red IP sin especificar los valores de subred.

Los parámetros de interfaz son para asignar direcciones de interfaz específicas y la máscara de subred apropiada.

FIGURA 6.28



El ruteo dinámico utiliza broadcast y multicast para comunicarse con otros ruteadores. Las métricas de ruteo ayudan a los otros ruteadores a encontrar la mejor ruta a cada red.

6.4.9 CONFIGURANDO RUTEO DINAMICO

Los comandos utilizados para configurar ruteo dinámico son: *router* y *network*.

Router(config)#*router* protocolo [palabra clave]

donde los parámetros especifican lo siguiente:

- Protocolo: RIP, IGRP, OSPF o EIGRP.
- Palabra Clave: Por ejemplo, número de sistema autónomo que es utilizado con esos protocolos que requieren de un sistema autónomo como IGRP.

El comando *network* es requerido porque permite el proceso de ruteo para determinar las interfaces que participarán en el envio y recepción de actualizaciones de ruteo. El comando *network* también permite al ruteador publicar esa red. Esto forma lo siguiente:

Router (config-router)# *network* numero de red

donde el número de red especifica una red directamente conectada.

El número de red debe estar basado en el número de redes de InterNIC, no en el número de subredes individuales. El número de red también debe identificar una red a la cual el ruteador está fisicamente conectado.

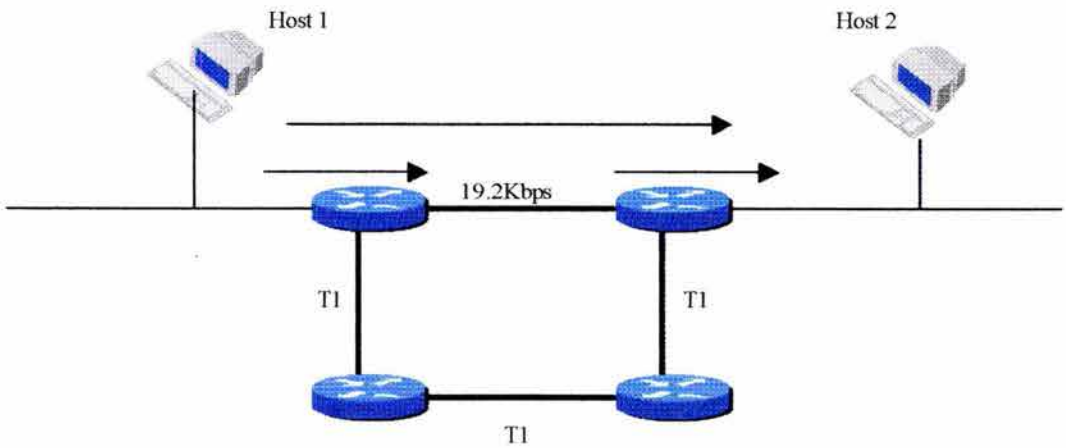
6.4.10 CONFIGURANDO RIP

Routing Information Protocol (RIP) fue originalmente especificado en RFC 1080. Las características claves de RIP incluyen los siguientes:

- Es un protocolo de vector distancia.
- La cuenta de saltos es utilizada como métrica para la selección de una ruta.
- El número máximo de saltos permitidos con 15, 16 es considerado inalcanzable.
- Las actualizaciones son broadcast cada 30 segundos.
- RIP tiene la habilidad de balanceo de carga sobre múltiples rutas.

El balanceo de cargas habilita al ruteador a utilizar dos o más rutas de igual costo para alcanzar un destino. En los ruteadores Cisco, el balanceo de cargas por RIP es habilitado por la definición de un número máximo de rutas paralelas instaladas en la tabla de ruteo. Si el número máximo de rutas está fijo en 1, el balanceo de cargas está deshabilitado. El RIP por defecto tiene balanceo de cargas habilitado. En la figura 6.29 el paquete del host 1 al host 2 podría cruzar por el enlace de 19.2Kbps porque la ruta utiliza la cuenta de saltos más baja.

FIGURA 6.29



Desafortunadamente, en este ejemplo, la ruta seleccionada no es la mejor ruta disponible. RIP fue desarrollado en una red homogénea. Si todo es conectado por un medio

simple, las métricas basadas en ancho de banda reducen la cuenta de saltos. Pero a diferentes tipos de medio, la métrica de cuentas de saltos de RIP no puede identificar consistentemente la mejor ruta como en este ejemplo.

6.4.10.1 COMANDOS DE CONFIGURACION DE RIP

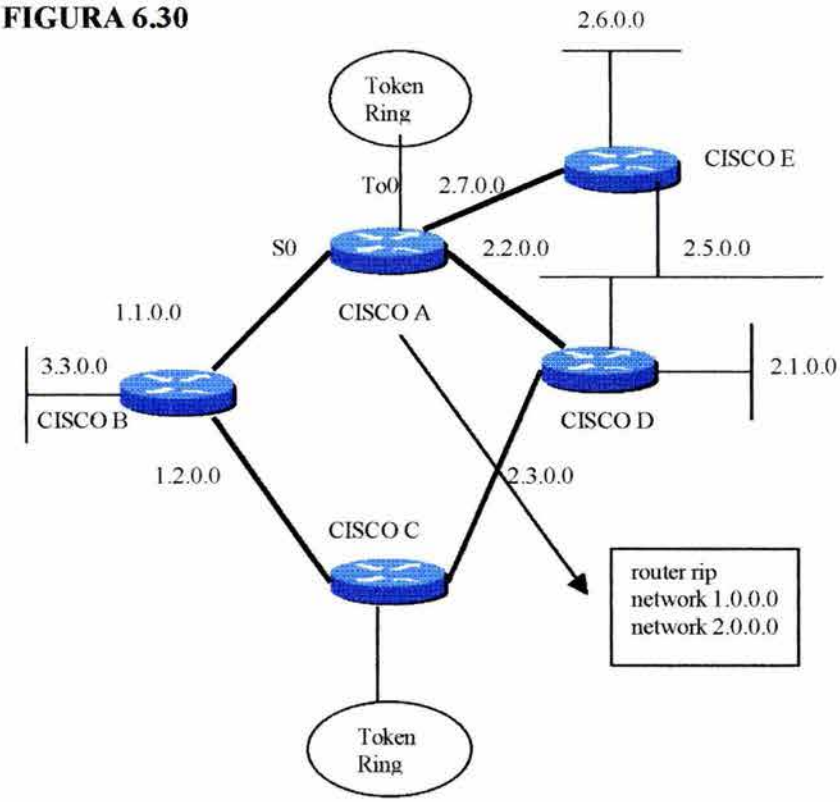
Los comandos utilizados para configurar un ruteador RIP son:

Router(config)#*router rip*
Router(config-router)#*network* número de red

El comando *router rip* selecciona a RIP. El comando *network* asigna una dirección IP para la red a la cual el ruteador está directamente conectado. El proceso de ruteo asociará interfaces con las direcciones IP apropiadas.

El estado de *network* no contiene información de subredes. Las redes son conectadas directamente y son especificadas como números de red de clase A, B o C. La figura 6.30 muestra configuración del ruteador Cisco A.

FIGURA 6.30



- router rip.- Selecciona RIP como protocolo de ruteo.
- network 1.0.0.0.- Especifica una red conectada directamente.
- network 2.0.0.0.- Especifica una red conectada directamente.

Las interfaces del ruteador Cisco A conectadas a las redes 1.0.0.0 y 2.0.0.0 enviarán y recibirán actualizaciones RIP. Estas actualizaciones de ruteo permitirán al ruteador aprender la tecnología de red.

El comando *network* da al protocolo de ruteo permiso para publicar las subredes conectadas al ruteador vecino. Sin el comando *network*, nada es publicado. Con el comando *network*, el ruteador publicará cada subred con clase A, B o C especificada en la configuración.

6.4.10.2 VISTA DE LA INFORMACIÓN DE RIP

Hay tres comandos que se utilizan para obtener una vista de la información RIP:

- show ip protocol
- show ip route
- debug ip rip

El comando *show ip protocol* despliega valores acerca de los temporizadores de ruteo e información de red asociada con el ruteador, como lo muestra la figura 6.31. Se utiliza esta información para identificar el ruteador sospechoso de entregar mala información de ruteo.

El rutedor de la figura 6.31 envía actualizaciones de información de la tabla de ruteo cada 30 segundos (este intervalo es configurable). Han pasado 17 segundos desde que se envió la última actualización, la próxima actualización será en 13 segundos. El ruteador también está inyectando rutas para redes en la línea *Routing for networks.*

FIGURA 6.31

```
Router> show ip protocol
Routing Protocol is "rip"
    Sending update every 30 seconds, nest due in 13
seconds
    invalid after 180 seconds, hold down 180, flushed after 240
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
Redistributing: rip
Routing for networks
    183.8.0.0
    144.253.0.0
Routing Information Sources:
Gateway          Distance      Last Update
    183.8.128.12      120        0:00:14
    183.8.64.130      120        0:00:19
    183.8.128.130     120        0:00:03
Distance: (default is 120)
```

El comando *show ip route* despliega el contenido de la tabla de ruteo IP, como lo muestra la figura 6.32.

FIGURA 6.32

```
Router> show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – Mobile, B – BGP
       D – EIGRP, Ex – EIGRP, O – OSPF. IA – OSPF inter area
       EI – OSPF extenal type 1, E2 – ISPF external type 2, E- EGP
       I – IS-IS. L1 - IS-IS level-1, L2 – IS-IS level –2, * - candidate default

Geteway of last resort is no t set

     144.253.0.0 is subnetted (mask is 255.255.255.0), 1 subnet
C    144.253.100.0 is directly connected, Ethernet1

R    153.50.0.0 [120/1] via 183.8.128.12, 00:00:09, Ethernet0
     183.8.0.0 is subnetted (mask is 255.255.255.128), 4 subnets
R    183.8.0.128 [120/1] via 183.8.128.130, 00:00:17, Serial0
     [120/1] via 183.8.64.130, 00:00:17, Serial1
C    183.8.128.0 is directly connected, Ethernet0
C    183.8.64.128 is directly connected, Serial1
C    183.8.128.128 is directly connected, Serial0
```

La tabla de ruteo contiene entradas para todas las redes y subredes conocidas y contiene un código que indica la manera en que la información fue aprendida.
Los valores definidos son como sigue:

- C indica una red que fue configurada con comandos de red.
- R indica una entrada aprendida a través de RIP.
- Via se refiere al ruteador que informó acerca de la ruta.
- 00:00:09 que RIP actualiza cada 30 segundos.
- La distancia administrativa es de 120.
- La cuenta a saltos a 153.5.0.0 es 1

El comando *debug ip rip* despliega actualizaciones de ruteo IP, así como enviar y recibir. Como muestra la figura 6.33, la actualización es enviada por 172.8.128.130. Esto es reportado en dos ruteadores, uno es inaccesible porque su cuenta a saltos es mayor que 15. El comando *no debug ip rip* deshabilita el despliegue de actualizaciones de ruteo IP.

FIGURA 6.33

```
Router>debug ip rip
RIP protocol debugging is on
Router#
RIP: received update from 172.8.128.130 on Serial0
     172.8.0.128 in 1 hops
     172.8.64.128 in 16 hops (inaccessible)
Rip: received update from 172.8.64.130 on Serial1
     172.8.0.128 in 1 hops
     172.8.0.128.128 in 1 hops
RIP: received update from 172.8.128.130 on Serial0
     172.8.0.128 in 1 hops
     172.8.64.128 in 1 hops
RIP: sending update to 255.255.255.255 via Ethernet0 (172.8.128.2)
     subnet 172.8.0.128, metric 2
     subnet 172.8.64.128, metric 6
     subnet 172.8.128.128, metric 1
     network 10.253.0.0, metric 1
```

6.4.11 CONFIGURANDO IGRP

Internet Gateway Routing Protocol (IGRP) es un protocolo de ruteo de vector distancia desarrollado por Cisco a mitad de los años 80. IGRP tiene varias características que lo diferencian de otros protocolos de vector distancia, tales como RIP. Esas características son las siguientes:

- Escalabilidad: Algunas redes grandes están basadas en IGRP.
- Respuesta rápida a cambios de red: Diferente a otros protocolos de vector distancia, IGRP envía actualizaciones cuando la topología de la ruta cambia.
- Métrica sofisticada: IGRP utiliza una métrica compuesta que provee una significante flexibilidad en la elección de una ruta. Retardo, ancho de banda, confiabilidad y carga son todos los factores en la desición de ruteo. IGRP puede ser utilizado para superar el límite de 15 saltos de RIP.
- Múltiples rutas: IGRP puede mantener arriba de 4 rutas desiguales entre la red fuente y la red destino. Las rutas múltiples pueden ser utilizadas para incrementar el ancho de banda disponible o para redundancia de rutas.

Se utiliza IGRP en redes que requieran de un protocolo de ruteo simple, robusto y escalable. IGRP también es útil cuando se trata de evitar el exceso de procesamiento del ruteador. Se puede redistribuir IGRP a RIP, OSPF y EIGRP; sin embargo, IGRP no soporta *Variable-Lenght Subnet Mask (VLSM)*[39].

6.4.11.1 ENTENDIENDO LA OPERACION DE IGRP

Los ruteadores que utilizan IGRP hacen actualizaciones periódicas de tablas de ruteo a ruteadores vecinos cada 90 segundos. IGRP provee un número de características para mejorar el desempeño y estabilidad y reducen la posibilidad de loops de ruteo. Como muestra la figura 6.34, esas características incluyen:

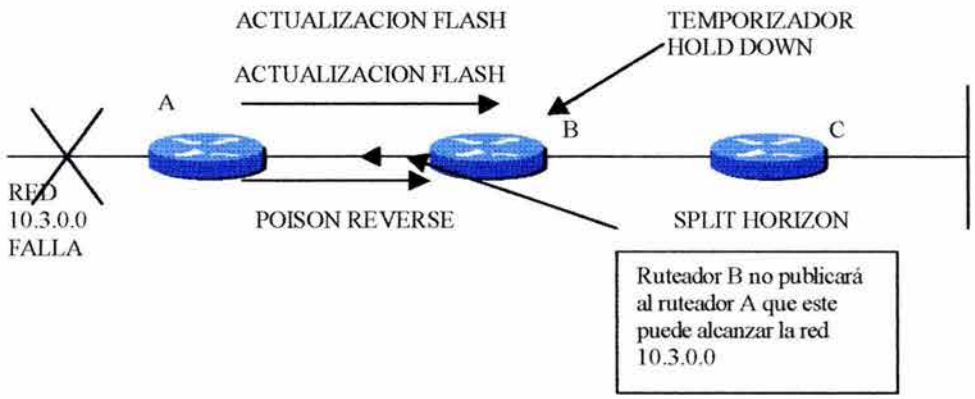
- Actualizaciones Flash: Además de sus actualizaciones periódicas de ruteo, IGRP utiliza actualizaciones Flash para la rápida convergencia del algoritmo de ruteo. Una actualización Flash es enviada cuando una topología de red cambia.
- Poison Reverse: Incremento en métricas de ruteo, generalmente indica los loops de ruteo. Las actualizaciones Poison Reverse son enviadas sí una métrica de ruteo ha incrementado en un factor de 1.1 o mayor.
- Hold Downs: IGRP tiene un temporizador Hold Down que previene los loops de ruteo mientras la convergencia tiene lugar. Una nueva ruta es aprendida hasta que le tiempo de Hold Down expira. Por defecto, el temporizador Hold Down es 3 veces el intervalo del tiempo de la actualización (90 segundos) más 10 segundos, o sea, 280 segundos. Los temporizadores pueden ser dehabilitados para mejorar el tiempo de convergencia, sin embargo, remover los temporizadores Hold Down incrementa la posibilidad de loops de ruteo. Se utiliza el comando *no metric holddown* para

[39] Permite el uso de algunas direcciones de host para definir una dirección de subred.

deshabilitar los hold downs. Como resultado después de que la ruta ha sido removida una nueva será aceptada inmediatamente.

- Split Horizon: En el capítulo 2 se mencionó que Split Horizon parte del hecho que no es útil enviar información de una ruta que regresa a la dirección de donde salió. En la figura 6.34, por ejemplo, el ruteador B no envía de regreso la información al ruteador A en relación con la red 10.

FIGURA 6.34



Periódicamente cada ruteador envía la tabla de ruteo entera a todos los ruteadores adyacentes. Cuando un ruteador recibe la tabla de ruteo, ésta la compara con la suya. Algunas nuevas rutas y destinos son añadidos a la tabla de ruteo. Las rutas en la tabla de ruteo son comparadas con las rutas existentes. Si una nueva ruta es mejor, la ruta existente será reemplazada.

Además de las actualizaciones periódicas cada 90 segundos, IGRP declara una ruta inaccesible si ésta no recibe una actualización del primer ruteador en el camino en tres periodos de actualizaciones (270 segundos). Después de siete periodos de actualización (630 segundos) la ruta es removida de la tabla de ruteo.

6.4.11.2 UTILIZANDO LA METRICA COMPUESTA DE IGRP

IGRP utiliza una métrica compuesta para identificar las rutas preferidas. La métrica compuesta IGRP es una cantidad de 24 bits que es una suma de los retardos del segmento y el ancho de banda más bajo del segmento para una ruta dada. Esta métrica combinada provee de gran exactitud cuando se elije una ruta al destino. En la figura 6.35, la ruta Token Ring y FDDI es la preferida para el enlace dual de 19.2Kbps.

La métrica IGRP no tiene la limitación de cuenta de saltos de RIP. Esta incluye los siguientes componentes:

- Ancho de banda: El ancho de banda más pequeño entra la fuente y el destino, expresado en kilobits.

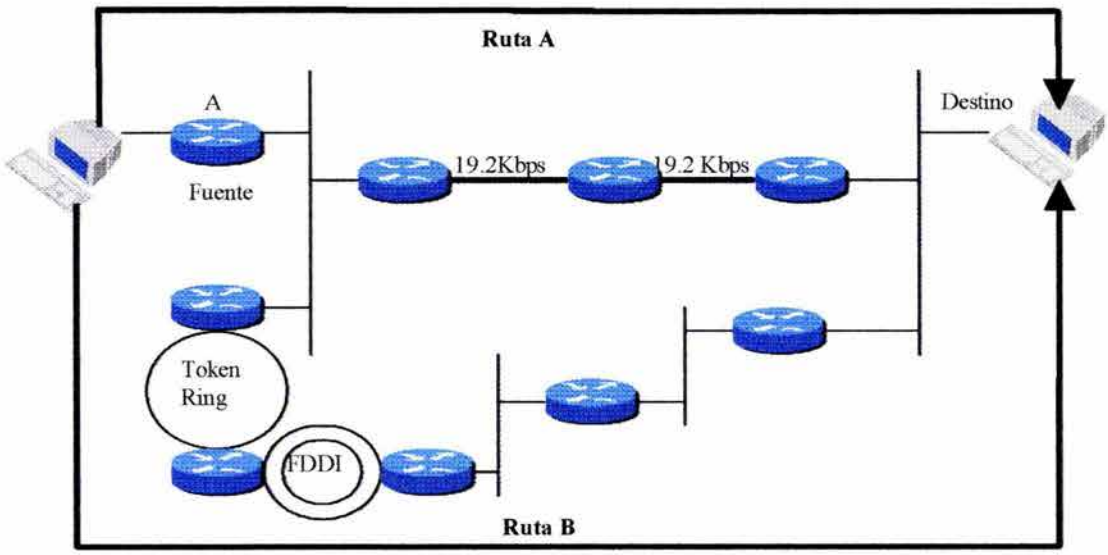
- Retardo: Retardo de interfaz acumulativa a lo largo de la ruta, expresado en microsegundos.
- Confiabilidad: Entre fuente y destino basado en keepalives, expresado en enteros de 0 a 255.
- Carga: Carga en el enlace entre la fuente y el destino, basado en bits por segundo.
- MTU: El valor de MTU más pequeño en la ruta, expresado en bytes.

La ruta que tiene el valor de la métrica más pequeño es la mejor ruta. Por defecto, sólo el ancho de banda y el retardo son utilizados por la métrica IGRP, pero se puede configurar para considerar la confiabilidad, la carga y el MTU. En la figura 6.35, por ejemplo, se puede configurar que el ruteador A envíe datos a través de la ruta A, en lugar de los lentos enlaces seriales. La ruta A incluye un enlace Token Ring de 16Mbps, un enlace FDDI de 100Mbps y algunos enlaces Ethernet de 10Mbps. Aunque hay más enlaces, la velocidad para atravesar la ruta A es mucho más rápida que los dos enlaces de 19.2Kbps.

PRECAUCION:

Ajustar los valores de la métrica de IGRP, pueden afectar dramáticamente el desempeño de la red. Se deben tomar las decisiones para ajustar los valores cuidadosamente.

FIGURA 6.35



6.4.11.3 CARACTERISTICA DE BALANCE DE CARGAS DE COSTO DESIGUAL

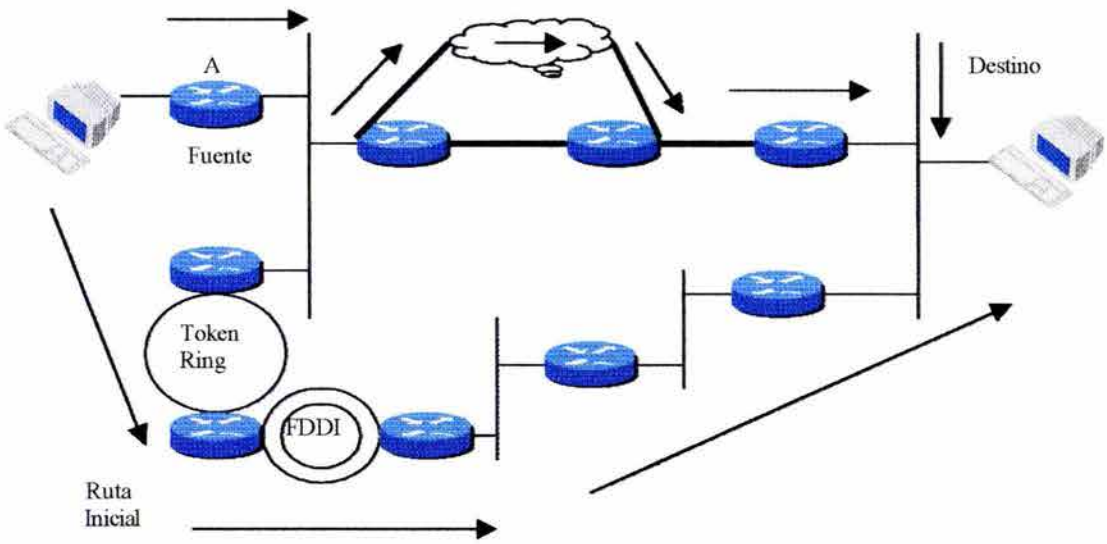
La métrica compuesta de IGRP soporta rutas múltiples entre la fuente y destino, ésta característica se llama *Balanceo de Carga de Costo Desigual* y permite redistribuir el tráfico entre arriba de cuatro rutas de costo desigual para proveer una alta confiabilidad.

Las siguientes reglas se aplican al balanceo de cargas de costo desigual:

- IGRP aceptará arriba de seis (cuatro es por defecto) rutas para un destino de red dado.
- El ruteador del próximo salto en algunas rutas debe de estar más cerca del destino que el del ruteador local.
- La métrica de ruta alternativa debe estar en variación especificada de la mejor métrica local.

Si esas condiciones son conocidas, la ruta es considerada factible y puede ser añadida a la tabla de ruteo. En la figura 6.36, por ejemplo, una segunda ruta desigual ha sido añadida a la ruta inicial entre la fuente y el destino.

FIGURA 6.36



Se puede utilizar el comando *default-metric* para cambiar la métrica por defecto.

6.4.11.4 CREANDO UN PROCESO DE RUTEO IGRP

Se utilizan los comandos *router igrp* y *netowrk* para crear un proceso de ruteo IGRP.

Router(config)# *router igrp* número de sistema autónomo
Router (config-router)#*network* numero de red

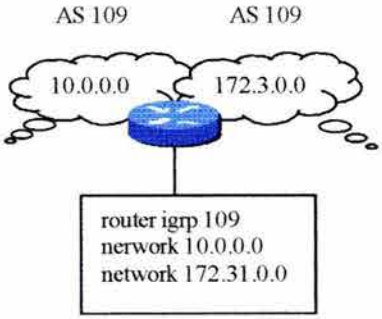
Por ejemplo para la figura 6.37, la siguiente configuración ha sido establecida:

- *router igrp* 109: Habilita el proceso de ruteo IGRP para el sistema autónomo 109.

- *network* 10.10.0.0: Asocia la red 10.10.0.0 con el proceso de ruteo IGRP.
- *network* 173.31.0.0: Asocia la red 172.31.0.0 con el proceso de ruteo IGRP.

IGRP envía actualizaciones a las interfaces en redes 10.0.0.0 y 172.31.0.0 e incluye información acerca de las redes 10.0.0.0 y 172.31.0.0.

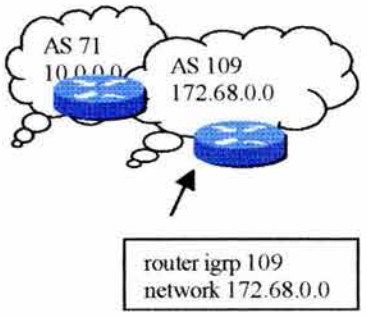
FIGURA 6.37



Aunque cada proceso de ruteo IGRP puede proveer información de ruteo a un solo sistema autónomo, el Cisco IOS Software, debe correr por separado un proceso IGRP y mantener una base de datos separada para cada sistema autónomo al cual sirve. Se pueden establecer diferentes sistemas autónomos cuando dos compañías se combinan, cuando se conectan con un solo proveedor de servicio o cuando se quiere aislar ciertos departamentos de la compañía.

Para configurar dos procesos de ruteo IGRP, se utilizan los comandos *router igrp* y *network* para definir cada proceso IGRP. Por ejemplo, en la figura 6.38, la red 10.0.0.0 está en el sistema autónomo 71 y la red 172.68.0.0 está en el sistema autónomo 109.

FIGURA 6.38



6.4.11.5 DESPLEGANDO INFORMACIÓN DE RUTEO IGRP

Se pueden utilizar los siguientes comandos para desplegar información de la configuración de ruteo IGRP y actualización de la tabla:

- show ip protocols
- show ip interfaces
- show ip route
- debug ip igrp transaction
- debug ip igrp events

El comando *show ip protocols* despliega parámetros, filtros e información de la red de todo el ruteador, como lo muestra la figura 6.39, se ve que el ruteador inyecta rutas para las redes 183.8.0.0 y 144.253.0.0.

FIGURA 6.39

```
Router>show ip protocols
Routing Protocol is "IGRP 300"
  Sending update every 90 seconds, next due in 55 seconds.
  Invalid after 270 secondas, hold down 280, flushed after 630
  Outgoing update filter lis of all interfaces is not set
  Incoming update filter lis of all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1. K2=0, K3=0, K4=0, K5=0
  IGRP maximum counthop 100
  IGRP maximum metric variance
  Redistribuition: igrp 300
Routing for networks
    183.8.0.0
    144.253.0.0
Routing Information Sources:
Gateway          Distance      Last Update
    144.253.100.1      120          0:00:52
    183.8.128.12       120          0:00:43
    183.8.64.130       120          0:00:02
Distance: (default is 100)
```

El comando *show interfaces* despliega los parámetros globales y el estado de las interfaces como en la figura 6.40.

FIGURA 6.40

```
Router>show ip interfaces
Ethernet0 is up, line protocol is up
  Internet address is 183.8.128.2 subnet mask is 255.255.255.128
  Broadcast address is 255.255.255.255
  Address determined by non-volatile
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast fordwarding is enabled
  Outogoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP SSE swotching is disabled
  Router Discovery is desabled
  IP output packet accounting is disabled
```

El Cisco IOS Software introduce una ruta directamente conectada en la tabla de ruteo si la interfaz es en la que el software puede enviar y recibir paquetes, cuando una interfaz está marcada como *up*. Si la interfaz no está en uso, es removida de la tabla de ruteo.

El comando *show ip route* despliega el contenido de una tabla de ruteo. La tabla contiene todas las redes y subredes conocidas y las métricas asociadas con cada entrada. Notar en la figura 6.41 que la información fue derivada de IGRP o de conexiones directas.

Se pueden utilizar los siguientes comandos para desplegar actualizaciones de tablas de ruteo.

Router#*debug ip igrp transaction* [dirección IP]
Router#*debug ip igrp events* [dirección IP]

El comando *debug ip igrp transaction* despliega información de las transacciones de ruteo IGRP. Si la dirección IP de un vecino IGRP es especificado, el resultado de la salida incluye mensajes describiendo actualizaciones de ese vecino y actualizaciones que el ruteador envía a ese vecino.

FIGURA 6.41

```
Router> show ip route
Codes: C – connected, S – static, I – IGRP, R – RIP, M – Mobile, B – BGP
       D – EIGRP, Ex – EIGRP EXTERNAL, O – OSPF. IA – OSPF inter area
       EI – OSPF extenal type 1, E2 – OSPF external type 2, E- EGP
       I – IS-IS. L1 - IS-IS level-1, L2 – IS-IS level –2, * - candidate default

Geteway of last resort is no t set

     144.253.0.0 is subnetted (mask is 255.255.255.0), 1 subnet
C    144.253.100.0 is directly connected, Ethernet1
I    133.3.0.0 [100/1200] via 144.253.100.200.1, 00:00:57, Ethernet1
I    153.50.0.0 0 [100/1200] via 1838.128.12, 00:00:05, Ethernet0
     183.8.0.0 is subnetted (mask 255.255.255,128), 4 subnets
I    183.8.0.128 [100/18067] via 183.8.64.130, 00:00:27, Serial1
     [100/18067] via 183.8.128.130, 00:00:27, Serial0
C    183.8.64.0 is directly connected, Ethernet0
C    183.8.64.128 is directly connected, Serial1
C    183.8.128.128 is directly connected, Serial0
I    172.16.0.0 [100/1200] via 144.253.100.1.1, 00:00:55, Ethernet1
I    192.3.63.0 [100/1300] via 144.253.100.1.200, 00:00:58, Ethernet1
```

Se utiliza el comando *no debug ip igrp transaction* para deshabilitar el debugging. Cuando hay algunas redes en la tabla de ruteo, desplegar toda la actualización para toda ruta puede saturar la consola y hacer al ruteador no funcionable. En este caso el comando *debug ip igrp events* es utilizado para deplegar un resumen de la información de ruteo IP. Este comando indica la fuente y el destino de cada actualización, así como el número de rutas en cada actualización.

Si la dirección IP de un vecino IGRP es especificado cuando se utiliza el comando *debug ip igrp events*, el resultado de la salida incluye mensajes describiendo actualizaciones desde ese vecino.

6.5 CONFIGURACION DE NOVELL IPX

Esta sección presenta una descripción de ruteo IPX y la manera en que los ruteadores se incorporan a las redes NetWare, protocolos IPX, direccionamiento IPX y encapsulación IPX.

6.5.1 RUTEADORES CISCO EN REDES NETWARE

En el ambiente de redes de hoy, ningún fabricante puede proveer todo el hardware y software requerido para soportar todas las necesidades de computación en los negocios. Como resultado, las mayoria de las redes incluyen una gran variedad de productos. Por esta razón, los ruteadores Cisco se encuentran también en redes NetWare aunque Novell ofrece productos de ruteo. Los Ruteadores Cisco ofrecen las siguientes características en los ambientes de redes Novell:

- Soporta un amplio rango de interfaces, incluyendo ISDN y ATM.
- Listas de Acceso[40] y filtros para IPX, RIP, SAP y NetBIOS.
- Protocolos de ruteo escalables incluyendo EIGRP y NLSP. Cisco utiliza una encapsulación de ruteo genérica para permitir transmisión de datagramas IPX a través de redes IP.
- Actualizaciones SAP y RIP y tamaños de paquetes configurables.
- Dial on Demand Routing (DDR)[41] para IPX y SPX. El tráfico es ruteado a través de por líneas donde sólo es necesario, limitando la cantidad de tiempo de uso de la línea.
- Características de diagnóstico y detección de averías. El comando *ping ipx* y algunos comandos *show* provee una información completa acerca del desempeño de IPX.

6.5.2 CONJUNTO DE PROTOCOLOS DE NOVELL NETWARE

Novell IPX es un conjunto de protocolos propietario que se deriva del conjunto de protocolos Xerox Network System (XNS). IPX es un datagrama, protocolo no orientado a conexión que no requiere de un reconocimiento para cada paquete. Es un protocolo de capa 3 que define direcciones de interred. En el ambiente NetWare, una estación de trabajo es llamada *nodo*.

Novell NetWare utiliza lo siguiente:

- IPX Routing Information Protocol (RIP), para facilitar el intercambio de ruteo de información.
- Service Advertisement Protocol (SAP), para publicar los servicios de red.
- Netware Core Protocol (NCP), para proveer conexiones de cliente/servidor y aplicaciones.
- Sequence Packet Exchange (SPX), es un servicio de capa 4 orientado a conexión.

Como una alternativa para RIP y SAP, Novell tiene un protocolo de ruteo de estado de enlace llamado *NetWare Link Services Protocol (NLSP)*. Como es un protocolo de estado de enlace, NLSP ofrece más confiabilidad y efectividad en el proceso de ruteo IPX RIP. Novell también tiene un directorio de servicio llamado *Novell Directory Service (NDS)*.

El conjunto de protocolos NetWare soporta todos los protocolos de acceso al medio. En la capa física y de enlace de datos son accesados a través de la interfaz Open Data-Link Interface (ODI).

---

[40] Las Listas de Acceso se revisarán en la siguiente sección.

[41] Técnica donde un ruteador puede automáticamente iniciar y cerrar una sesión de circuito switcheado como estaciones transmisoras.

De la capa 3 a la 7 son únicos para Novell:

- La capa 3 abarca IPX, un servicio de datagrama.
- SAP provee servicio para parte de la capa 3 y todos los servicios de la capa 4 a la capa 7.
- La capa 4 es caracterizada por SPX, el cual provee un servicio confiable orientado a conexión.

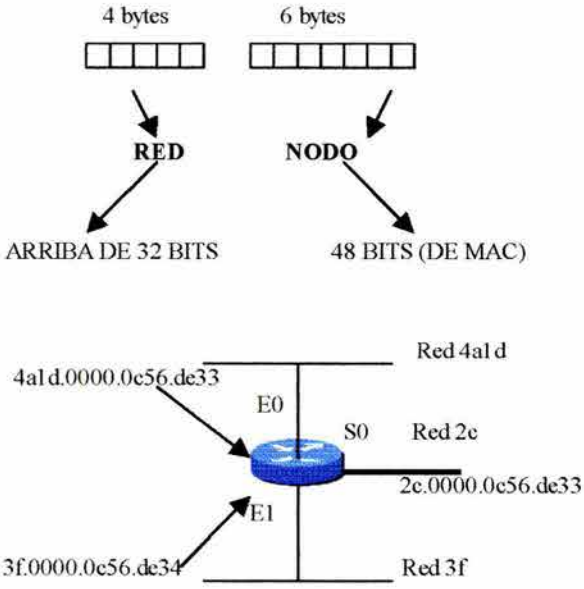
La emulación NetBIOS (Network Basic Input/Output System) desempeña tareas aplicables a la capa de Transporte y de sesión del modelo OSI. Novell NetWare define un paquete especial IPX llamado Type 20[42] para aplicaciones NetBIOS.

6.5.3 CARACTERÍSTICA CLAVE DE NOVELL NETWARE

Como muestra la figura 6.42, una dirección Novell IPX tiene 80 bits: 32 bits para el número de red y 48 bits para el número de nodo. El número de nodo contiene la dirección MAC de la interfaz. Novell IPX soporta múltiples redes lógicas en una interfaz individual; cada red requiere de un tipo de encapsulación simple.

Novell RIP es el protocolo de ruteo por defecto en los productos NetWare obsoletos; NLSP es el protocolo por defecto en NetWare 4.11 o superiores.

FIGURA 6.42



[42] Para que el NetBIOS funcione en ambientes NetWare, los ruteadores deben propagar cierto tipo de paquete broadcast. El paquete Type 20 esta diseñado para desempeñar la propagación de broadcast en algunos protocolos. Cuando un ruteador IPX recibe un paquete Type 20, reenvios los broadcasts a todas las interfaces, excepto a la interfaz de la que salío el broadcast.

Los clientes NetWare automáticamente descubren servicios de redes disponibles porque los usuarios NetWare y los ruteadores anuncien sus servicios utilizando broadcast SAP. El filtrado de publicación de un servicio es un punto crítico en las redes Novell. El tráfico SAP llega a ser excesivo y puede impactar severamente el ancho de banda disponible.

Un tipo de publicación SAP es *Get Nearest Server (GNS)* el cual habilita un cliente para localizar el servidor más cercana y abrir una sesión de red.

6.5.4 DIRECCIONAMIENTO NOVELL IPX

El direccionamiento Novell IPX utiliza dos partes: el número de red y el número de nodo.

- El número de red IPX puede ser de arriba de 4 bytes (8 dígitos hexadecimáles). Usualmente sólo los dígitos significativos son listados. Este número es asignado por el administrador de red. En la figura 6.43, la red IPX es es 4a1d. Otras redes son mostradas como 2c y 3f.
- El número de nodo IPX es de 6 bytes (12 dígitos hexadecimáles). Este número es usualmente obtenido de una interfaz de red. En la figura 6.42, el nodo IPX es 0000.0c56.de33 otro nodo de red es 0000.0c56.de34.

Notar en la figura 6.42 que el mismo número de nodo aparece para E0 y S0. Las interfaces seriales no tienen direccion MAC, entonces el ruteador crea este número de nodo para S0 utilizando la dirección MAC de E0. Cada interfaz retiene su propia dirección. El uso de direcciones MAC en la dirección lógica IPX elimina la necesidad para utilizar Address Resolution Protocol (ARP).

6.5.5 DETERMINANDO UNA DIRECCION IPX

Se debe utilizar una dirección de red IPX válida cuando se configura un ruteador Cisco. Como las redes NetWare son establecidas con direcciones IPX, se puede determinar una dirección IPX en redes ya establecidas. La dirección IPX se refiere al medio lógico; todos los ruteadores en el mismo medio comparten la misma direccion IPX.

El primer camino (y es recomendado) para encontrar la dirección IPX es preguntándole al administrador de NetWare. Hay que estar seguros que el administrador de NetWare especifica la direccion IPX para la misma red donde se quiera habilitar el ruteador. El ruteador debe utilizar la misma red que el servidor NetWare especificado por el administrador.

Si no se puede obtener la dirección IPX por medio del admistrador de NetWare, se puede utillizar una dirección directamente de un ruteador vecino. Elegir el más apropiado de varios métodos para hacer esto.

- Si el ruteador vecino es otro ruteador Cisco, se puede utilizar el comando *show cdp*.
- Se puede hacer una sesión Telnet al ruteador vecino, entrar en el modo apropiado y se despliega la configuración del ruteador vecino.
- Si el ruteador vecino es un ruteador Cisco se debe ser capaz de abrir una sesión y manejar la utilidad de configuración NetWare para determinar la direccion IPX.

En un ruteador Cisco se debe utilizar la misma dirección IPX como la dirección que ya existe en la red. Alternativamente si se tiene acceso al servidor de consola, se debe utilizar el comando NetWare *config*. El comando *config* despliega una ventana con la dirección IPX del segmento que le servidor NetWare comparte con el ruteador Cisco.

6.5.6 MULTIPLES ENCAPSULACIONES NOVELL

NetWare permite múltiples estructuras de frame de capa 2 para paquetes Novell IPX. Los ruteadores Cisco soportan todas las variaciones de framing. Por ejemplo, hay cuatro diferentes tipos de framing Ethernet, como lo muestra la figura 6.43. Cada tipo de encapsulación es apropiado en situaciones específicas:

- Ethernet 802.3: También llamado *Row Ehternet*. Por defecto para NetWare versiones 2 a 3.11.
- Ethernet 802.2: Por defecto para NetWare 3.12, 4 y 5.
- Ethernet II: Utilizado con TCP/IP y DECnet.
- Ethernet SAP: Utilizado con TCP/IP y DECnet.

Encapsulaciones múltiples pueden ser especificadas en la interfaz pero **si y sólo si** múltiples números de red han sido asignados. Aunque varios tipos de encapsulación pueden compartir la misma interfaz, clientes y servidores con diferentes tipos de información no pueden comunicarse directamente entre sí. La encapsulación por defecto en los ruteadores Cisco es *novell-ether* (Novell Ethernet_802.3).

FIGURA 6.43

	NOMBRE NOVELL IPX	NOMBRE CISCO IOS
ETHERNET	Ethernet_802.3 Ethernet_802.0 Ethernet_II Ethernet_SNAP	novell_ether sap arpa snap
TOKEN RING	Token-Ring Token-Ring_SNAP	sap snap
FDDI	FDDI_SNAP FDDI_802.2 FDDI_Raw	snap sap novell-fddi

Cuando se configura una red IPX se puede especificar un tipo de encapsulación por defecto en los servidores Novell o en los ruteadores Cisco. Como ayuda para especificar el tipo de encapsulación utilizar la tabla de la figura 6.43.

Cuando se configura el Cisco IOS Software para Novell IPX, se usa el nombre de Cisco para la encapsulación apropiada. Se debe estar seguro de que la encapsulación en los clientes, servidores y ruteadores en todos ellos corresponde.

Los dispositivos que utilizan diferentes tipos de encapsulación no pueden comunicarse entre ellos. Si no se tiene un tipo de encapsulación especificado cuando se configura un ruteador para IPX, el ruteador utilizará el tipo de encapsulación por defecto en sus interfaces.

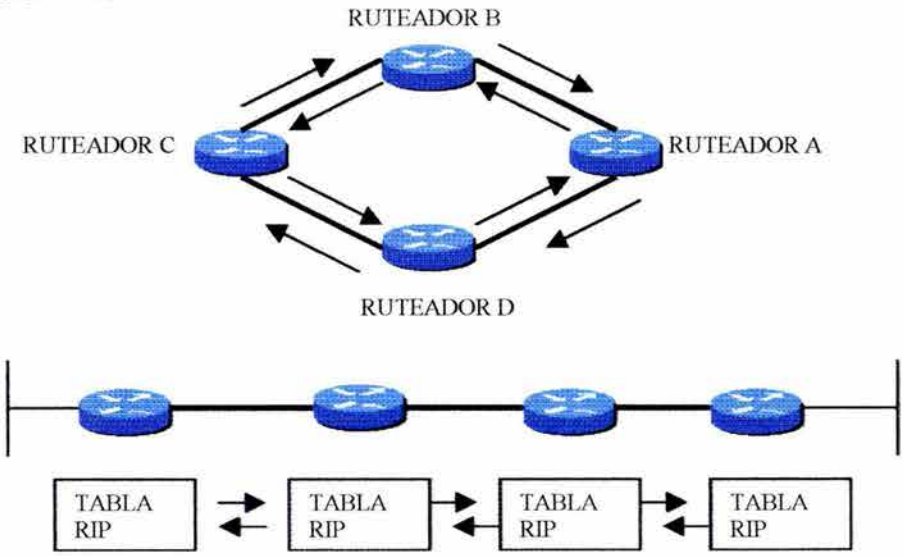
Los tipos de encapsulación por defecto en las interfaces de ruteadores son:

- Ethernet: novell-ether
- Token Ring: sap
- FDDI: snap
- Serial: HDLC

6.5.7 NOVELL UTILIZA RIP PARA RUTEO

IPX RIP utiliza dos métricas para tomar decisiones de ruteo: Ticks (una medida de tiempo) y cuenta de saltos. IPX RIP revisa esas métricas primero, para comparar las Ticks de rutas alternativas. Si dos o más rutas tienen el mismo valor de Tick, IPX RIP compara la cuanta de saltos. Si dos o más rutas tienen la misma cuenta a saltos, el rutador utilizará la edad o el tiempo de la entrada como un desempatadador; las entradas más recientes en las tablas serán las preferidas. Cada ruteador IPX envía broadcast de una copia de su tabla de ruteo a todas las redes directamente conectadas a él, como en la figura 6.44.

FIGURA 6.44



Sobre recibo de esos broadcasts, los ruteadores vecinos IPX añaden vectores distancia como se requirió antes de mandar la copia de su tabla de ruteo a otras redes. Un algoritmo de Split Horizon previene que la información de tablas de ruteo regrese de donde salió. La tabla de ruteo se actualiza cada 60 segundos. Esto puede causar un tráfico excesivo en la red.

6.5.8 SAP: SOPORTANDO LA PUBLICACION DE SERVICIOS

Todos los servidores en las redes NetWare pueden publicar sus servicios y direcciones.

Todas las versiones de NetWare soportan broadcast de SAP para anunciar y localizar servicios de red registrados, como en la figura 6.45.

Cada servicio de SAP es un tipo de objeto identificado por un número hexadecimal, por ejemplo:

- 4.- Servidor NetWare.
- 7.- Servidor de Impresión.
- 278.- Servidor de directorio.

Todos los servidores y ruteadores mantienen una lista completa de servicios disponibles a través de la red en tablas de información.

FIGURA 6.45

Por defecto, la publicación de servicios ocurre en intervalos de 60 segundos. Sin embargo, aunque las publicaciones de servicios pueden trabajar bien en una LAN, los servicios de broadcast pueden requerir mucho más ancho de banda para ser aceptable en redes grandes o en redes enlazadas con conexiones WAN Seriales.

Los ruteadores no pueden reenviar los broadcasts de SAP. En lugar de eso, cada ruteador construye su propia tabla de SAP y la envía a otros ruteadores. Por defecto, esto ocurre cada 60 segundos.

Las publicaciones SAP pueden ser filtradas en entrada o salida de información o desde un ruteador específico:

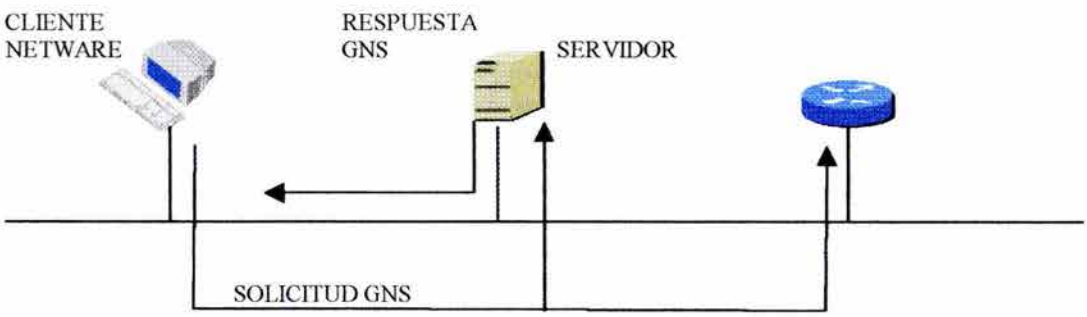
- Una entrada IPX: El filtro SAP permite al administrador controlar servicios que son añadidos a la tabla SAP del ruteador desde una interfaz física.
- Una salida IPX: El filtro SAP permite al administrador especificar servicios incluidos en las actualizaciones SAP que se envían a una interfaz específica.
- El ruteador IPX: El filtro SAP es usado para filtrar los mensajes SAP recibidos desde un ruteador específico en una interfaz específica.

6.5.9 GNS: EL PROCESO GET NEAREST SERVER

La interacción cliente/servidor NetWare empieza cuando el cliente se enciende y corre sus programas de arranque. Esos programas utilizan el adaptador de red del cliente en la LAN e inicia la secuencia de conexión para el cliente NetWare a utilizar.

GNS es un broadcast que viene desde un cliente que utilizan SAP. El servidor NetWare responde con una respuesta SAP, como lo muestra la figura 6.46. Desde ese puerto el cliente abre una sesión de red en el servidor, hace una conexión, fija el tamaño del paquete y precede a utilizar los recursos del servidor, el cliente es un usuario autorizado para utilizar ese servidor.

FIGURA 6.46



Si un servidor NetWare es localizado en el segmento, éste responde a la solicitud del cliente. Si no hay servidores NetWare en la red local, el ruteador responderá a la solicitud GNS con una dirección del servidor o servicio más cercano especificado por el cliente.

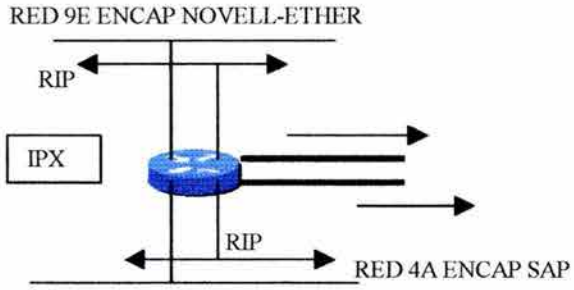
Un administrador puede querer filtrar el fragmento de una respuesta GNS. Para hacer este filtrado, el administrador utiliza un filtro de salida GNS para limitar la tabla de SAP de los servidores preferidos o cercanos que responden al broadcast GNS.

6.5.10 CONFIGURACION DE RUTEO IPX

La configuración de Novell IPX como protocolo de ruteo involucra parámetros globales y de interfaz:

- Los parámetros globales incluyen: Comenzar el proceso de ruteo IPX. Habilitar la carga compartida si es apropiado para la red. La carga compartida es el proceso de dividir las tareas de ruteo entre múltiples ruteadores para balancear el trabajo y mejorar el desempeño de la red.
- Las tareas de interfaz incluyen: Asignar una única red en cada interfaz, como muestra la figura 6.47. Los números de red múltiples pueden ser asignados a una interfaz permitiendo el soporte de diferentes tipos de encapsulaciones.

FIGURA 6.47



6.5.10.1 COMANDOS DE CONFIGURACION GLOBAL

Se utilizan tres comandos para instalar el modo de configuración global IPX:

- *ipx routing* [nodos]
- *ipx maximum-paths* [rutas]
- *ipx route destination-net next-hop* [estatico-flotante]

El comando *ipx routing* [nodo] habilita el ruteo IPX. Si no es especificada una dirección de nodo, el ruteador utiliza la dirección MAC de la interfaz. Si el ruteador sólo tiene interfaces, una dirección debe ser especificada.

El comando *ipx maximum-paths* [rutas] habilita la carga compartida. La carga compartida ocurre cuando dos rutas paralelas están disponibles entre la fuente y el destino. El parámetro *maximum paths* indica el número de rutas idénticas que pueden ser consideradas para la carga compartida. El valor por defecto del número de rutas, que es 1, significa que la carga compartida está deshabilitada por defecto.

El comando *ipx route destination-net next-hop* es una variación del comando *ipx routing* y utiliza la siguiente sintaxis:

ipx route {red[máscara de red]|por defecto} {nodo de red|interfaz} [estático flotante]

Esta extensión de comando permite que las rutas estáticas sean impuestas por un aprendizaje de ruteo dinámico. Estas rutas alternativas son aprendidas desde IPX RIP, EIGRP y NLSP. El uso de una ruta estática flotante es que si una ruta estática cae, una ruta dinámica es disponible para su uso.

6.5.10.2 COMANDOS DE CONFIGURACIÓN DE INTERFAZ

Dos comandos son utilizados para la configuración de interfaz:

- *interface*
- *ipx network*

El comando *interface* es utilizado para asignar un número de red a interfaces que soportan redes múltiples, normalmente utilizan subinterfaces. Una subinterfaz es un mecanismo que permite a una interfaz física simple soportar múltiples interfaces lógicas o redes. Esto es que varias interfaces logicas o redes puedan ser asociadas con una interfaz de hardware simple. Cada subinterfaz debe utilizar distinta encapsulación y esa encapsulación debe corresponder con la de los clientes y servidores utilizando el mismo número de red.

La sintaxis del comando *ip network* es:

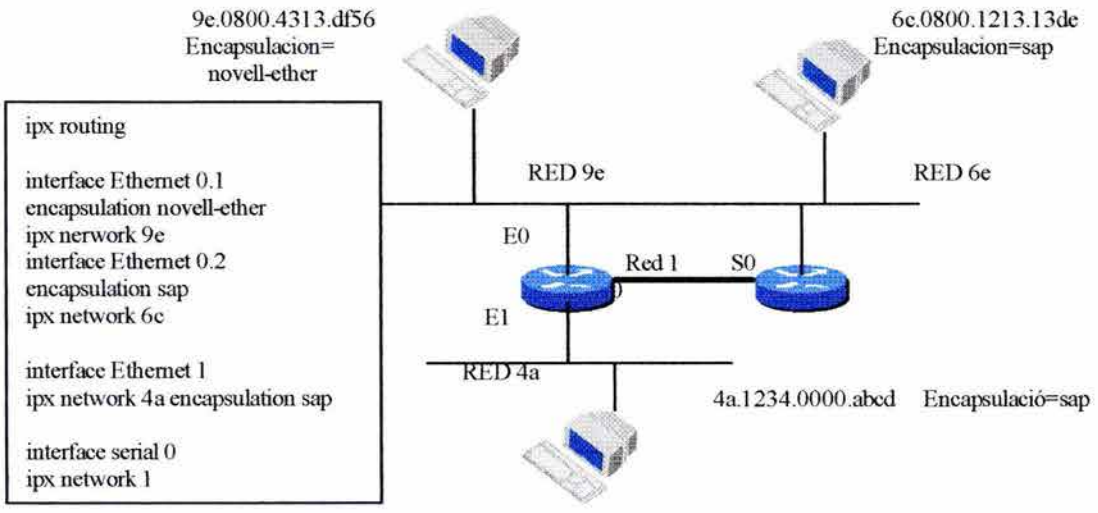
ipx network red [*encapsulation* tipo de encapsulación] [secondary]

Cuando se añade un número de red que soporta múltiples redes, se puede configurar redes primarias y redes secundarias. La primera red lógica que se configura en la interfaz es considerada la red primaria. Otra vez, cada red en la interfaz utiliza distinta encapsulación. Asignar la segunda red es necesario si un tipo de encapsulacion adicional es conectado a una red individual.

6.5.10.3 EJEMPLO DE CONFIGURACIÓN NOVELL IPX

Considerar el ejemplo de configuración IPX mostrado en la figura 6.48:

FIGURA 6.48



La siguiente lista define las funciones configuradas para el ruteador lógico en la figura 6.48:

- *ipx routing*: Selecciona IPX como protocolo de ruteo y empieza el proceso de ruteo.
- *ipx maximum-path 2*: Permite carga compartida sobre rutas paralelas al destino. El número de rutas paralelas esta limitado a 2.
- *interface ethernet 0.1*: Indica la primer subinterfaz en la interfaz E0.
- *encapsulation novell-ether*: Especifica el formato de frame que es el único utilizado en ese segmento de red.
- *ipx network 9e*: El número de red asignado a la subinterfaz E0.1.
- *interface ethernet 0.2*: Indica la segunda subinterfaz en la interfaz E0.
- *Encapsulation sap*: Especifica que el formato de frame Ethernet 802.2 es utilizado en ese segmento de red.
- *ipx network 6c*: El número de red asignado a la subinterfaz E0.2.
- *interface ethernet1*: Indica la primera interfaz en la interfaz E1.
- *ipx network 4a encapsulation sap*: Especifica que un nuevo formato de frame por defecto es utilizado en esta red, la cual tiene la dirección de red 4a.
- *interface serial 0*: Indica la primera interfaz en la interfaz Serial 0.
- *ipx network 1*: Fija la dirección IPX del enlace serial en 1.

6.5.11 VERIFICANDO Y MONITOREANDO EL RUTEO IPX

Siempre es importante verificar la configuración después que se ha completado ésta. Se utilizan comandos definidos en esta sección para garantizar que el ruteador se ha configurado correctamente.

Una vez que el ruteo IPX es configurado se puede monitorear y localizar averías utilizando los siguientes comandos:

- Comandos de monitoreo

    1. *show ipx interface*
    2. *show ipx route*
    3. *show ipx server*
    4. *show ipx traffic*

- Comandos de detección de averías

    1. *debug ipx routing activity*
    2. *debug ipx sap*

El comando *show ipx interface* muestra el estado de la interfaz IPX y los parámetros IPX configurados en cada interfaz, como lo muestra la figura 6.49. La primera línea en negrita muestra la dirección IPX, el tipo de encapsulación y el estado de la interfaz. La

segunda línea en negrita muestra que los flitros SAP no están fijos. La última línea en negrita muestra el Fast Switching activado.

Se puede fijar la métrica Tick manualmente. Se utiliza el comando *ipx delay* "número" donde "número" son los Ticks que se asocian a una interfaz. Este comando impone lo siguiente en los ruteadores:

- Para interfces LAN, una Tick.
- Para interfaces WAN, 6 Ticks.

Algunos campos desplegados incluyen:

- Dirección IPX: La dirección de red y de nodo de una interfaz del ruteador es seguida del tipo de encapsulación en la interfaz.
- Lista de filtros de entrada SAP: Números de filtros de entrada SAP aplicada a la interfaz con el comando *ipx input-sap-filter*.
- Lista de filtros de salida SAP: Números de filtros de salida SAP aplicada a la interfaz con el comando *ipx output-sap-filter*.
- Lista de filtros de ruteador SAP: Números de filtros de ruteador SAP aplicada a la interfaz con el comando *ipx router-sap-filter*.
- Fast Switching IPX: Indica si el Fast Swiching es habilitado o deshabilitado para la interfaz con el comando *ipx route-cache*.

FIGURA 6.49

```
Router#show ipx interface ethernet 0
Ethernet 0 is up, line protocol is up
  IPX address is 3010.aa00.0400.0284, NOVELL-ETHER [up] line-up, RIPPQ:0, SAPPQ: 0
  Delay of this Novell network, in ticks is 1
  IPXWAN processing nor enable on this interface.
  IPX SAP update interval is 1 minute(s)
  IPX SAP Type 20 propagation packet forwarding
  Outgoing access list is not set
  IPX Helper access list is nor set
  SAP Input filter list is not set
  SAP Output filter list is not set
  SAP Router filter list is not set
  SAP GNS output filter list is not set
  Input filter list is not set
  Output filter is not set
  Router filter is not set
  Netbios Input host access list is not set
  Netbios Input bytes access list is not set
  Netbios Output host access list is not set
  Netbios Output bytes access list is not set
  Update time is 60 seconds
  IPX accounting I disabled
  IPX fast switching is configured (enable)
  IPX SSE switching is disabled
  RIP packets received 1, RIP packets sent 10006
  SAP packets received 1, SAP packets sent 6
--More—
```

El comando *show ipx route* despliega el contenido de la tabla de ruteo como en la figura 6.50. La primera línea en negrita provee información de ruteo para una red remota:

- La información fue aprendida de una actualización RIP, indicada por una R.
- La red es el número 3030.
- Esta localizada a 6 Ticks o a un salto. Esta información es utilizada para determinar las mejores rutas.
- El próximo salto en la ruta es el ruteador 3021.0000.0c031.13d3.
- La información fue actualizada hace 23 segundos.
- Las actualizaciones se enviarán a través de la interfaz llamada Serial1

FIGURA 6.50

```
Router#show ip route
Codes: C – Connected primary network, c – Connected secondary network
       R – RIP, E – EIGRP, S – static, W – IPXWAN connected
5 Total IPX routes

Up to 2 parallel paths allowed Niovell routing algorithm variant in use

R  Net  3030 [6/1] via 3021.0000.0c03.13d3, 23sec, Serial1
                   via 3020.0000.0c03.13d3, 23sec, Serial0

C  Net  3021 (x25), Serial0
C  Net  3010 (NOVELL-ETHER), Ethernet0
C  net  3000 (NOVELL-ETHER), Ethernet1
```

La segunda línea en negrita provee información acerca de una conexión directa, indicado por C:

- El número de red es 3010.
- La encapsulación es de tipo NOVELL-ETHER

De particular interés están los valores de retardo y métrica. El factor retardo está especificado en Ticks ([1/18] de segundo). Los Ticks no son implementados por todo el equipamiento de red; por lo tanto, las decisiones de rutas pueden estar basadas en información incorrecta. Los valores de métrica especificada como 6/1 se refieren a Tick y cuenta a saltos.

El comando *show ipx servers* lista los servicios IPX descubierto a través de publicaciones SAP, como en la figura 6.51

FIGURA 6.51

```
Router>show ipx servers
Codes : P – Periodic, I – Incremental, H – Holddown, S – static
1 Total IPX Servers

Table ordering is based on routing and server info

Type   Name     Red      Dirección  Puerto    Ruta       Saltos   Itf
P4     Maxime   AD33000.0000.1b04.0288:051   332800/1   2        Et3
```

Este ejemplo provee la siguiente información:

- El servicio aprendido acerca del servidor de una actualización SAP.
- Nombre del servidor, localización de la red, dirección de dispositivo y número de socket fuente.
- Ticks y saltos para la ruta, tomados de la tabla de ruteo.
- El número de saltos, tomando del protocolo SAP.
- La interfaz a través de la cual se alcanza el servidor.

El comando *show ipx traffic* despliega información del número y tipos de paquetes IPX recibidos y transmitidos por el ruteador, como en la figura 6.52.

FIGURA 6.52

```
Router#show ip traffic
System Traffic for 2018.0000.0000.0001 System-Name: dtp-18
Revd:    23916 total, 13795 format errors 0 checksum erros, 0 bad hop count
         0 packtes pitched, 23916 local destination, 0 multicast
Beast:   17111 received, 9486 sent
Sent:    16707 generated, 0 forwarded
         0 encapsulation filed, 0 no route
SAP:     6 SAP requests, 6 SAP replies, 2309 servers
         0 SAP Nearest Name requests, 0 replies
         0 SAP General Name requests, 0 replies
         1521 SAP advertisements received, 2212 sent
         0 SAP flash updates sent, 0 CAP format errors
RIP:     6 RIP request, 6 RIP replies, 2979 routes
         8033 RIP advertisement received, 4300 sent
         154 RIP flash updates sent, 0 RIP format errors
Echo:    Revd 0 requests, 0 replies
         Sent 0 requests, 0 replies
         0 unknown: 0 no socket, 0 filtered, 0 no helper
         0 SAPs throttled, freed NDB len 0
Watchdog:
         0 packetes received, 0 replies spoofed
Queue Lengths:
         IPX input: 0. SAP0, RIP 0, GNS 0
         SAP throttling length: 0/(no limit), o nets pending lost route
reply
         Delayed priocess creration: 0
```

Hay que notar que en la figura 6.52, un alto porcentaje del total de los números de paquetes enviados y recibidos fueron publicaciones RIP.

El comando *debug ipx routing activity* despliega información acerca de paquetes de actualización de ruteo IPX así como en la figura 6.53.

Un ruteador envía una actualización cada 60 segundos. Cada paquete de actualización puede tener arriba de 50 entradas. Si hay más de 50 entradas en la tabla de ruteo, la

actualización incluye más de un paquete. En la figura 6.53 el ruteador envía paquetes pero no los recibe. Las actualizaciones recibidas desde otros ruteadores podrán también aparecer en esta lista.

FIGURA 6.53

```
Router#debug ipx routing activity
IPX routing debigging is on
Router#
IPXRIP: posting full update to 3010.fff.fff.fff via Ethernet 0 (broadcast)
IPXRIP: posting full update to 3000.fff.fff.fff via Ethernet 1 (broadcast)
IPXRIP: posting full update to 3020.fff.fff.fff via Serial 0 (broadcast)
IPXRIP: posting full update to 3021.fff.fff.fff via Serial 1 (broadcast)
IPXRIP: sending update to 3020.fff.fff.fff via Serial 0
IPXRIP: src=3020.000.0c03.14d8, dat=3020.fff.fff.fff, packet sent
      network 3121, hops 1, delay 6
      network 3110, hops 1, delay 6
      network 3100, hops 1, delay 6
IPXRIP: sending update to 3021.fff.fff.fff via Serial 1
IPXRIP: src=3021.000.0c03.14d8, dat=3021.fff.fff.fff, packet sent
      network 3120, hops 1, delay 6
      network 3110, hops 1, delay 6
      network 3100, hops 1, delay 6
IPXRIP: sending update to 3010.fff.fff.fff via Ethernet 0
IPXRIP: src=3010.aa00.0400.0284, dat=3010.fff.fff.fff, packet sent
      network 3130, hops 2, delay 7
      network 3120, hops 1, delay 1
      network 3121, hops 1, delay 1
      network 3000, hops 1, delay 1
IPXRIP: sending update to 3000.fff.fff.fff via Ethernet 1
```

El comando *debug ipx sap [Activity|Events]* despliega información acerca de los paquetes SAP que son transmitidos o recibidos.

Como las actualizaciones RIP, las actualizaciones SAP son enviadas cada 60 segundos y pueden contener múltiples paquetes. Cada paquete SAP aparece como líneas múltiples e incluye un mensaje de resumen y un mensaje de servicio detallado. Los paquetes SAP pueden ser de los siguientes tipos:

0x1.- Solicitud General
0x2.- Respuesta General
0x3.- Solicitud Get Nearest Server
0x4.- Respuesta Get Nearest Server

En cada línea, la dirección y la distancia al ruteador destino es listada. Cada actualización toma líneas múltiples y un resumen. La figura 6.54 muestra tres SAPs:

Una salida SAP, indicado por una I
Una actualización SAP, enviada a la red IPX 160

Una salida SAP, indicada por una O, con información acerca del servidor llamado Magnolia.

FIGURA 6.54

```
Router#debug ipx sap events
IPX service events debigging is on
Router#
NovellSAP: at 0023F778
I SAP Response type 0x2 len 160 src: 160.000.0c00.070d dest: 160.fff.fff.fff(452)
  type 0x4, "HELL02", 199.0002.0004.0006 (451), 2 hops
  type 0x4, "HELL02", 199.0002.0004.0006 (451), 2 hops
NovellSAP: sendig update to 160
NovellSAP: at 00169080
    SAP Update type 2x0 len 96 ssec: 0x452 dest: 160.fff.fff.fff(452)
Novell: type 0x4 "Mangnolia", 42.0000.0000.0001 (451), 2 hops
```

Las opciones *activity* y *events* no son opciones reales porque uno u otro es requerido. El comando *debug ipx activity* provee más detalles y la opción *events* provee pocos detalles porque se enfoca en paquete SAP que contienen eventos interesantes. Para información más útil, se utilizan esos dos comandos juntos.

6.6 ADMINISTRACION DE TRAFICO CON LISTAS DE ACCESO

Esta sección presenta una descripción de listas de acceso, incluyendo dónde y cuándo deben utilizarse y la manera en que trabajan. Una lista de acceso es utilizada para definir el tipo de tráfico que debe ser permitido o restringido a través de un ruteador.

6.6.1 ¿POR QUÉ UTILIZAR LISTAS DE ACCESO?

Primero, las redes de ruteo conectadas a redes LAN escalables. Después, el administrador de red agrandó las conexiones de ruteo e incremento el uso de Internet trayendo nuevos retos de control de acceso. La nueva tecnología, desde Backbones ópticos a servicios de banda ancha y switches de alta velocidad, incrementó el control otra vez.

Los administradores de sistemas se encontraron con el siguiente dilema: ¿Cómo negar el tráfico no deseado y permitir un acceso apropiado? Aunque otras herramientas tales como Passwords y dispositivos físicos de seguridad ayudan, ellos carecen de flexibilidad y controles específicos que la mayoría de los administradores prefieren.

Las listas de acceso ofrecen otra herramienta útil para el control de la red. Estas listas añaden flexibilidad para filtrar el flujo de paquetes dentro y fuera de las interfaces del ruteador. Tal control puede ayudar a limitar el tráfico de red y restringir el uso de red para ciertos usuarios o dispositivos. Las listas de acceso diferencian el tráfico por categorías que permiten o niegan otras características. Se pueden utilizar listas de acceso también para:

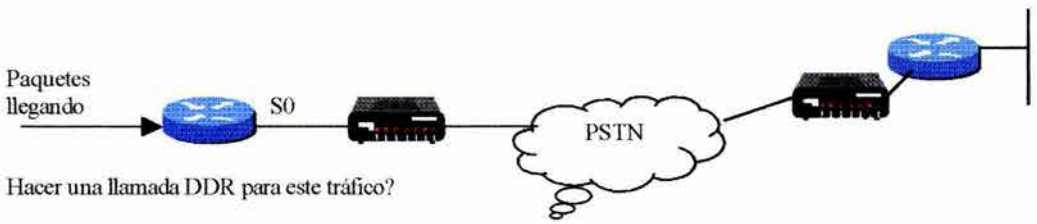
Identificación de paquetes para *Priority* y *Custom Queuing*[43]: La prioritización puede asignar ciertos paquetes a ser procesados por el ruteador antes que otro tipo de tráfico en el paso de un protocolo.
Restringir o reducir el contenido de la actualización de ruteo: Estas restricciones son utilizadas para limitar la información acerca de redes específicas.
Identificación de paquetes para levantar una conexión DDR: Garantiza que los paquetes que no son vitales para el proceso de una comunicación, no haga una comunicación WAN.

Las listas de acceso también procesan paquetes para otras características de seguridad:

Provee control de acceso dinámico con autenticación de usuarios mejorado usando la característica "lock and key".
Identificación de paquetes por encriptación.
Identificación de acceso Telnet permitido para las terminales virtuales del ruteador.

Según lo observado, la lista de acceso puede utilizarse para definir el tráfico que puede levantar un enlace WAN (ver figura 6.55). Comparado a una red el tráfico de una red que utiliza DDR es típicamente de bajo volumen. DDR inicia una llamada WAN a un sitio remoto sólo cuando hay tráfico a transmitir. Para identificar este tráfico, se especifican los paquetes que el proceso DDR en el ruteador interpretará como tráfico interesante. Por ejemplo, la dirección de red destino, la dirección de red fuente y el servicio o información de red puede ser definido como interesante y entonces ser permitido o restringido en el enlace WAN.

FIGURA 6.55



Cuando se configura DDR, se deben introducir los comandos que indican qué paquetes constituyen un tráfico interesante para iniciar la llamada, se debe introducir listas de acceso para identificar las direcciones fuente y destino y escoger una selección específica de protocolo para iniciar la llamada. Entonces, se establecen las interfaces donde inicia la llamada DDR. Este paso asigna un "grupo de marcado". El "grupo de marcado" asocia los resultados de la especificación de listas de acceso de paquetes interesantes a las interfaces del ruteador para una llamada WAN.

---

[43] *Priority Queuning*. Es una característica de ruteo en el cual los frames de una cola de salida de interfaz son prioritizados basados en varias características, tales como tamaño de paquete y tipo de interfaz.
Custom Queuing. Permite reservar un porcerntaje de ancho de banda para protocolos específicos.

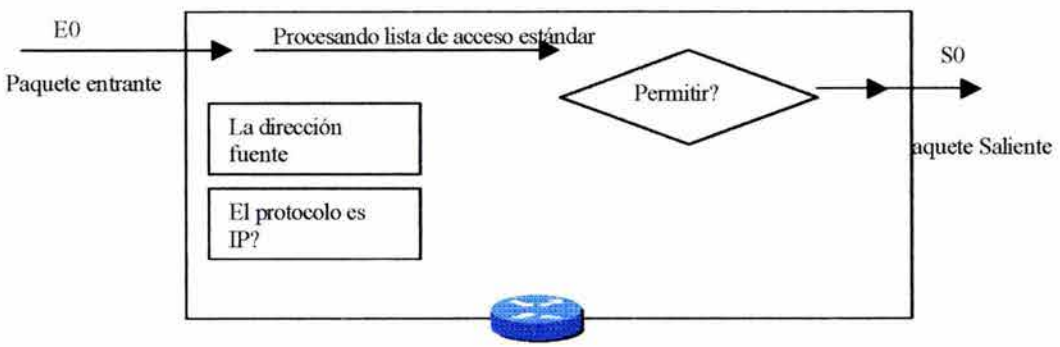
Para DDR, así como otras aplicaciones, las listas de acceso expresan un conjunto de reglas que proveen de control para paquetes que entran en interfaces y paquetes que salen de las interfaces del ruteador.

Hay dos tipos de listas de acceso:

- Listas de acceso estándar: Revisa las direcciones IP fuentes de paquetes que pueden ser ruteados. El resultado permite o niega la salida del protocolo IP basado en red/subred/host.
- Lista de acceso extendidas: Revisa la dirección fuente y destino de los paquetes. También revisa los protocolos específicos, números de puerto y otros parámetros, los cuales permiten a los administradores más flexibilidad para describir la revisión que hará la lista de acceso. Los paquetes pueden ser permitidos o negados al salir basándose en donde se origina el paquete y su destino.

Por ejemplo, en la figura 6.56, los paquetes que vienen de E0 son revisados en la dirección fuente, la dirección destino y el protocolo. Si los paquetes pertenecen a un protocolo y direcciones fuente y destino, son permitidos sólo a través de S0, la cual está agrupada a una lista de acceso. Si no es así, los paquetes son descartados.

FIGURA 6.56



Las listas de acceso extendidas también permiten o niegan con más exactitud. Por ejemplo, se puede permitir tráfico de correo electrónico desde E0 a S0 mientras se niegan sesiones remotas a transferencias de archivos.

Las listas de acceso también pueden corresponder con otros encabezados de paquete, por ejemplo, protocolo IP y puerto TCP.

6.6.2 ¿CÓMO TRABAJAN LAS LISTAS DE ACCESO?

El proceso de comienzo es el mismo sin importar si las listas de acceso son utilizadas: como un paquete entra en una interfaz, el ruteador revisa su tabla de ruteo para ver si el

paquete es ruteable. Si no lo es, el paquete será descartado. Si el paquete es ruteable, una tabla de ruteo indica un destino de red, alguna métrica de ruteo y la interfaz para enviar el paquete.

Después, el ruteador revisa para ver si la interfaz destino es agrupada a una lista de acceso. Si no es agrupada, el paquete puede ser enviado a un buffer de salida. Por ejemplo, si el paquete utilizará To0 como interfaz destino y esta interfaz no tiene lista de acceso, el paquete utilizará To0 directamente.

Si la interfaz destino del paquete es agrupada una lista de acceso, el paquete se debe de filtrar a través de esa lista. Por ejemplo, supongamos que una interfaz, E0, ha sido agrupada a una lista de acceso extendida. El administrador utiliza expresiones lógicas para fijar las listas de acceso. Antes de que el paquete sea procesado a esa interfaz, el paquete es probado por una combinación de parámetros de lista de acceso asociado con esa interfaz.

Basado en las pruebas de listas de acceso, el paquete puede ser permitido o negado. La negación de permiso quiere decir que el paquete se descarta. Cuando se descartan paquetes, algunos protocolos regresan un paquete especial que notifica que el destino es inalcanzable. Por ejemplo, un paquete ICMP puede ser enviado para indicar que el destino es inalcanzable. Permitir un paquete quiere decir que se tiene acceso a la interfaz destino.

6.6.3 UNA LISTA DE PRUEBAS: NEGAR O PERMITIR

Los parámetros de lista de acceso operan en orden secuencial y lógico. Ellos evalúan los paquetes desde abajo. Si el encabezado de un paquete y un parámetro de lista de acceso corresponden, el paquete se salta los demás parámetros. Si la condición de correspondencia es verdadera, el paquete es permitido o negado. Puede haber una sola lista de acceso por protocolo de interfaz.

Solamente si el paquete no correponde a las condiciones de la primera prueba se decartará al próximo parámetro de lista de acceso. Se asume que diversos parámetros de paquetes corresponden con la siguiente prueba, un parámetro de permiso. El paquete permitido procede a la interfaz del destino.

Otro paquete que no corresponde a las condiciones de la primera o segunda, pero corresponde a las condiciones del próximo parámetro de la lista de acceso; otra vez, el paquete es permitido.

6.6.4 DESCRIPCION DEL COMANDO *ACCESS LIST*

Hay dos elementos generales de comandos de configuración de listas de acceso:

1. El proceso de listas de acceso contiene declaraciones globales:

   Router(config)#**access-list** *numero de lista de acceso* {**permit** | **deny**}

{condiciones de prueba}

- Esta declaración global identifica la lista de acceso, usualmente un número de lista de acceso. Este número se refiere al tipo de lista de acceso que estará.
- Los términos **permit** o **deny** en la declaración de lista de acceso indica la manera en que los paquetes resuelven las condiciones de prueba que son manejadas por el Cisco IOS. **Permit** quiere decir que uno o dos interfaces pueden utilizar el paquete.
- El término o términos finales especifican las condiciones de prueba utilizadas por la declaración de lista de acceso. La prueba puede ser tan simple como para una simple dirección fuente, pero usualmente las condiciones de prueba son extendidas para incluir varias condiciones de prueba. Se utilizan varias declaraciones de lista de acceso con el mismo identificador para ampilar varias condiciones de prueba en una secuencia lógica o lista de prueba.

2. El comando *access-group* activa las listas de acceso en la interfaz.

Router(config)#*protocolo* **access-group** *numero de lista de acceso*

6.6.5 IDENTIFICACION DE LISTAS DE ACCESO

Las listas de acceso pueden controlar la mayoría de los protocolos en los ruteadores. La siguiente tabla muestra los protocolos y el rango de números de los tipos de lista de acceso.

TIPO DE LISTA DE ACCESO	NUMERO DE RANGO
IP estandar	1-99
extendida	100-199
IPX extendida	800-899
estandar	900-999
filtros SAP	1000-1099
Apple Talk	600-699

El administrador introduce un número en el rango de número de protocolo como el primer argumento de la declaración global de lista de acceso. El ruteador identifica el software de la lista de acceso a utilizar basado en el número que se introdujo. Las condiciones de prueba seguidos como argumentos. Estos argumentos especifican pruebas de acuerdo a las reglas del conjunto de protocolos dado.

Algunas listas de acceso son posibles para un protocolo. Se selecciona un número diferente desde el rango del protocolo para cada lista de acceso nueva; sin embargo, el administrador puede especificar sólo una lista por protocolo por interfaz.

Generalmente, los rangos de número permiten 100 listas de acceso diferentes en cada tipo de protocolo.

6.7 LISTAS DE ACCESO TCP/IP

6.7.1 PREPARANDO PAQUETES CON LISTAS DE ACCESO IP

Para los filtros de paquete TCP/IP, las listas de acceso del Cisco IOS revisa el paquete y los encabezados de capas superiores. Por ejemplo, las listas de acceso pueden revisar el paquete para:

- Direcciones IP fuente utilizando listas de acceso estándar; identifica éstas con un número en el rango de 1 a 99.
- Direcciones IP fuente y destino o protocolos específicos utilizando listas de acceso extendidas; identificadas con el número en el rango de 100 a 199.
- Los numeros de puerto TCP o UDP además de otras pruebas, identificada también con el número en el rango 100 a 199.

Para todas esas listas de acceso TCP/IP, después de que un paquete es revisado para una correspondencia con la declaración de listas de acceso, pueden ser negadas o permitidas para utilizar una interfaz en el grupo de acceso.

6.7.2 CONCEPTOS CLAVE PARA LISTAS DE ACCESO

Para crear listas de acceso se utiliza el proceso de configuración global del ruteador. Especificar un número de listas de acceso de 1 a 99 da instrucciones al ruteador para aceptar declaraciones de listas de acceso estándar. Especificar un número de listas de acceso de 100 a 199 da intrucciones al ruteador a aceptar declaraciones de listas de acceso IP extendida.

El administrador debe cuidadosamente especificar lógicamente controles de acceso y ordenar a las declaraciones llevar a cabo esos controles.

Seleccionar los protocolos IP para ser revisados. Después, en el procedimiento puede también especificar un puerto destino opcional.

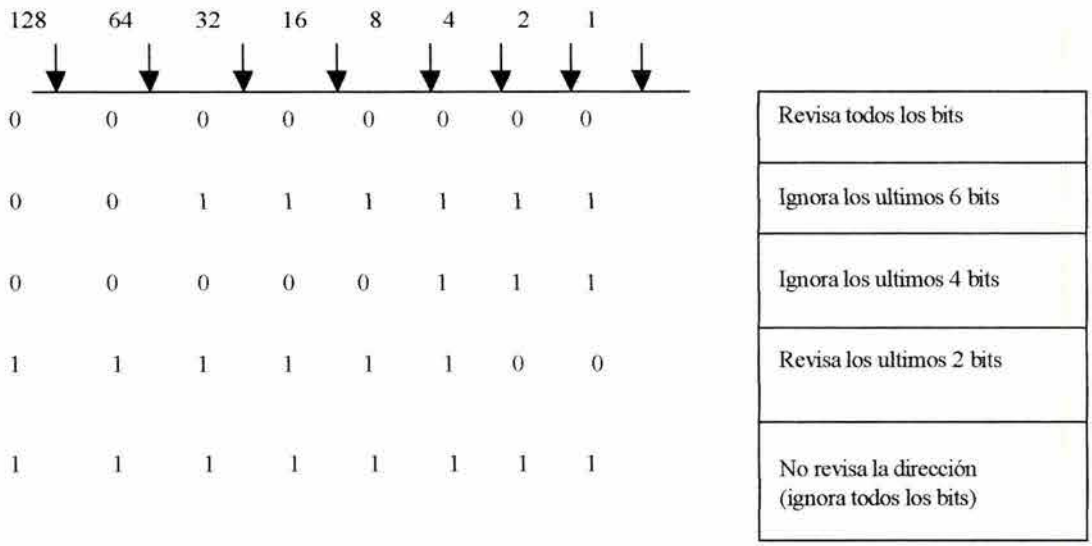
El filtrado de dirección ocurre utilizando *Mascara Wildcard* para identificar la manera en que revisa o ignora los bits de la dirección IP correspondiente (0 Revisa, 1 Ignora).

6.7.3 USO DE MASCARA WILDCARD

Las listas de acceso IP utiliza *Máscara Wildcard* para identificar simples o múltiples direcciones IP para permitir o negar pruebas. Una *Máscara Wilcard* hace pareja con una dirección IP y utiliza los numeros 0 y 1 para identificar la manera en que se debe de tratar la correpondencia de las direcciones IP (ver figura 6.57).

- Un bit 0 de la *Máscara Wildcard* significa "checar el valor del bit correpondiente en la dirección IP".
- Un bit 1 de la *Mascara Wildcard* significa "ignorar el valor de bit correspondiente en la dirección IP".

FIGURA 6.57

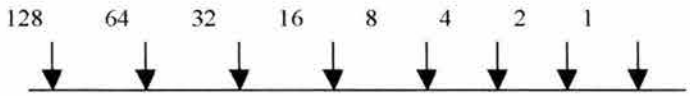


Aunque son cantidades de 32 bits, la Mascara Wildcard y las Máscaras de subred IP operan diferente. Recordar que los 0 y 1 en la máscara de subred determinan la red, subred y porción del host de una dirección IP correspondiente. Los 0 y 1 de una Máscara Wildcard, determinan si los bits correspondientes en la dirección IP deben ser revisados o ignorados para propósitos de listas de acceso.

El término *Máscara Wildcard* es un sobrenombre para el proceso de correspondencia *mascara-bit* de listas de acceso.

Se ha visto cómo los bits 0 y 1 en una máscara Wildcard de lista de acceso causa que la lista de acceso revise o ignore el bit correspondiente en la dirección IP. En la figura 6.58, el proceso de máscara Wildcrd es aplicada.

FIGURA 6.58



0	0	0	0	0	0	0	0	Revisa todos los bits
0	0	1	1	1	1	1	1	Ignora los ultimos 6 bits
0	0	0	0	0	1	1	1	Ignora los ultimos 4 bits
1	1	1	1	1	1	0	0	Revisa los ultimos 2 bits
1	1	1	1	1	1	1	1	No revisa la dirección (ignora todos los bits)

Un administrador quiere probar una dirección IP para subredes que serán permitidos o negados. Se asume que la dirección IP es clase B[44].
El administrador quiere utilizar bits de Máscara Wildcard para igualar las subredes 172.30.16.0 a 172.30.30.1.

- Para empezar las Máscara Wildcard revisará los dos primeros octetos (172.30) utilizando los bits 0 correspondientes.
- Como no hay interés en las direcciones de host individuales (un ID del host no será .00 en el fin de la dirección), la Máscara Wildcard ignorará el octeto final utilizando los bits correspondientes en la Máscara Wildcard.
- En el tercer octeto, donde la dirección de subred ocurre, la Máscara Wildcard ignorará el valor.

En este ejemplo, la dirección 172.30.16.0 con una Máscara Wildcard 0.0.15.255 corresponde con subredes de 172.30.16.0 a 172.30.31.0. La Máscara Wildcard no corresponde con ninguna otra subred.

6.7.4 CORRESPONDENCIA CON CUALQUIER DIRECCIONAMIENTO IP

Trabajar con representaciones de decimales con bits binarios de Máscara Wildcard puede ser tedioso. Para los usos más comunes de Máscara Wildcard, se pueden utilizar palabras abreviadas. Esas palabras abreviadas reducen los números que un administrador requerirá incorporar mientras configura las direcciones de condiciones de prueba. Un

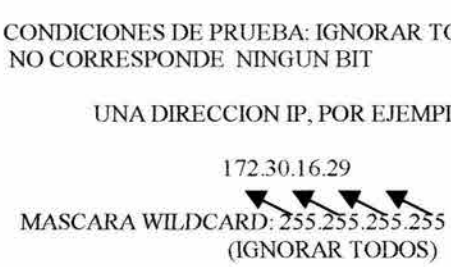
[44] Recordar Clase B es para redes intermedias con direcciones de host de 16 bits y direcciones de red de 14 bits.

ejemplo que se puede utilizar es una abreviación en lugar de una cadena larga de Máscara Wildcard cuando se quiere correponder algunas direcciones.

Considerar un administrador de red que quiere especificar que alguna dirección destino sea permitida en una prueba de lista de acceso, como en la figura 6.59. Para indicar alguna dirección IP, el administrador introducirá 0.0.0.0; entonces, para indicar que la lista de acceso deberá ignorar (permitir sin revisar), algún valor, la correspondencia de bits de la Máscara Wildcard para esta dirección deberan ser 1 (que es, 255.255.255.255).

El administrador puede utilizar la abreviatura *any* para comunicar estas mismas condiciones de prueba en el Cisco IOS Software en el lugar de introducir 0.0.0.0 255.255.255.255.

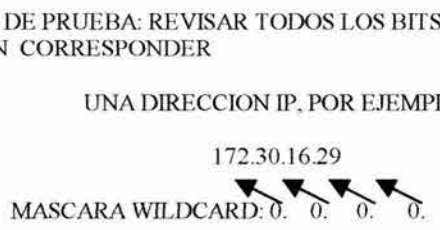
FIGURA 6.59



6.7.5 CORRESPONDIENDO UNA DIRECCION DE HOST ESPECIFICA

Una segunda condicion común es en la cual el Cisco IOS permitirá un término abreviado en la Máscara Wildcard de listas de acceso extendidas cuando el administrador quiere tener correspondencia en todos los bits de la dirección IP del host, como en la figura 6.60.

FIGURA 6.60



Considerar un administrador de red que quiere especificar que una dirección de IP host será negada en la prueba de lista de acceso. Para indicar una dirección IP del host, el administrador de red debe introducir la dirección entera, 172.30.16.29. Entonces, para indicar que la lista de acceso deberá revisar todas las direcciones, la correspondencia de bits de máscara Wildcard para esta dirección deberán ser todos 0; que es 0.0.0.0.

El administrador puede utilizar la abreviación *Host* para comunicar esta misma condición de prueba a Cisco IOS Software. En este ejemplo, en lugar de escribir 172.30.16.29 0.0.0.0, el administrador puede utilizar la cadena host 172.30.16.29.

6.7.6 CONFIGURACION DE LISTAS DE ACCESO ESTANDAR

El comando *access-list* crea una entrada en una lista de filtro de tráfico. El formato de este comando es:

Router(config)#*access-list* numero de lista de acceso {*permit* | *deny*} *source* [máscara fuente]

donde los parámetros y palabras clave tienen los siguientes significados:

- Número de lista de acceso: Identifica la lista a la cual la entrada pertenece.
- *Permit* | *Deny*: Indica si esta entrada permite o bloquea tráfico desde una dirección específica.
- *Source*: Identifica la dirección IP fuente. Se utiliza la palabra clave *any* como abreviación para una fuente y una Máscara Wildcard de 0.0.0.0 255.255.255.255.
- Máscara Fuente: Identifica los bits que corresponden en el campo dirección.

El comando *ip access-group* enlaza una lista de acceso existente a una interfaz de salida. Solo una lista de acceso por puerto por protocolo por dirección es permitido: el formato de este comando es:

Router (config)# *ip access group* número de lista de acceso {*in* | *out*}

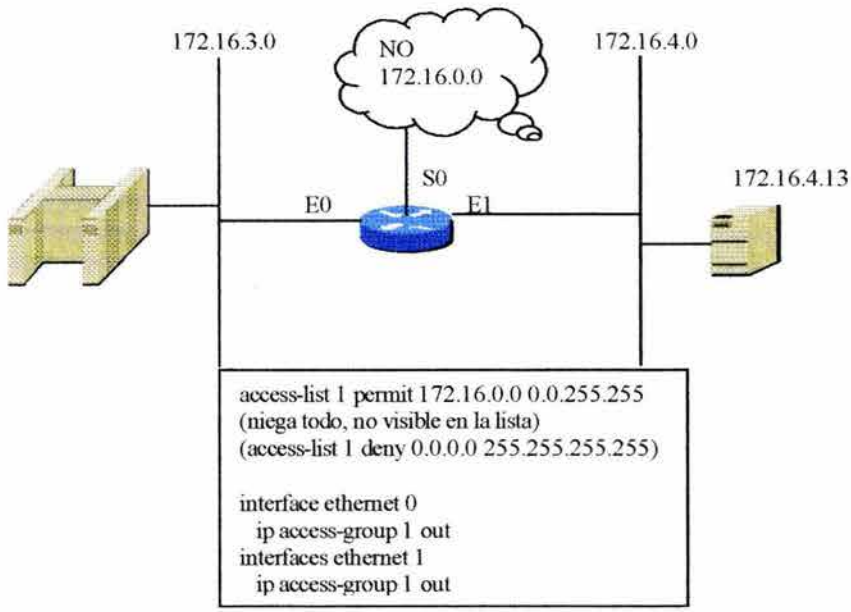
donde los parámetros y palabras clave tienen los significados:

- Número de lista de acceso: Indica el número de lista de acceso a ser colocada en esa interfaz.
- *In* | *out*: Selecciona si la lista de acceso son aplicadas a una interfaz de entrada y de salida. Si *in* o *out* no son especificados, *out* está por defecto.

6.7.6.1 EJEMPLO 1: PERMITIR SOLO MI RED

La figura 6.61 ilustra una situación en la cual la lista de acceso sólo permite tráfico de la red fuente 172.16.0.0 sea enviado. El tráfico que no es de la red 172.16.0.0 es bloqueado.

FIGURA 6.61



En la figura anterior los parámetros del comando *access-list* son como siguen:

- 1: Número de lista de acceso; indica que es una lista estándar.
- Permit: Tráfico que será enviado.
- 172.16.0.0: Direcciones IP que serán utilizadas con la máscara Wildcard para identificar la red fuente.
- 0.0.255.255: Máscara Wildcard; 0 indica las posiciones que deben corresponder.

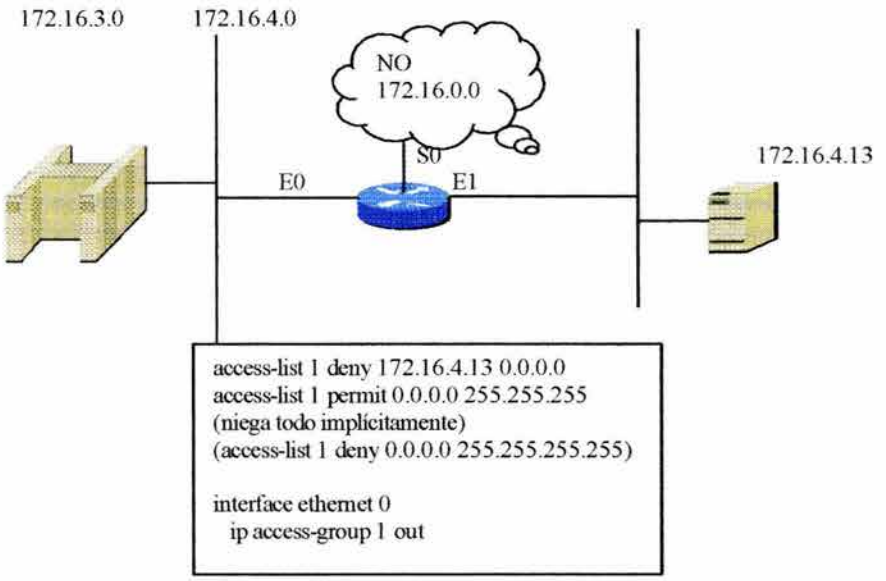
También en la figura 6.61 el comando *ip access-group out* enlaza la lista de acceso 1 a una interfaz de salida.

Para remover una lista de acceso, primero se introduce el comando *no access-group* con todos sus parámetros y después introducir el comando *no access-list* también con todos sus parámetros.

6.7.6.2 EJEMPLO 2: NEGAR UN HOST ESPECÍFICO

La figura 6.62 representa una muestra de lista de acceso para bloquear tráfico de una dirección específica. Esta lista de acceso está diseñada para bloquear tráfico de una dirección especifica, 172.16.4.13 y permitir que otro tráfico sea enviado por una interfaz ethernet 0.

FIGURA 6.62



El primer comando *access-list* utiliza el parámetro *deny* para negar el tráfico de un host identificado. La máscara en la dirección 0.0.0.0 en esta línea requiere la prueba para tener correspondencia con todos los bits. Si esta máscara es omitida, el ruteador asume que la máscara está implícita.

En el segundo comando *access-list*, la combinación dirección IP/máscara Wildcard 0.0.0.0 255.255.255.255 identifica el tráfico desde alguna fuente. Esta combinación también puede ser escrita usando una palabra clave.

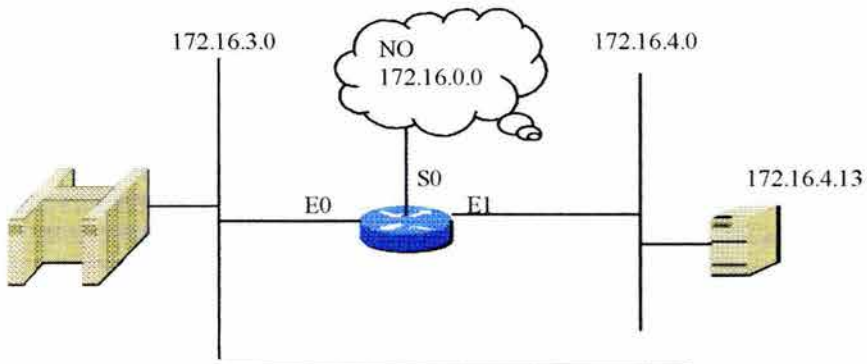
Un paquete que no corresponde con la primera línea de lista de acceso, correponderá con la segunda y será enviada.

6.7.6.3 EJEMPLO 3: NEGAR UNA SUBRED ESPECÍFICA

La figura 6.63 representa una lista de acceso para bloquear tráfico desde una subred específica.

Esta lista de acceso está diseñada para bloquear el tráfico desde una subred específica, 172.16.4.0 y permitir otro tráfico que sea enviado. Revisar la máscara Wildcard 0.0.0.255, el 0 en los tres primero octetos indican que esas posiciones deben corresponder. Notar que la abreviación *any* ha sido utilizada para dirección IP de la fuente.

FIGURA 6.63




```
access-list 1 permit 172.16.4.0 0.0.0.255
acess-list 1 permit any
(negar todo implicitamente)
(access-list 1 deny 0.0.0.0 255.255.255.255)

interface ethernet 0
  ip access-group 1 out
```

6.7.7 LISTAS DE ACCESO EXTENDIDAS

Las listas de acceso estándar no proveen el control de filtrado necesario. Los filtros de listas de acceso estándar basados en la dirección fuente y la máscara, permiten o niegan el conjunto entero de protocolo IP.

Para un control de filtrado más preciso, se utilizan las listas de acceso extendidas. Además, en el final de la declaración de listas de acceso extendidas, se obtiene precisión adicional desde un campo que especifica el número de puerto de protocolo TCP o UDP.

Se puede especificar la operación lógica que las listas de acceso desempeñarán en protocolos específicos. Las listas de acceso extendidas utilizan un número de 100 a 199.

6.7.8 CONFIGURACIÓN DE LISTAS DE ACCESO EXTENDIDAS

El comando *access-list* crea una entrada para especificar una expresión en un filtro complejo. El formato es:

Router(config)#*acces*s-list número de lista de acceso {permit | deny} protocol source source mask destination destination mask [operador operando] [ESTABLECIDO]

donde lo parámetros y palabras clavetienen los siguientes significados:

- Número de lista de acceso: Indica el número de lista a ser enlazada.

- *permit | deny*: Indica se la entrada permite o bloque la dirección especificada
- Protocol: IP, TCP, UDP, ICMP, IGRP.
- Source y destination: Identifica la dirección IP fuente y destino.
- Source mask y destination mask: Máscara wildcard
- Operador y Operando: lt, gt, eq, neq (menor que, mayor que, igual, desigual) y un número de puerto y nombre.
- ESTABLECIDO: Permite al tráfico TCP si el paquete utiliza una conexión establecida.

El comando *ip access-group* enlaza una lista de acceso existente a una interfaz de salida. El formato del comando es:

Router(config)#*ip access-group* numero de lista de acceso {*in* | *out*}

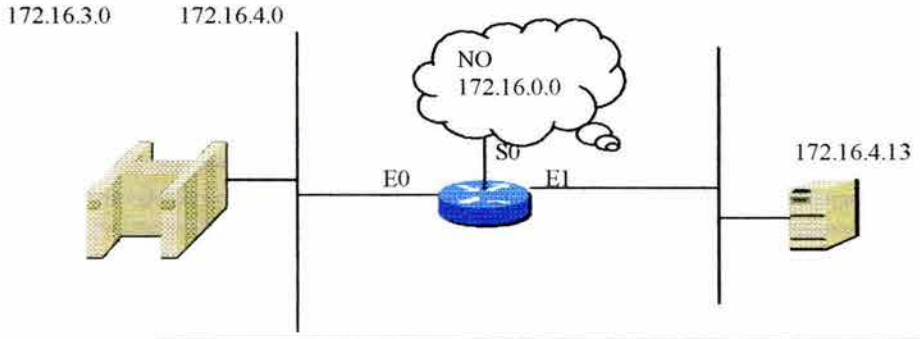
donde los parámetros y palabras clave son las siguientes:

- Número de lista de acceso: Indica el numero de lista de acceso a ser enlazado.
- *in | out*: Selecciona si las listas de acceso son aplicada a una interfaz de entrada o de salida.

6.7.8.1 EJEMPLO 1: NEGAR FTP PARA E0

La figura 6.64 muestra una lista de acceso extendida que bloquea el tráfico FTP.

FIGURA 6.64




```
access-list 101 deny tcp 172.16.4.0  0.0.0.255 172.16.3.0.0  0.0.0.0255 eq21
access-list 101 deny tcp 172.16.4.0  0.0.0.255 172.16.3.0.0  0.0.0.0255 eq20
access-list 101 permit ip 172.16.4.0.  0.0.0.255 0.0.0.0 255.255.255.255
(niega todo implicitamente)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0. 255.255.255.255)

 interface ethernet 0
   ip access-group 101 out
```

La declaración *permit* permite el tráfico desde la subred 172.16.4.0 para ser enviado a todas las redes y subredes por la interfaz E0. El resto de los parámetros de listas de acceso en este ejemplo son los siguientes:

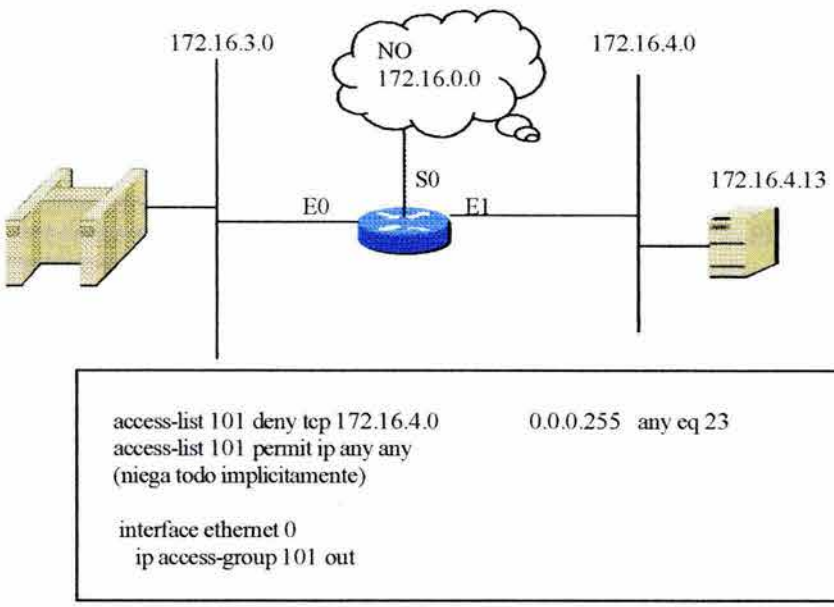
- 101: Este número de lista de acceso indica una dirección IP extendida.
- Deny: El tráfico que corresponde con los parámetros seleccionado será bloqueado.
- TCP: Protocolo de capa de red.
- 172.16.4.0 y 0.0.0.255: Dirección IP y máscara; los primeros tres octetos deben de corresponder.
- 172.16.3.0 y 0.0.0.255: Dirección destino IP y máscara, los primeros tres octetos deben corresponder.
- eq21: Especifica un número de puerto conocido para FTP.
- eq20: Especifica un número de puerto conocido FTP para datos.

El efecto del comando *interface E0 access-group* es enlazar lista 101 al puerto de la interfaz de salida E0.

6.7.8.2 EJEMPLO 2: NEGAR SOLO TELNET FUERA DE E0

La figura 6.65 muestra otras listas de acceso extendidas.

FIGURA 6.65



Este ejemplo niega que el tráfico Telnet (eq23) desde 172.16.4.0 sea enviado fuera de la interfaz E0. Otro tráfico desde otra fuente a algun destino es permitido. La interfaz E0 es configurada con el comando *ip access-group101*.

6.7.9 NOMBRAMIENTO DE LAS LISTAS DE ACCESO

El nombramiento de listas de acceso permite que las listas de acceso estándar y extendidas sean identificadas con un número entero alfanumérico (nombre) en lugar de la representación actual numerica.

Con las listas de acceso numeradas anteriormente, primero se requerirá de un administrador que desee alterar las listas de acceso para borrar todas las declaraciones en la lista de acceso numerada. Este borrado utiliza la palabra *no* precediendo cada declaración.

El nombramiento de listas de acceso puede ser utilizado para borrar entradas individuales de una lista de acceso específica. Borrar las entradas da la capacidad de modificar las listas de acceso y reconfigurar. Se utiliza el nombramiento de listas cuando:

- Se quieren identificar listas de acceso intuitivamente utilizando un número alfanumérico.
- Se tiene más de 99 listas de acceso simples y 100 listas de acceso extendidas en un ruteador para un protocolo dado.

Considerar lo siguiente antes de implantar el nombramiento de listas de acceso:

- El nombramiento de listas de acceso no es compatible con los Releases del Cisco IOS Software anteriores a 11.2.
- No se puede utilizar el mismo nombre para múltiples listas de acceso. Además, las listas de acceso de diferentes tipos no pueden tener el mismo nombre. Por ejemplo, no se puede especificar una lista de acceso estandar con el nombre de "Jorge" y una lista de acceso extendida con el mismo nombre.

La mayoría de las listas de acceso comúnmente utilizadas aceptan el nombrado de listas de acceso. Los siguientes comandos pueden ser utilizados para definir el nombrado de la lista de acceso:

Router(config)#ip *access-list* {estandar | extendida} nombre

El modo de configuración de lista de acceso, especifica una o más condiciones permitidas o negadas. Este determina si el paquete es permitido o negado:

Router(config (std- | ext-)nacl)#
deny {fuente [fuente wildcard] | *any*}
permit {fuente [fuente wildcard] | *any*}

La siguiente configuración crea una lista de acceso estándar nombrada *Internet-filter* y una lista de acceso nombrada *marketing-group*:

interface ethernet0/5
ip address 2.0.5.1 255.255.0

```
ip access-group internet-filter out
ip access-group marketing-group in
...
ip access-list standard internet-filter
permit 1.2.3.4
deny any
ip access-list extended marketing-group
permit tcp any 171.69.0.0 0.0.255.255 eq telnet
deny tcp any any
permit icmp any any
deny udp any 171.69.0.0 0 .0.255.255 lt 1024
deny ip any any log
```

Para activar el nombrado de lista de acceso en una interfaz, se utiliza el siguiente commando:

Router(config-if)#*ip access-group* {nombre | *1-99 {in | out}*}

Lo siguiente es una configuración de salida

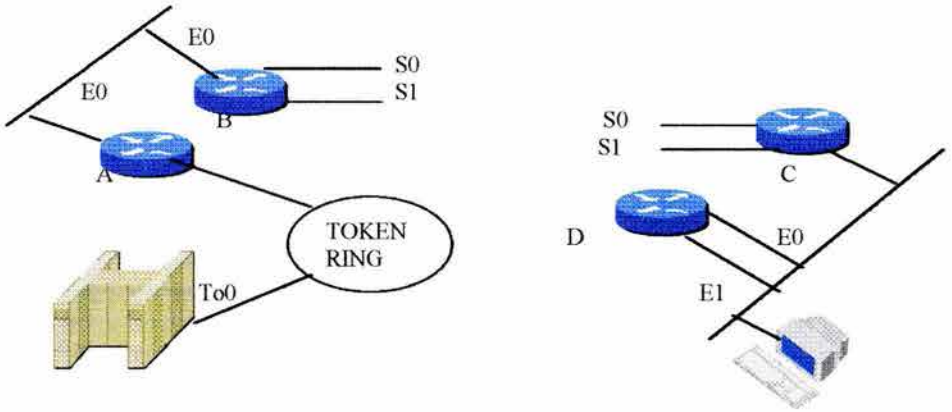
```
ip access-list extended come_on
permit tcp any 171.69.0.0 0.0.255.255 eq telnet
deny tcp any any
permit icmp any any
deny udp any 171.69.0.0 0.0.255.255 lt 1024
deny ip any any
interface ethernet0/5
ip address 2.0.5.1 255.255.255.0
ip access-group over_and out
ip access-group come_on in
ip access-list standard over_and
permit 1.2.3.4
deny any
```

6.7.10 ¿DONDE SE UTILIZAN LAS LISTAS DE ACCESO?

Las listas de acceso son utilizadas para controlar el tráfico por filtrado y eliminación de paquetes indeseados. El lugar donde el administrador pone la declaración de lista de acceso puede reducir el tráfico necesario. El tráfico que es negado a un destino remoto no debe utilizar recursos de red a lo largo de la ruta al destino.

Supongamos que una política de una empresa es negar el tráfico en el ruteador A a la red switcheada LAN en el puerto E1 en el ruteador D, como muestra la figura 6.66. Al mismo tiempo otro tipo de tráfico debe ser permitido. Varias aproximaciones pueden lograr esa politica.

FIGURA 6.66



La aproximación recomendada utiliza una lista de acceso extendida. Esta especifica la dirección fuente y destino. Se coloca esta lista de acceso en el ruteador A. Entonces los paquetes no atraviesan el ruteador A, no atraviesan las interfaces seriales del ruteador B y C y no entran en el ruteador D. El tráfico con diferentes fuente y destino pueden ser permitidos.

La regla, con listas de acceso extendidas, es poner las listas de acceso tan cerca como es posible de la fuente de tráfico denegado.

Las listas de acceso estándar no especifican dirección destino. El administrador tendría que poner la lista de acceso estándar tan cerca del destino como sea posible.

6.7.11 VERIFICANDO LISTAS DE ACCESO

El comando *show ip interface* despliega información de la interfaz IP e indica si alguna lista de acceso está fija. La figura 6.67 muestra el resultado del comando *show ip interface*.

FIGURA 6.67

```
Router#show ip interfaces
Ethernet 0 is up, line protocol is up
    Internet address es 192.54.222.2, subnet mask is 255.255.255.0
    Broadcast address is 255.255.255.255
    Address determined is 192.52.71.4
    MTU is 1500 bytes
    Helper address is 192.52.71.4
    Secondary address 131.192.115.2
    Outgoing access list 10 is set
    Inbound access list is not set
    Proxy ARP is enable
    Security level is default
    Split horizon is enable
    ICMP redirects are always sent
    ICMP unreachables are always sent
    ICMP mask replies are never sent
    IP fast switching is enabled
   Gateway Discovery es disabled
    IP accounting is disabled
    TCP/IP header compression is disabled
```

6.7.12 MONITOREANDO DECLARACIONES DE LISTAS DE ACCESO

El comando *show access list* despliega el contenido de todas las listas de acceso, como muestra la figura 6.68. Este comando provee más detalles acerca de las declaraciones de listas de acceso. Al introducir un número de lista de acceso a un número como una opción para este comando, se puede ver una lista específica.

Se pueden ver también listas de acceso con los comandos *show running-config* y *show startup-config*. Sin embargo, con estos otros comandos, los detalles de listas de acceso se mezclan entra todas la otras declaraciones del archivo de configuración.

FIGURA 6.68

```
Router#> show access list

Standard IP access list 19
      permit 172.16.19.0
      deny   0.0.0.0 wildcard bits 255.255.255.255
Standard IP access list 49
      permit 172.16.31.0 wildcard bits 0.0.0.255
      permit 172.16.194.0 wildcard bits 0.0.0.255
      permit 172.16.195.0 wildcard bits 0.0.0.255
      permit 172.16.195.0 wildcard bits 0.0.0.255
      permit 172.16.196.0 wildcard bits 0.0.0.255
      permit 172.16.197.0 wildcard bits 0.0.0.255
Extended IP access list 101
      permir tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 23
Type code access list 202
      permit 0x6001 0x0000
Type code access list 202
      permir 0x6004 0x0000
      deny  0x0000  0xFFFF

Router>
```

6.8 LISTAS DE ACCESO NOVELL IPX

En esta sección aprenderemos la manera en que se puede bloquear o permitir tráfico IPX específico a través de una ruteador.

6.8.1 PROBANDO PAQUETES UTILIZANDO LISTAS DE ACCESO NOVELL IPX

Para los filtros de paquetes que se verán en esta sección, las listas de acceso del Cisco IOS revisan el encabezado del paquete para:

- Direcciones IPX fuente y destino utilizando una lista de acceso estándar; identificando esa lista con un número en el rango de 800 a 899.

- Números de servicios de publicación además de otras pruebas en los filtros SAP de las listas de acceso, identificando esas listas con un número en el rango de 1000 a 1099.

Para esas listas de acceso IPX, después de que un paquete es revisado para una correspondencia con declaraciones de lista de acceso, ésta puede ser permitida o negada en el uso de una interfaz en el grupo de acceso.

6.8.2 CONCEPTOS CLAVE PARA LISTAS DE ACCESO IPX

El direccionamiento IPX está basado en el formato de *red.nodo.socket*. El número de red es asignado por el administrador; la porción del nodo es derivada de la dirección MAC de la interfaz individual. Las líneas seriales adoptan la dirección MAC de la otra interfaz en la creación de sus direcciónes lógicas. El número de socket se refiere al proceso o aplicación.

Por ejemplo, AABB0001.00001B03AC33.0452 puede ser interpretado como sigue:

- AABB0001, es la dirección de red.
- 00001B03AC33, es la dirección del nodo.
- 0452, es el numero de socket.

Cada servidor de archivos NetWare tiene un número de red interno y desempeña ruteo IPX. El número de red IPX asignado a la interfaz de un ruteador debe ser único y consistente con los números de red conocidos por el servidor.

Las listas de acceso IPX estándar utilizan números en el rango de 800 a 899. Estas listas de acceso revisan la dirección fuente o la dirección fuente y destino. Para identificar las partes de la dirección para identificar o ignorar, las listas de acceso IPX estándar utilizan la máscara wildcard que opera como la máscara utilizada con direcciones IP.

Para controlar el tráfico desde SAP, se utilizan los filtros SAP que van en el rango de 1000 a 1099. Varios de los otros paquetes y de los filtros de ruteo pueden ayudar a administrar la sobrecarga del tráfico IPX. Por ejemplo, las listas de acceso pueden controlar Get Nearest Server (GNS), Routing Information Protocol (RIP) y NetWare Link Services (NLSP).

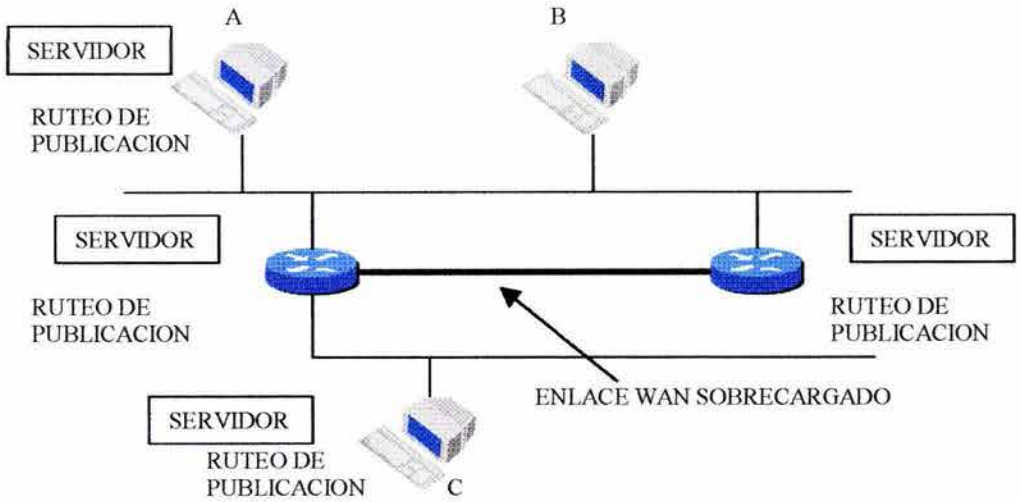
Las listas de acceso extendidas, por otro lado, filtran en protocolos específicos o sockets. El filtrado de sockets IPX usan las listas de acceso numerada en el rango de 900 a 999.

6.8.3 CONTROLANDO LA SOBRECARGA DE IPX

El ruteo IPX y los procesos de publicación fueron diseñados para correr en redes LAN. Como las redes LAN se interconectan con más lentos y costosos enlaces WAN, como en la

figura 6.69, la sobrecarga de control de paquetes IPX puede reducir el ancho de banda disponible para el tráfico de aplicaciones.

FIGURA 6.69



La figura 6.69 muestra cuatro redes IPX y múltiples servidores que publican rutas y servicios.

Cuando una estación de trabajo se inicializa, envía su propio broadcast SAP para encontrar un servidor; entonces busca el servidor más cercano, la estación de trabajo puede iniciar una sesión en el servidor y correr aplicación de red.

Cuando todos esos protocolos son indeseados, un administrador de red puede utilizar listas de acceso IPX. Con la lista de acceso IPX estándar, el filtrado *permitir/negar* actúa en todos los paquetes IPX para las direcciones de interfaz.

6.8.4 CONFIGURACIÓN DE LISTAS DE ACCESO ESTANDAR IPX

Se utiliza del comando **access-list** para filtrar el tráfico en una red IPX. El uso de filtros en la interfaz de salida del ruteador permite o restringe protocolos diferentes y aplicaciones en redes individuales. La forma completa del comando de lista de acceso es:

> Router(config)#*access-list* número de lista de acceso *{deny | permit}* red fuente [nodo fuente] [máscara de nodo fuente] [red destino] [nodo destino] [máscara de nodo destino]

donde los parámetros y palabras clave tienen los siguientes significados:

- Número de lista de acceso: Número de lista de acceso. Este es un número decimal de 800 a 899.

- *deny*: Niega el acceso si las condiciones corresponden.
- *permit*: Permite el acceso si las condiciones corresponden.
- Red fuente: Número de red del cual el paquete está siendo enviado. Este es un numero hexadecimál de 8 dígitos que únicamente identifica un segmento de red. Este puede ser un número en el rango de 1 a FFFFFFFE.
- Nodo fuente (opcional): Nodo en la red fuente del cual el paquete esta siendo enviado. Este es un número de 48 bits representado por tres bloques de cuatro dígitos hexadecimales separados por puntos.
- Máscara de nodo fuente (opcional): Máscara a ser aplicada al nodo fuente.
- Red destino (opcional): Numero de red en cual el paquete es recibido. Este es un número hexadecimal de 8 dígitos que únicamente identifica un segmento de red. Este puede ser un número en el rango de 1 a FFFFFFFE.
- Nodo destino (opcional): Nodo de red destino en el cual el paquete es recibido. Este es número de 48 bits representado por tres bloques de cuatro dígitos hexadecimales separados por puntos.
- Máscara de nodo destino (opcional): Máscara a ser aplicada a al nodo destino.

Se utiliza el comando *ipx acess-group* para enlazar un filtro de tráfico IPX a una interfaz como sigue:

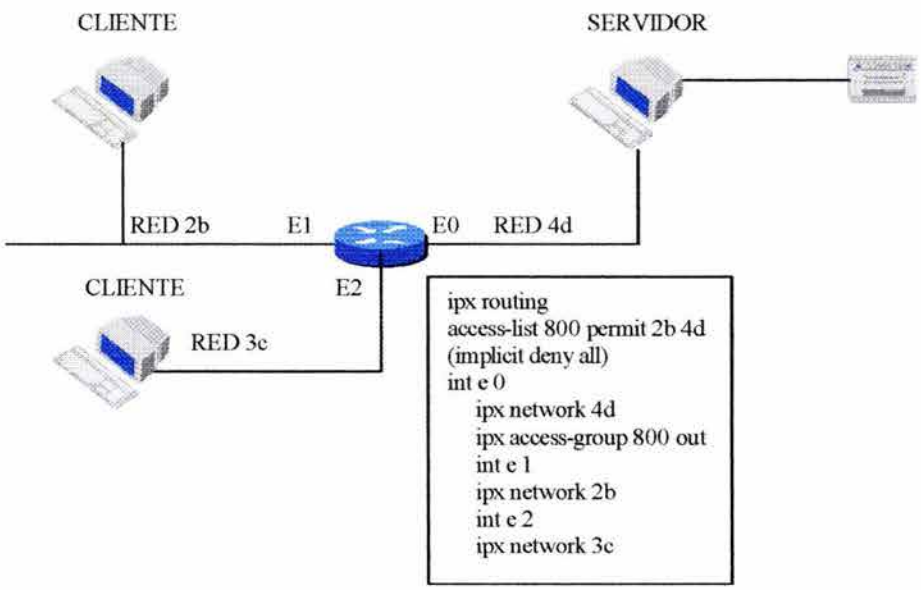
Router(config-if)# *ipx access-group* número de lista de acceso {*in* | *out*}

donde número de *lista de acceso* es un filtro IPX de 800 a 899.

6.8.4.1 EJEMPLO DE LISTA DE ACCESO IPX ESTANDAR

La figura 6.70 muestra una lista de acceso permitiendo el tráfico IPX de una red 2b destinada a la red 4d para ser enviada fuera de Ethernet0.

FIGURA 6.70



Los detalles del comando *access-list 800* de la figura 6.70 son los siguientes:

- 800: Especifica una lista de acceso IPX estándar.
- permit: El tráfico que corresponde con los pará metros seleccionados será enviado.
- 2b: Número de red fuente.
- 4d: Número de red destino.
- (implicit deny all): Comando de configuración válida. El resto de tráfico a ser enviado.

La interfaz E0 es configurado con el comando *ipx access-group 800 out*; que es *access-list 800* es enlazada a la interfaz de salida E0.

6.8.5 CONFIGURACION DE LISTAS DE ACCESO EXTENDIDAS

Para definir una lista de acceso IPX extendida, se utiliza la versión extendida del comando de configuración global[45].

Los filtros de lista de acceso extendida en el tipo de protocolo con todos los otros parámetros son opcionales. Para algunas versiones de NetWare, el campo de tipo de protocolo no es un indicador confiable del tipo de paquetes encapsulado en el encabezado IPX. En esos casos se utiliza el socket fuente o destino.

La forma completa del comando de listas de acceso extendida IPX es:

Router(config)#*access list* número de lista de acceso {*deny* | *permit*} protocolo Novell red fuente [dirección fuente [máscara fuente]] socket fuente red destino [dirección destino [máscara destino]] socket destino **[log]**

Algunos parámetros mostrados en esta lista de acceso fueron cubiertos anteriormente en la configuración de lista de acceso estándar. Las siguientes son definiciones de nuevos parámetros y palabras clave:

- Número de lista de acceso: Este es un número de 900 a 999.
- Protocolo: Nombre o número (decimal) de un tipo de protocolo IPX. Esto algunas veces se refiere al tipo de paquete.
- socket fuente: El nombre de socket o numero (hexadecimal) en el cual el paquete está siendo enviado.
- socket destino: El nombre de socket o numero (hexadecimal) en el cual el paquete está siendo recibido.
- Log (opcional): Regitros de violaciones de control de listas de acceso IPX siempre que un paquete corresponda a una entrada de lista de acceso en particular. La

[45] En el prompt de *Router#* en modo EXEC privilegiado introducir el comando *configure terminal.*

información de los registros incluye, dirección fuente y destino, socket fuente y destino, tipo de protocolo y una acción tomada (permitir o negar).

Se utiliza el siguiente comando para activar la lista de acceso extendida IPX en una interfaz:

Router(config-if)#*ipx access-group* numero de lista de acceso {*in* | *out*}

6.8.6 OPERACION NORMAL DE IPX SAP

Los broadcast SAP sincronizan la lista de servicios disponibles. El servidor de archivos NetWare actúa como un ruteador IPX. El ruteador actúa como un ruteador SAP.

Si el ruteador pasa un SAP cada vez que éste recibe uno, el enlace WAN se satura con el tráfico SAP. El ruteador no reenviará los broadcast SAP.

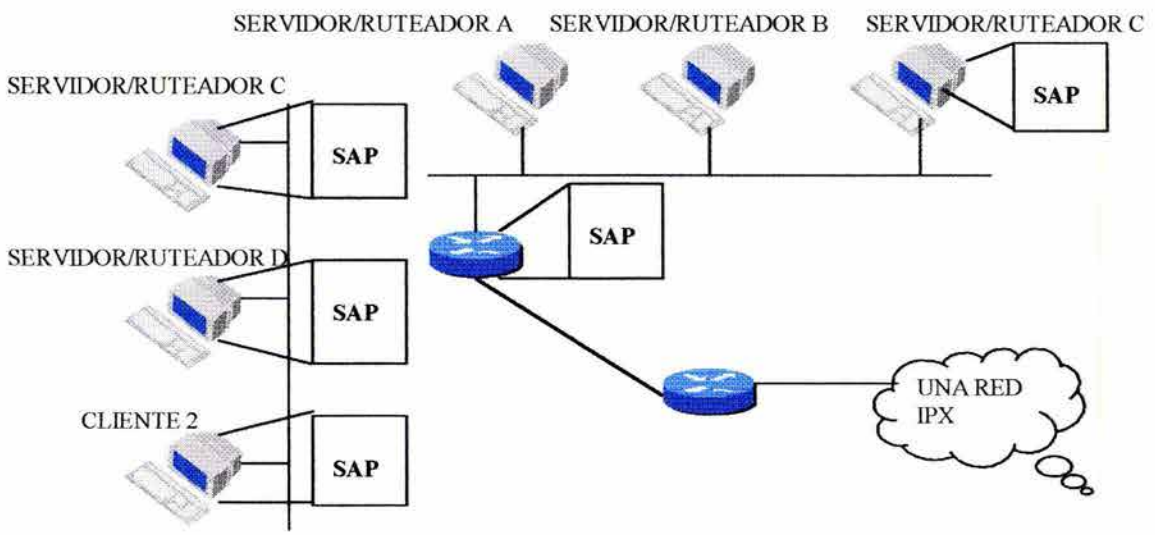
En lugar de eso, los servidores de archivos y ruteadores escuchan los mensajes de SAP y construyen una tabla de SAP, como muestra la figura 6.71. Todos los dispositivos que construyen tablas SAP publican esa información cada 60 segundos. Sobre un enlace WAN el intervalo de 60 segundos de SAP puede ser cambiado. Sin embargo, es posible que otros dispositivos IPX no soporten ese cambio.

Para cambiar el intervalo de actualización SAP, se utiliza el siguiente comando:

ipx-sap-interval intervalo

donde el intervalo entre actualizaciones SAP enviadas por el ruteador son especificadas en minutos. El valor por defecto es 1 minuto. Si el intervalo es 0 las actualizaciones periódicas nunca se envían.

FIGURA 6.71



6.8.7 USO DE LOS FILTROS SAP

Se debe tener un plan de filtrado SAP antes de configurar éste. Hay que estar seguros que los clientes verán las publicaciones necesarias para su proceso de aplicación. Se necesitará incorporar los filtros SAP en todos los ruteadores en los cuales se desee que los filtros funcionen. La siguente tabla lista los numeros SAP más comunes.

NUMERO SAP	TIPO DE SERVIDOR
4	Servidor de archivos NetWare
7	Servidor de Impresión
278	Servidor de Directorio NetWare

Se ubican los filtros SAP cerca del ruteador. La ubicación apropiada de los filtros SAP conserva el ancho de banda crítico, especialmente en los enlaces seriales.

La siguiente lista provee un ejemplo de los objetivos de los filtros:

- Negar tipo 7 (servidor de impresión) SAP de 2a.
- Negar tipo 98 (servidor de acceso) SAP de 5b.
- Negar tipo 24 (ruteador) SAP a 7c.
- Negar tipo 4 (servidor de archivo) SAP de 4a.
- Negar tipo 26a (NMS[46]).

Cuando las publicaciones SAP llagan a la interfaz del ruteador, el contenido toma lugar en la porción de la tabla de ruteo de la memoria principal. El contenido de la tabla es propagada durante la próxima actualización SAP.

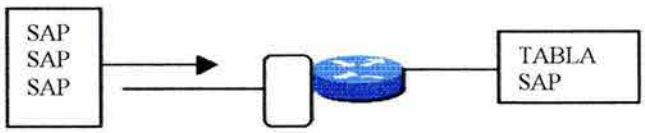
La figura 6.72 muestra dos tipos de filtros de lista de acceso que controlan el tráfico SAP:

- Filtro SAP IPX de entrada: Cuando un filtro SAP de entrada tiene lugar, el número de servicios que tiene la tabla SAP son reducidos. Las actualizaciones SAP propagadas representan una tabla entera pero contiene sólo una subred de todos los servicios. Se utiliza este tipo de filtro cuando se desee reducir el tamaño de la tabla SAP.
- Filtro SAP IPX de salida: Cuando un filtro SAP de salida tiene lugar, el número de servicios propagados desde la tabla es reducido. Las actualizaciones SAP propagadas representan una porción de la tabla contenida y son un subconjunto de servicios. Cuando se utiliza este filtro, el ruteador aún contiene una lista de los servicios conocidos.

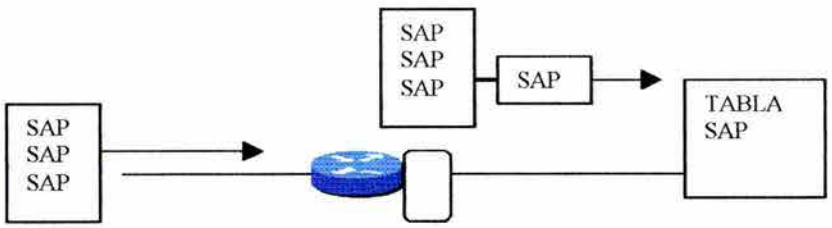
[46] Network Management System.

FIGURA 6.72

FILTRO DE ENTRADA: NO AGREGAR LOS SAP FILTRADOS A LA TABLA SAP



FILTRO DE SALIDA: NO AGREGAR LOS SAP FILTRADOS A LA TABLA SAP ENVIADA



6.8.8 COMANDOS DE CONFIGURACION DE FILTROS SAP

Se utiliza el comando *access-list* para controlar la propagación de mensajes SAP como sigue:

Router(config)#*access-list* número de lista de acceso {*permit* | *deny*} red [nodo] [máscara de red máscara de nodo] [tipo de servicio [nombre servidor]]

donde los parámetros y parámetros clave tienen los siguientes significados:

- Número de lista de acceso: Número de 1000 a 1099. Indica una lista de filtros SAP.
- red [nodo]: Número de red interno fuente de Novell con un número de nodo opcional.
- Máscara de red y máscara de nodo: Máscara a ser aplicada a la red y al nodo.
- Tipo de servicio: Tipo de servicio SAP a filtrar. Cada tipo de servicio SAP es identificado por un número hexadecimal.
- Nombre de servicio: Nombre de servicio provisto.

Los comandos *ipx input-sap-filter* y *ipx output-sap-filter* ubican un filtro SAP en una interfaz. El uso de *input* y *output* determina si los SAP son filtrados antes de entrar en la tabla SAP o si el contenido de la tabla SAP es filtrado durante la próxima actualización.

Router(config-if)#*ipx output-sap-filter* número de lista de acceso
Router(config-if)#*ipx intput-sap-filter* número de lista de acceso

¿Por qué se utilizaría un filtro SAP en lugar de otro? Considerar, por ejemplo, un ruteador que conecta dos redes Ethernet (E0 y E1) y dos enlaces seriales (S0 y S1). Suponer que se quiere que los dispositivos en los puertos LAN (E0 y E1) conozcan acerca de los servicios locales, pero no se quieren los mismos servicios publicados sobre los enlaces seriales, en este caso se utilizaría un filtro SAP de salida para S0 y S1.

El contenido de la tabla SAP puede ser filtrado en la salida utilizando el comando *ipx router-sap-filter*, el cual identifica desde qué ruteador las actualizaciones SAP son recibidas. Hay que notar que sólo una de las tres clases de filtros SAP puede ser activada en una interfaz.

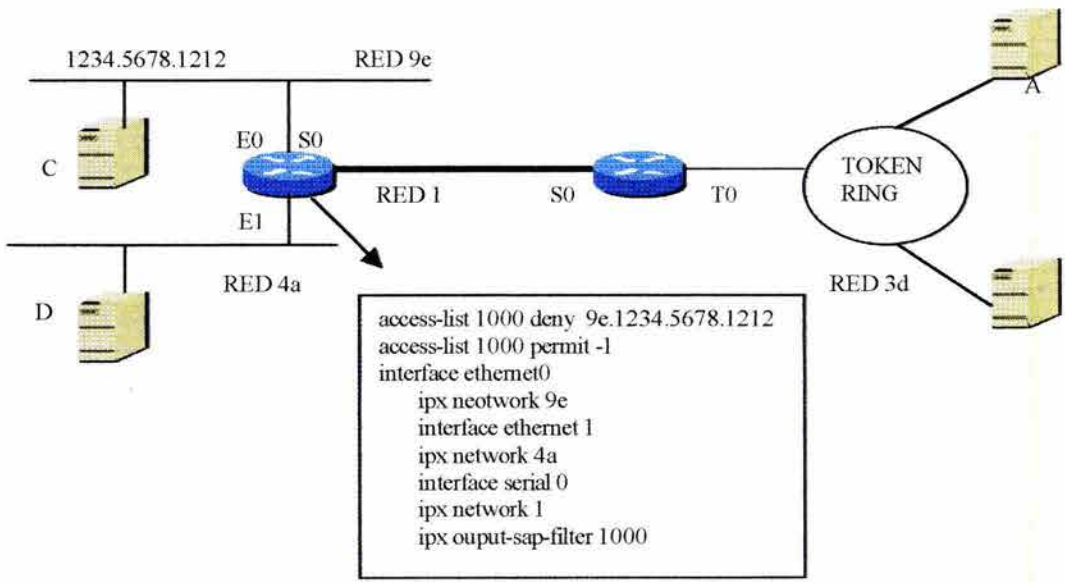
6.8.8.1 EJEMPLO 1: FILTRADO DE SAP EN SALIDA

En la figura 6.73, el administrador de red quiere prevenir que publicaciones del servidor de archivos desde el servidor C sean enviadas por la interfaz serial (S0). Todos los otros servicios SAP de alguna fuente deben ser reenviados a la interfaz (S0). La configuración para lograr esto está en la figura 6.73.

Los detalles del comando *access-list 1000 deny* son los siguientes:

- 1000: Número de lista de acceso en el rango de filtros SAP
- deny: Los servicios SAP que corresponden con los parámetros seleccionados serán bloqueados.
- 9c.1234.5678.1212: Dirección de red fuente de publicaciones SAP
- 4: Tipo de servicio SAP.

FIGURA 6.73



Los detalles del comando *access-list permit -1* son los siguientes:

- 1000: Número de lista de acceso.
- Permit: Los filtros SAP que corresponden a los parámetros corresponden serán reenviados.
- -1: Número de red fuente; -12 significa todas las redes.

El comando *ipx output-sap filter- 1000* tomó lugar en la lista de acceso 1000 en la interfaz S0 como un filtro SAP de salida. Por la aplicación de la lista como una interfaz de salida, se pueden restringir las publicaciones en el enlace serial.

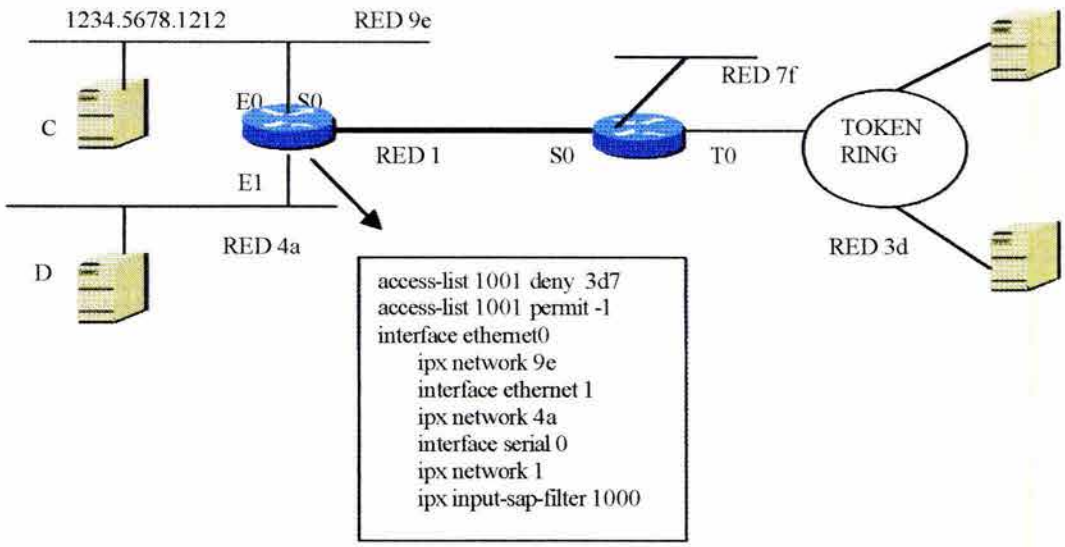
El servidor C en la figura 6.73 está en la esquina superior izquierda. Específicamente, la red *9e* es la fuente con dirección MAC terminando en 1212. El identificador completo para el servidor es 9e1234.5678.1212. El valor 4 en el final de la primera línea de lista de acceso identifica el tipo de servicio. Este valor indica un servidor de archivo de publicaciones SAP. Entonces la línea de completa niega el servicio de publicaciones de archivos del servidor 9e.1234.5678.1212, fuera del ruteador.

El comando *access-list 1000 permit -1* permite que todas las publicaciones se propaguen en la interfaz serial.

6.8.8.2 EJEMPLO 2: FILTRO SAP DE ENTRADA

En la figura 6.74, publicaciones de servidor de impresión desde los servidores A y B no son incorporadas en la tabla SAP. Todos los otros servicios de alguna fuente serán añadidos a la tabla SAP. Notar que la primera línea de lista de acceso especifica el tipo de servicio 7, servidor de impresión. Notar también que el comando *ipx input-sap-filter 1001*, el cual tiene lugar en la lista de acceso 1001 en la interfaz S0 como un filtro SAP de entrada.

FIGURA 6.74



6.8.9 VERIFICANDO LAS LISTAS DE ACCESO IPX

El comando *show ipx interface* despliega información acerca de la interfaz. La figura 6.75 muestra que el filtro de entrada es 800 y el filtro de salida es 801.

También en la figura figura 6.75 el comando *show access-list* despliega el contenido de las listas 800 y 801.

FIGURA 6.75

```
Router#show ipx interface1/1

Ethernet 1/1 is up, line protocol is up
   IPX address is 10.0000.0c0d.724f, NOVELL-ETHER [up]
   Delay of this IPX network, in ticks is 1 through 0 link delay 0
   IPXWAN processing not enabled on this interface.
   IPX SAP update interval is 1 minute(s)
   IPX Type 20 propagation packet forwarding is disabled
   Incoming access list is not set
   Outgoing access list is not set
   IPX helper access list is not set
   SAP GNS processing enabled, delay 0 ms, output filter list is not set
   SAP input filter list is not set
   SAP output filter list is not set
   SAP router filter list is not set
   Input filter list is 800
   Output filter list is 801
                          *
```

```
dtp-19#show access-list
IPX access list 800
     deny 8000
IPX access list 801
      deny all
```

CAPITULO 7

INTRODUCCION A LAS CONEXIONES WAN

En este capítulo discutiremos los servicios de WAN y cómo el usuario utiliza los servicios de telefonía para la red. También se discuten las descripciones y configuraciones de Point- to Point Protocol (PPP), X.25 y Frame Relay como protocolos de WAN.

7.1 SERVICIOS DE WAN

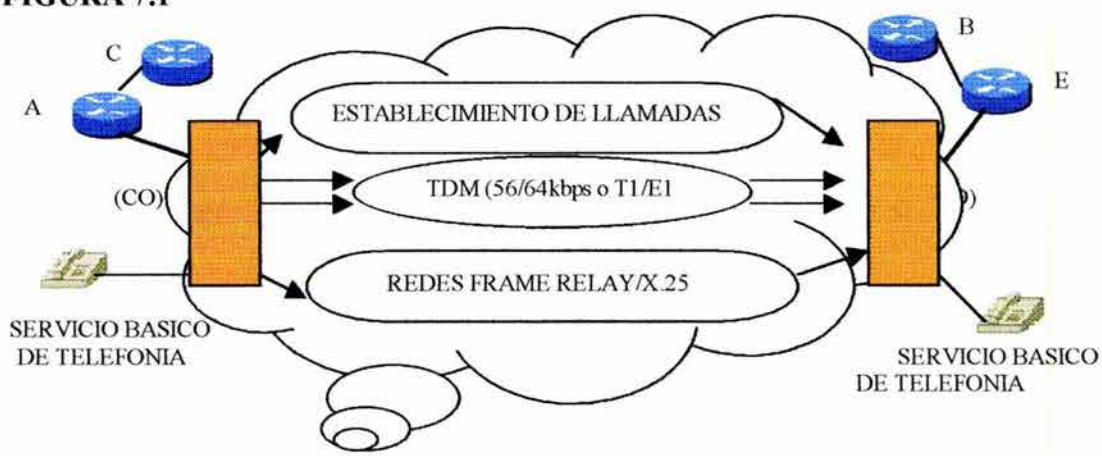
El servicio telefónico es los servicios de WAN más utilizado. El servicio telefónico y el servicio de datos son ruteados por medio de la interfaz de premisas del cliente[47] con la nube de proveedor de servicios a una oficina central (CO), como muestra la figura 7.1.

La descripción de la nube WAN organiza los servicios del proveedor en tres pricipales tipos:

- Servicios de establecimiento de llamadas
- Multiplexación por división de tiempo.
- Servicio de X.25 y Frame Relay

El servicio de establecimiento de llamadas fija conexiones entre puntos finales. Por ejemplo, cuando una sucursal necesita intercambiar datos con su coporativo, el proceso de establecimiento de llamadas fija una conexión entre los dos ruteadores en cada punto del enlace WAN. Un vez que la conexión está establecida, el enlace puede ser utilizado para la transferencia de datos.

FIGURA 7.1



[47] Una interfaz que se encuentra en la organización solicitadora del servicios WAN. Se explicará más adelante.

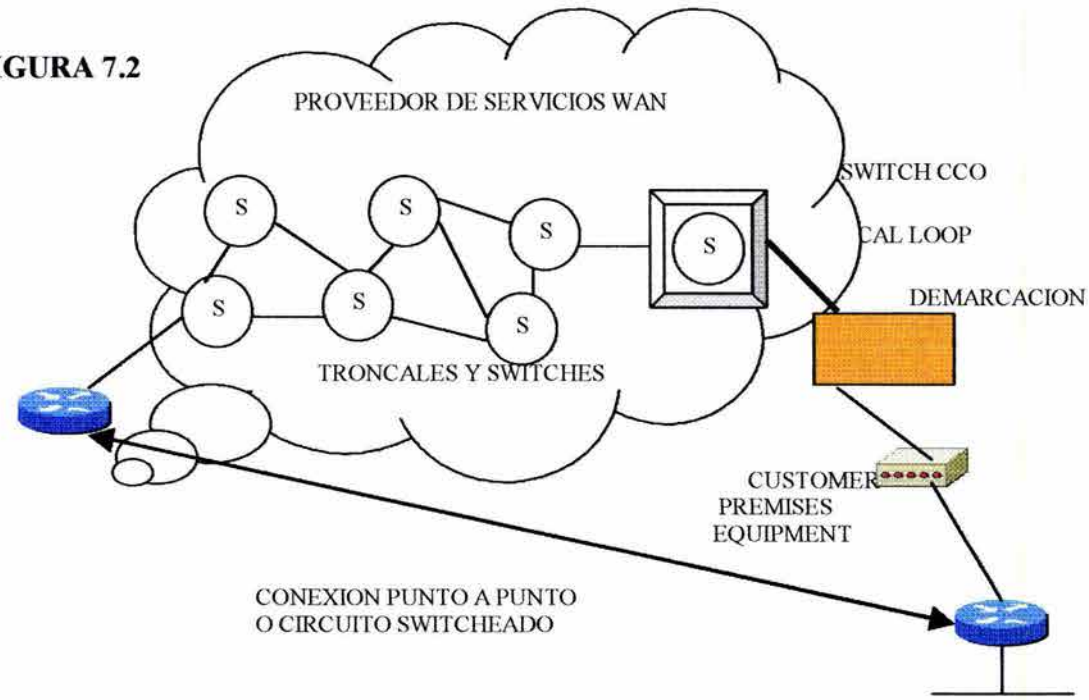
En TDM, la información de múltiples fuentes tiene asignación de ancho de banda en cada medio simple. Un circuito switcheado[48] utiliza señalización para determinar la ruta, la cual es un camino dedicado entre el transmisor y receptor. Por multiplexación de tráfico en *time slots*[49] fijos, el TDM evita las facilidades de congestión y retardos variables: el servicio de telefonía básica e Integrated Services Digital Network (ISDN) utiliza circuitos TDM.

En los servicios X.25 y Frame Relay, la información contenida en paquetes o frames comparten un ancho de banda con otros datos a lo largo del enlace WAN. Los paquetes switcheados X.25 utilizan el ruteo de capa 3 en el direccionamiento del transmisor contenido en el paquete. Frame Relay utiliza identificadores de capa dos y circuitos permanentes virtuales (PVC).

7.1.1 INTERCONECTANDO CON LOS PROVEEDORES DE SERVICIOS WAN

Cuando una organización se subscribe a un proveedor de servicios WAN, el proveedor asigna parámetros a la organización para conectar llamadas de WAN. La organización realiza conexiones a destino como llamadas punto a punto, como en la figura 7.2.

FIGURA 7.2



[48] Permite conexiones que pueden ser iniciadas cuando es necesario y terminadas cuando la conexión es completada. El servicio telefónico es un ejemplo.
[49] Canales dentro de un enlace. Un enlace E1 tiene 32 canales o *time slots*.

Los términos más comúnmente utilizados para las principales partes de un usuario-proveedor de servicios WAN son:

- Customer Premises Equipment (CPE)
- Demarcación
- Local Loop
- Switch CO
- Red Toll

7.1.1.1 CUSTOMER PREMISES EQUIPMENT

Son dispositivos localizados en el terreno de la organización solicitadora de servicios WAN. Ellos incluyen los dispositivos propios de la organización solicitadora o los dispositivos prestados por el proveedor de servicios. Por ejemplo, terminales, teléfonos y módems que se conectan al proveedor de servicios son considerados un CPE. La organización solicitadora debe saber la manera en que el CPE se conecta con el proveedor de servicios.

7.1.1.2 DEMARCACION

El punto de demarcación del CPE con la porción del Local Loop del servicio que comienza. El punto de demarcación a menudo tiene lugar en el cuarto de telecomunicaciones.

7.1.1.3 LOCAL LOOP

El Local Loop consiste en el cableado (usualmente de cobre) que se extiende desde el punto de demarcación hasta CO del proveedor de servicios. El Local Loop algunas veces se conoce como *última milla*.

7.1.1.4 SWITCH DE CO

Es una facilidad de switcheo que provee el punto de prescencia más cercano para el servicio de WAN.
La oficina central (CO) actúa como:

- Un punto de entrada a la nube WAN para realizar una llamada.
- Un punto de salida desde la WAN para los dispositivos que llaman.
- Un punto de switcheo para llamadas.

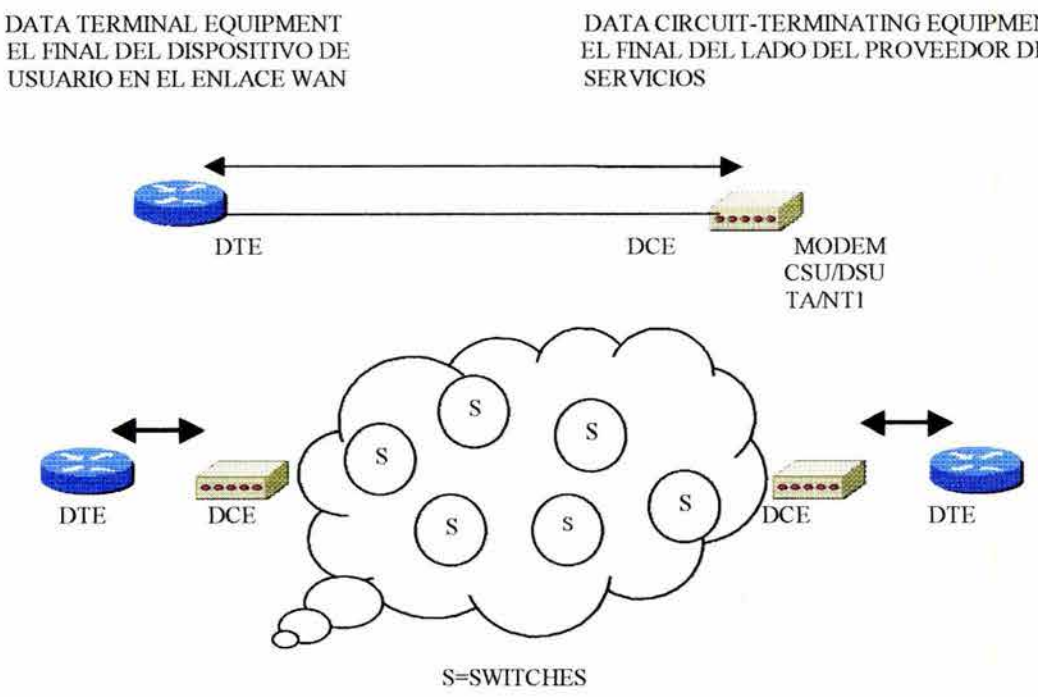
7.1.1.5 RED TOLL

Una colección de switches y facilidades (troncales) dentro de la nube WAN.

7.1.2 DE LA ORGANIZACIÓN SOLICITADORA A LA INTERFAZ DEL PROVEEDOR DE SERVICIOS

Una interfaz clave en el *customer premises* ocurre entre el Data Teminal Equipment (DTE) y el Data Circuit-Terminatig Equipment (DCE), como muestra la figura 7.3. La porción de debajo de la figura 7.3 representa el DTE/DCE a cada punto final de la red switcheada WAN.

FIGURA 7.3



Típicamente, el DTE es el ruteador donde reside la aplicación de switcheos de paquetes. El DTE es el dispositivo utilizado para convertir los datos en una forma aceptable para la facilidad del servicio WAN. Como muestra la figura 7.3, el DCE puede ser un MODEM, un Channel Unit/Service Unit (CSU/DSU) o un Terminal Adapter/Network Termination 1 (TA/NT1)[50].

La comunicación de los datos sobre la WAN conectan los DTEs y ellos pueden compartir recursos. El camino entre los DTEs se llama enlace, circuito, canal o línea. El DCE primeramente provee la interfaz en el enlace de comunicación en la nube WAN. La interfaz actúa como límite donde la responsabilidad para el tráfico pasa entre la organización solicitadora y el proveedor de servicios.

[50] Dispositivos pertenecientes a la tecnología de WAN ISDN.

La interfaz DTE/DCE utiliza uno de varios protocolos disponibles tal como EIA/TRA 232 o X.25. Esos protocolos establecen los códigos que los dispositivos utilizan para comunicarse entre ellos. La comunicación determina la manera en que el establecimiento de llamadas opera y la manera de cruzar la red WAN.

Data Switching Equipment (DSE) es un término adicional que algunas veces se utiliza para describir los componentes del switch que aparecen en la nube WAN. El DSE conecta el tráfico de varias fuentes a su destino final a través de otros switches.

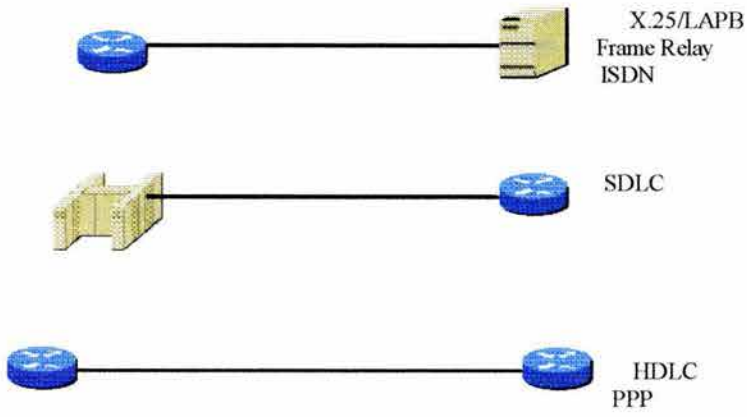
7.1.3 UTILIZANDO LOS SERVICIOS WAN CON RUTEADORES

Se puede acceder de tres formas a los servicios WAN con ruteadores:

- La primera forma utiliza los servicios switcheados y retransmitidos. Ejemplos de esta forma de WAN incluyen X.25, Frame Relay e ISDN.
- La segunda forma provee una interfaz a los mainframes de IBM. Esta forma de WAN utiliza Synchronous Data Link Control (SDLC) para conexiones punto a punto y punto multipunto de dispositivos remotos al mainframe central.
- Con la tercera forma se puede acceder a los servicios de WAN utilizando protocolos que conectan dispositivos iguales. Esta forma utiliza encapsulación High-Level Data Link Control (HDLC) o encapsulación PPP[51] en los dispositivos. También esta forma de WAN puede utilizar Dial-on-Demand Routing (DDR) como opción.

La figura 7.4 muestra esas tres formas de servicio WAN.

FIGURA 7.4



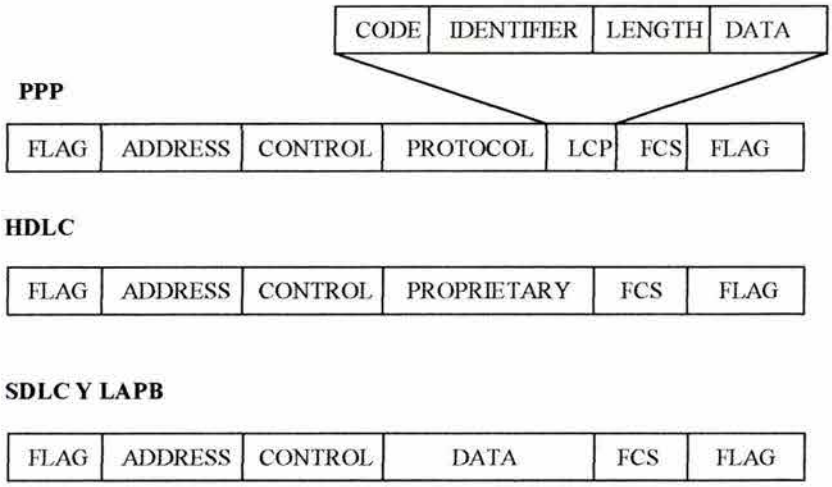
[51] Pont-to-Point Protocol. Este protocolo se revisará más adelante

7.1.4 RESUMEN DEL FORMATO DE FRAME WAN

Las diferentes formas de servicios WAN disponibles con los ruteadores utilizan diferentes tipos de frames. Si el tipo de frame por defecto no es utilizado se debe especificar el framing necesario.

La figura 7.5 muestra las diferencias entre los tipos de frames WAN comúnmente utilizados.

FIGURA 7.5



LAPB, utilizado por X.25, es un derivado de HDLC. HDLC es un protocolo de enlace de datos que encapsula el dato en enlaces seriales asíncronos. Frame Relay utiliza una variación de HDLC.

HDLC no soporta multiprotocolos en un enlace simple porque no tiene un estándar para indicar cuál protocolo está funcionando. El frame HDLC de Cisco utiliza un campo de tipo propietario que actúa como un campo protocolo, el cual hace esto posible para múltiples protocolos de capa de red para compartir el mismo enlace serial.

PPP extiende el frame HDLC básico incorporando un campo de protocolo. El campo de protocolo identifica el protocolo encapsulado en el campo de información del frame.

Los campos PPP tienen herencia de algunos atributos que no son comúnmente utilizados. Por ejemplo, el campo dirección es asignado en la secuencia binaria 11111111, la dirección broadcast estándar.

El Link Control Protocol (LCP) utilizado por PPP provee un método de establecimiento configuración, mantenimiento y terminación de la conexión punto a punto.

7.2 UNA DESCRIPCION DE POINT-TO POINT PROTOCOL (PPP)

Los desarrolladores de Internet diseñaron PPP para hacer la conexión de enlaces punto a punto. PPP, originalmente descrito por RFC 1661 y 1332, encapsula la información del protocolo de capa de red sobre enlaces punto a punto.

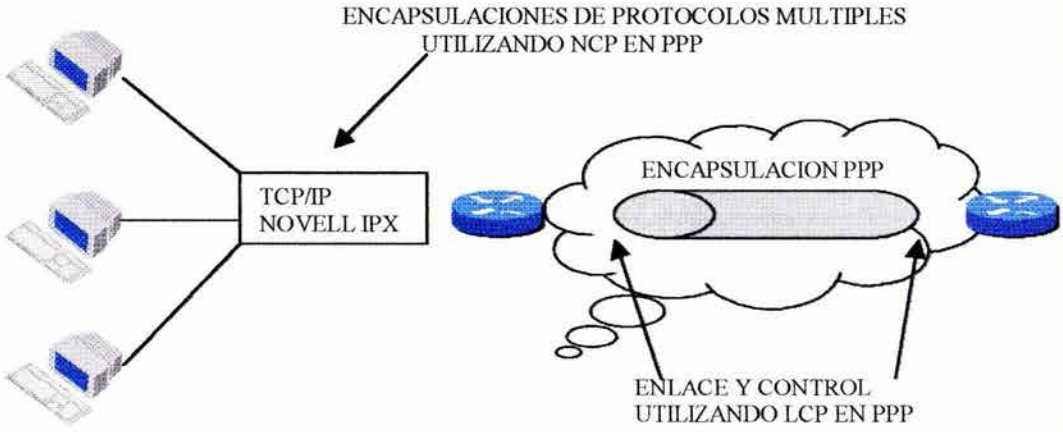
Se puede configurar PPP en los siguientes tipos de interfaz física:

- Serial asíncrono.
- HSSI (High-Speed Serial Interface)
- ISDN
- Serial síncrono

PPP utiliza su componente Network Control Protocol (NCP) para encapsular múltiples protocolos. Como muestra la figura 7.6. Este uso de NCP sobrepasa los límites del predecesor de PPP, Serial Line IP (SLIP), el cual sólo podría fijar transporte para paquetes IP.

PPP utiliza otro componente, Link Control Protocol (LCP) para negociar y fijar opciones de control en el enlace WAN.

FIGURA 7.6

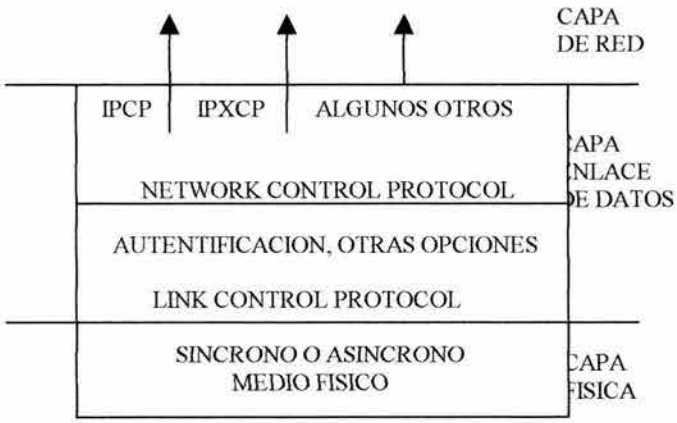


7.2.1 ELEMENTOS DE CAPA PPP

PPP utiliza una arquitectura en capas, como muestra la figura 7.7. Con las funciones de las capas más bajas, PPP puede utilizar:

- Un medio físico síncrono como los que conectan ISDN.
- Un medio físico asíncrono como los que utiliza el servicio básico de telefonía para las conexiones de modem.

FIGURA 7.7



PPP ofrece un conjunto amplio de servicios que controlan un enlace de datos. Estos servicios son opciones en LCP y son primeramente negociación y revisión de frame para implementar los controles punto a punto que un administrador especifica para la llamada.

Con esas funciones de alto nivel, PPP lleva los paquetes de varios protocolos de capas de red en NCP. Esos son campos funcionales que contienen códigos estandarizados para indicar el tipo de protocolos de capa de red que PPP encapsula.

7.2.2 OPCIONES DE CONFIGURACIÓN DE LCP

RFC 1548 describe la operación PPP y opciones de configuración LCP. Los ruteadores que utilizan encapsulación PPP incluyen las opciones LCP mostradas en la siguiente tabla:

CARACTERISTICA	CÓMO OPERA	PROTOCOLO
Autentificación	Requiere un password Lleva a cabo un intercambio de saludos	PAP CHAP
Compresion	Compresion de datos en fuente; Reproducción de datos en destino	Stacker Predictor
Detección de error	Monitoreo de datos caidos en el enlace Evita el retorno de frames	Calidad Numero Mágico
Multilink	Balanceo de carga a través de multiples enlaces	MP

Las opciones de autentificación requiere que el lado que realiza la llamada en el enlace introduzca información que ayude a garantizar que el que relizó la llamada tenga el permiso del administrador de red para hacer ésta. Los ruteadores iguales intercambian mensajes de autentificación. Hay dos alternativas:

- Password Authetification Protocol (PAP).
- Challange Handshake Authetification Protocol (CHAP).

Para una major seguridad el Cisco IOS Release 11.1 ofrece *callback* sobre PPP. Con esta opción LCP, un ruteador puede actuar como un cliente *callback* o un servidor *callback*.

El cliente realiza un llamado DDR para ser regresado y terminado. El servidor *callback* responde la llamada inicial y regresa la llamada al cliente basado en su declaración de configuración.

Las opciones de compresión incrementa la tasa promedio de paquetes recibidos existosamente en las conexiones PPP por la reducción de la cantidad de datos en el frame que deberá viajar a través del enlace. El protocolo descompresiona el frame en su destino.

Dos protocolos de compresión de compresión disponibles en los ruteador son Stacker y Predictor.

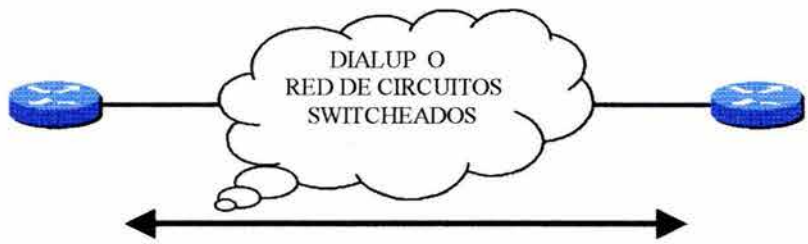
Los mecanismos de error de protección con PPP habilitan un proceso para identificar condiciones de falla. La calidad y número mágico ayudan a garantizar un confiable enlace de datos.

Los Cisco IOS Release 11.1 y superiores soportan *multilink PPP*. Esta alternativa provee balanceo de carga sobre interfaces del ruteador que PPP utiliza

7.2.3 ESTABLECIMIENTO DE SESION PPP

El establecimiento de una sesión PPP tiene tres fases como lo muestra la figura 7.8.

FIGURA 7.8



ESTABLECIMIENTO DE SESION PPP

1. FASE DE ESTABLECIMIENTO DE ENLACE
2. FASE DE AUTENTIFICACION OPCIONAL
3. FASE DE PROTOCOLO DE CAPA DE RED

FASE 1: ESTABLECIMIENTO DE ENLACE

En esta fase, cada dispositivo PPP envía paquetes LCP para probar y configurar el enlace. Los paquetes contienen un campo Configuration Option que permite a los dispositivos que negocien en el uso de opciones como, la unidad de máxima recepción, la compresión de ciertos campos PPP y el protocolo de autentificación de enlace.

FASE 2: AUTENTIFICACIÓN (OPCIONAL)

Después de que el enlace es establecido y el protocolo de autentificación tiene lugar, los dispositivos son autentificados. La autentificación, si se utiliza, tiene lugar antes de entrar en la fase de protocolos de capa de red.

FASE 3: PROTOCOLO DE CAPA DE RED

En esta fase, los dispositivos PPP envían paquetes NCP para elegir y configurar uno o más protocolos de capa de red, tal como IP. Después de que los protocolos de red elegidos son configurados, datagramas de cada protocolo pueden ser enviados sobre el enlace. PPP soporta varios protocolos de red incluyendo IP e IPX.

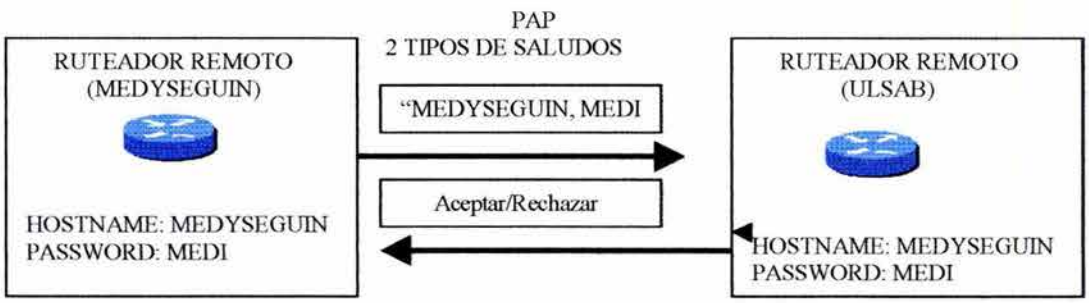
7.2.4 SELECCIONANDO UN PROTOCOLO DE AUTENTIFICACION PPP

Cuando se configura la autentificación PPP, se puede seleccionar PAP o CHAP. CHAP es el protocolo preferido.

7.2.4.1 PAP

PAP provee un método simple para un nodo remoto para establecer su identidad utilizando dos tipos de saludo, como lo muestra la figura 7.9. PAP se hace solamente sobre el establecimiento del enlace inicial.

FIGURA 7.9



Después de que la fase de establecimiento de enlace PPP es completa, un nombre de usuario/password es repetidamente enviada por el nodo remoto al ruteador hasta que la autentificación es reconocida o la conexión terminada.

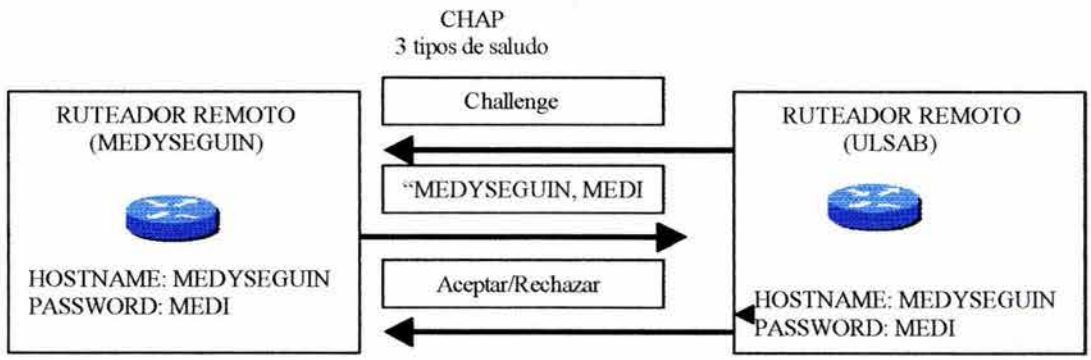
PAP no es un protocolo de autentificación robusta. Los passwords son enviados a través del enlace y no hay protección para ataques de errores. Se debe utilizar PAP cuando un dispositivo que requiere autentificación no soporte CHAP.

7.2.4.2 CHAP

CHAP es utilizado en el inicio del enlace y periódicamente verifica la identidad del nodo remoto utilizando tres tipos de saludo.

Después que la fase de establecimiento es completada, el ruteador local envía un mensaje *challenge* al nodo remoto. El nodo remoto responde con un número ID encriptado, un password secreto y un número aleatorio. El ruteador local revisa el valor de la respuesta de acuerdo a su cálculo, la autentificación es reconocida, si no, la conexión es terminada inmediatamente. La figura 7.10 resume este preceso.

FIGURA 7.10

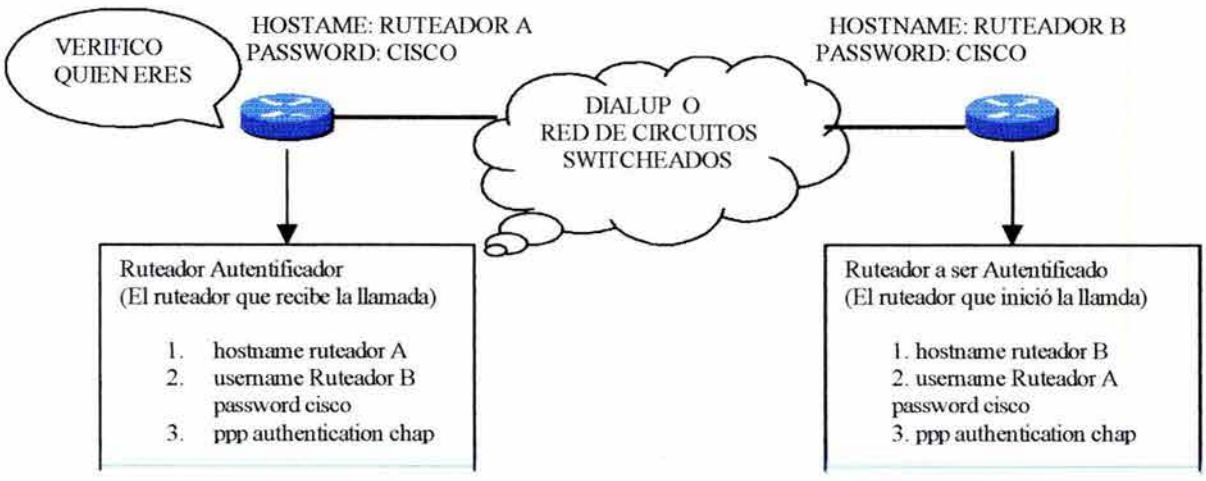


Se utiliza le comando *debug ppp authentication* para desplegar la secuencia de intercambio como va ocurriendo.

7.2.5 CONFIGURANDO LA AUTENTIFICACION PPP

Los ruteadores en cada lado de la WAN deben ser configurados para autentificación PPP, como lo muestra la figura 7.11.

FIGURA 7.11



Para configurar la autentificación PPP, se debe hacer lo siguiente:

1. En cada ruteador se define un nombre de usuario. El formato del comando es:

   Router(config)# *username* nombre *password* secreto

donde los parámetros y palabras clave significan los siguiente:

- Nombre: Este es el nombre del host del ruteador remoto.
- Secreto: En los ruteadores, el password secreto debe ser el mismo en ambos ruteadores.

Añadir una entrada de nombre de usuario para cada sistema remoto que se comunica con el ruteador local y requiere de auntentificación. El dispositivo remoto debe también tener un nombre de usuario para el ruteador local.

Para habilitar al ruteador local para que responda los *chap challenges*, un nombre de usuario debe ser el mismo que el nombre del host.

2. Entrar al modo de configuración de interfaz de la interfaz deseada.
3. Configurar la interfaz para la encapsulación PPP

   Router(config)#encapsulation PPP

4. Configurar la autentificación PPP

   Router (config)#ppp authentication {chap | chap pap | pap chap | pap}

Hay cuatro diferentes opciones disponibles para la autentificación PPP:

- CHAP solo
- CHAP y PAP
- PAP y CHAP
- PAP solo

Si la opción PAP y CHAP está habilitada, el primer método especificado será solicitado durante la negociación del enlace. Si uno de los dispositivos sugiere utilizar el segundo método o simplemente rechaza el primero, el segundo método será utilizado.

Los siguientes comandos podrán ser utilizandos para simplificar las tareas de configuración CHAP en el ruteador:

- Utilizando el mismo nombre en múltiples ruteadores. Cuando se quiere que los usuarios remotos piensen que están conectados al mismo ruteador cuando se autentifique y configure el mismo nombre del host en el ruteador.

  Router(config)#*ppp chap hostname* nombre del host

- Utilizando un password para autentificar a un ruteador desconocido. Para limitar el numero de entrada nombre de usuario/password en el ruteador, configurar un password que será enviado a los host que se quiere que el ruteador autentifique.

  Router(config)#*ppp chap password* secret

7.2.6 VERIFICANDO PPP

Cuando PPP es configurado, se puede revisar el estado de LCP y NCP utilizando el comando *show interfaces*.

7.3 CONFIGURANDO X.25

Esta sección presenta una descripción del protocolo X.25 y explica la manera en que los paquetes son direccionados y encapsulados en X.25. También se revisa la configuración y monitoreo.

7.3.1 DESCRIPCION DE X.25

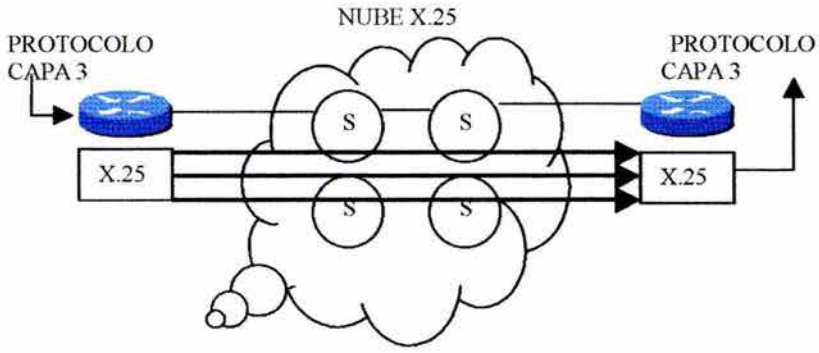
X.25 es un estándar que define una conexión entre una terminal y una red de paquetes switcheados. Virtualmente cada nación utiliza alguna red X.25.

Se diseñó X.25 para transmitir y recibir datos entre terminales tontas a través de líneas telefónicas. X.25 habilita a las terminales tontas para accesar remotamente aplicaciones almecenadas en Mainframe y minicomputadoras.

Como las nuevas aplicaciones necesitan comunicación LAN-to-WAN-to-LAN, los ingenieros diseñaron más nuevas formas de tecnología WAN: ISDN y Frame Relay. En algunas situaciones esas tecnologías remplazan a X.25

Algunos protocolos de capa de red pueden ser transmitidos a través de circuitos virtuales X.25, este proceso es llamado *Tunneling*. En *Tunneling*, los datagramas u otros paquetes de capa 3 son encapsulados para su transporte a través de una red WAN vía circuitos virtuales X.25 (ver figura 7.12). Cada paquete de capa 3 mantiene el direccionamiento para su protocolo respectivo.

FIGURA 7.12



X.25 soporta los siguientes tipos de comunicación:

- IP
- Apple Talk
- Novell IPX
- Banyan VINES
- XNS
- DECnet
- ISO-CLN
- Apollo
- Compressed TCP
- Bridging

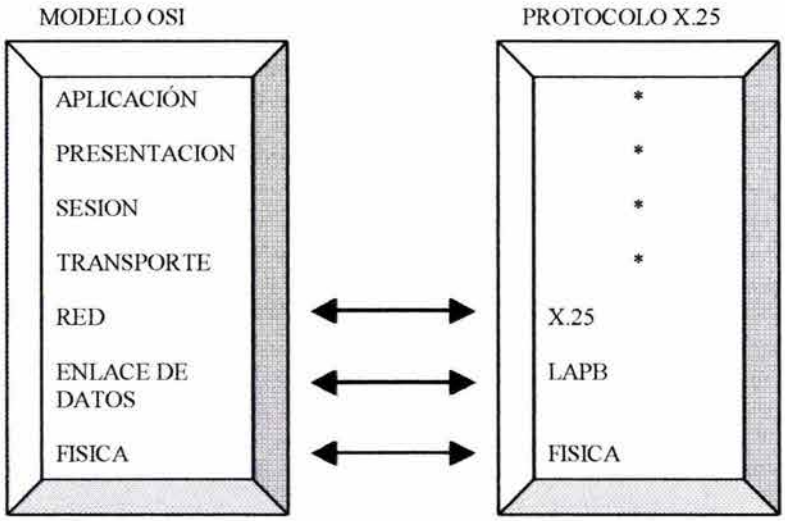
7.3.2 PROTOCOLOS X.25

El conjunto de paquetes switcheados X.25 se comparan con las capas inferiores del modelo OSI, como lo muestra la figura 7.13.

En general, se puede pensar de X.25 como una sobrerreingeniería de enlace de datos en el mundo de las interredes. X.25 en capa 3 y Link Access Procedure Balanced (LAPB) en capa 2 proveen confiabilidad.

La capa 3 y la capa 2 fueron diseñadas con un control de flujo robusto y revisión de errores para reducir el requerimiento para las funciones externas a X.25.

FIGURA 7.13



LAPB provee un servicio de datos entre dos puntos.Todos los datos son confirmados y el servicio garantiza la entrega ordenada punto a punto sin caídas ni duplicaciones. Si este servicio no puede entregar, el protocolo se restaura con un conjunto de Modos Balanceados Asíncronos (SABM) o SABM extendido (SABME) que interrumpe el servicio de capa 3.

El Packet Level Protocol (PLP) de X.25 depende del servicio garantizado LAPB. La capa de red provee conexiones multiplexadas sobre una conexión LAPB punto a punto. PLP también garantiza la entrega ordenada sin caídas ni duplicaciones de paquetes. Si el servicio es interrumpido, un VC señala la posible pérdida de dato (RESET) o la caída (CLEAR).

X.25 se desarrolló en tiempos de los circuitos analógicos cuando rangos de errores eran más grandes que hoy en día. Las nuevas tecnologías, como Frame Relay, han tomado ventaja de los rangos de errores.

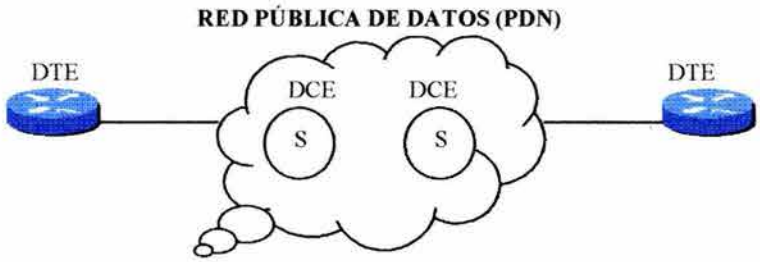
X.25 fue diseñado en tiempos de terminales alfanuméricas. Las demandas en el switcheado de paquetes eran más bajas que hoy. Aplicaciones en estaciones de trabajo demandan más ancho de banda y velocidad. Las tecnologías más nuevas, como ISDN y X.25 sobre Frame Relay, añaden la capacidad de switcheado de paquetes.

7.3.3 DTE Y DCE X.25

Cada estación en una conexión X.25 es un DTE o un DCE. El DTE X.25 es típicamente un ensamblador/desamblador de paquetes (PAD). El DCE X.25 actúa como el límite a la red pública de datos (PDN) en un switch o concentrador. La figura 7.14 ilustra la relación entre DCE y DTE en PDN. El switch X.25 en el sitio del proveedor también es llamado Data Switching Equipment (DSE).

Aunque las terminales DTE y DCE tienen lugar en las tres capas de X.25, el protocolo X.25 implementa circuitos virtuales entre el DTE y el DCE.

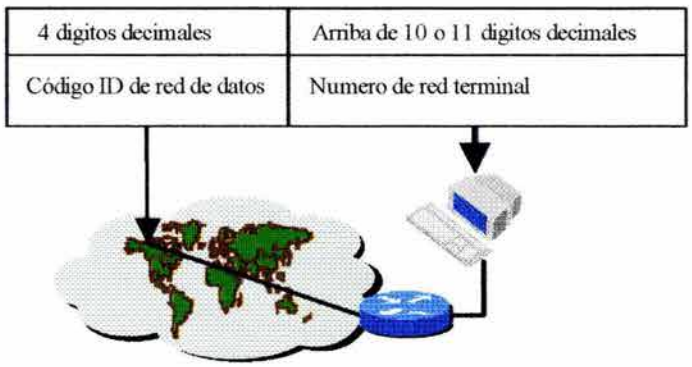
FIGURA 7.14



7.3.4 FORMATO DE DIRECCIONAMIENTO X.25 (X.121)

El formato X.25 es definido por el estándar ITU-T X.121. La figura 7.15 muestra el formato de direccionamiento X.25.

FIGURA 7.15



Los primeros cuatro dígitos especifican el Data Network Identification Code (DNIC). Este es el código del país y el número del proveedor asignado por el ITU.

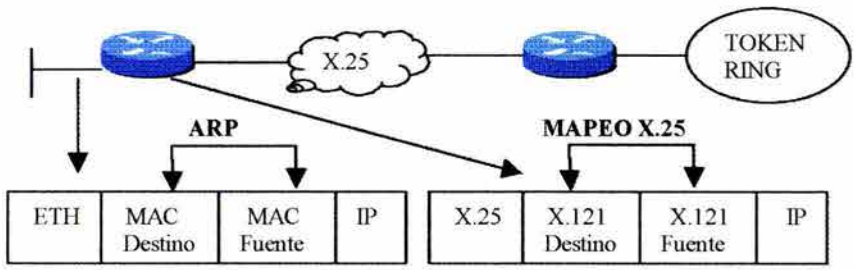
Los diez dígitos restantes especifican el Network Terminal Number (NTN); los primeros 8 dígitos son asignados por el Packet Switched Network (PSN) y los dos últimos dígitos son un número óptimo asignado localmente. Esos dos últimos números podrán ser utilizados para identificar una aplicación o dispositivo en particular. Los primeros 8 dígitos junto con los cuatro dígitos DNIC forman la dirección única dada a usuarios cuando se incorporan en la red X.25.

Para diferentes protocolos de red a conectar a través de X.25, las declaraciones son incorporadas en el ruteador para mapear la dirección de capa de red del próximo salto. Por

ejemplo, una dirección de capa de red es mapeada a una dirección X.121 para identificar el próximo salto a un host al otro lado de la red.

Esas declaraciones son lógicamente equivalentes a Address Resolution Protocol (ARP) que dinámicamente mapea una dirección de capa de red a una dirección MAC de enlace de datos, como muestra la figura 7.16. Los mapeos son requeridos para cada protocolo porque ARP no es soportado por una red X.25.

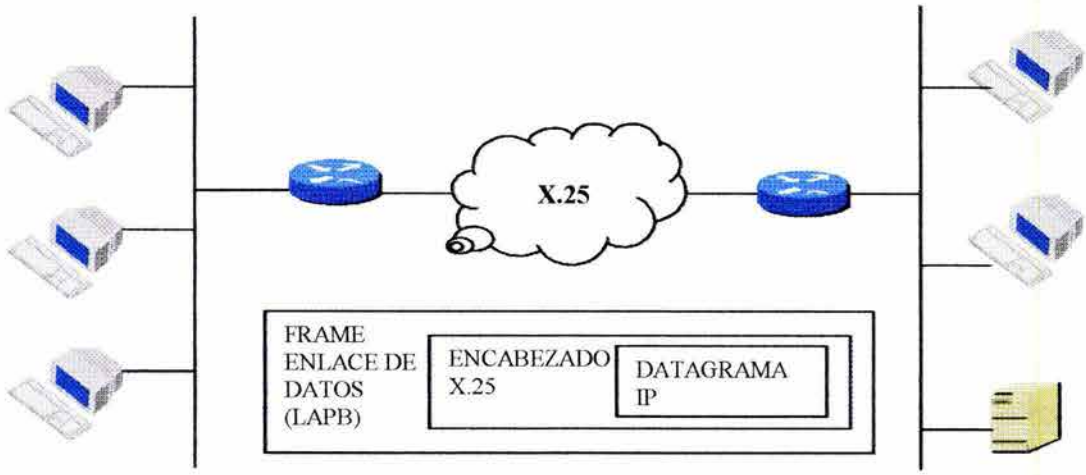
FIGURA 7.16



7.3.5 ENCAPSULACION X.25

El movimiento de datos de capa de red a través de la interred usualmente involucra encapsulación de datagramas dentro de frames, como en la figura 7.17. Como cada frame llega al ruteador y el frame es descartado, el ruteador analiza el datagrama y ocupa un nuevo frame y es reenviado.

FIGURA 7.17



Similarmente, en un ambiente X.25, el frame LAPB llega al ruteador, el cual extrae el datagrama del paquete o paquetes. El ruteador descarta el frame encapsulado y analiza el datagrama para identificar el formato y el próximo salto. Basado en la determinación de la ruta, el ruteador encapsula el datagrama para ser reenviado.

7.3.6 CIRCUITOS VIRTUALES X.25

El término Circuito Virtual (VC) es utilizado intercambiablemente con los términos *Virtual Circuit Number (VCN), logical channel number (LCN)* y *Virtual Channel Identifier (VCI)*.

Un VC puede ser un *Circuito Virtual Permanente (PVC)* o más comúnmente, un *Circuito Switcheado Virtual (SVC)*. Un SVC existe sólo por la duración de la sesión.

Hay tres fases asociadas con SVC:

- Establecimiento de llamadas.
- Transferencia de Información.
- Término de llamadas.

Un PVC es similar a utilizar una línea dedicada. El proveedor de la red y el subscriptor a X.25 debe de hacer disponible el circuito virtual. El PVC no utiliza establecimiento de llamadas ni terminación de éstas, en lugar de eso, el PVC siempre está disponible.

La figura 7.18 muestra los circuitos virtuales a través de una nube X.25.

FIGURA 7.18

El protocolo X.25 ofrece servicios simultáneos a varios host (por ejemplo, mutiplexación). Una red X.25 puede soportar alguna configuración de SVCs y PVCs sobre el mismo circuito físico asociado a la interfaz X.25. Sin embargo, configurar un número grande de VC sobre una interfaz serial podría resultar que se tenga un desempeño pobre.

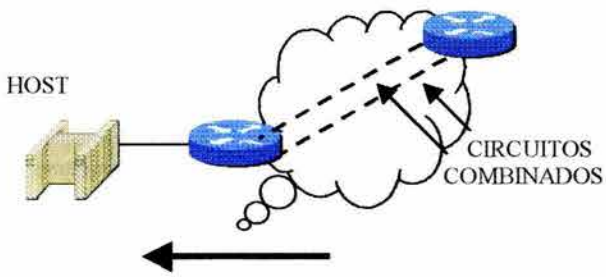
7.3.7 USO DE SVC

Arriba de 4,095 SVCs pueden ser configurados en una interfaz X.25.

La tasa de transferencia por encapsulación de un protocolo puede mejorar utilizando múltiples SVCs. Múltiples SVCs pueden proveer un tamaño de ventana de gran efectividad. El tamaño de ventana se refiere a la cantidad de datos que pueden ser transferidos en una cadena simple con la intervención de un reconocimiento de recibo[52].

Volver a secuenciar el tráfico es importante porque éste viaja por diferentes rutas y puede llegar en desorden. En la figura 7.19, tres SVC son combinados para proveer una tasa de transferencia grande a través de la nube X.25.

FIGURA 7.19

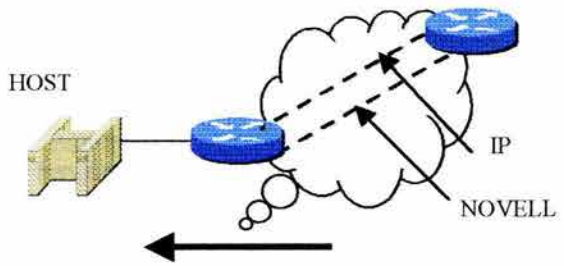


7.3.8 CIRCUITO VIRTUAL DE UN PROTOCOLO SIMPLE

El método de encapsulación tradicional habilita a diferentes protocolos para transportar sus datagramas a través de la nube X.25 porque el ruetador utiliza VC separados como en la figura 7.20

Cada protocolo es especificado en una declaración individual del comando *x.25 map* que hace referencia a la dirección X.121.

FIGURA 7.20

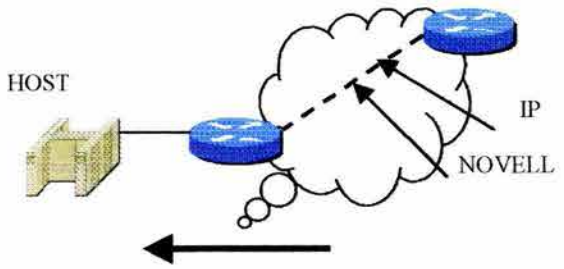


[52] Revisar la sección *Control de Flujo y Windowing, Capitulo 1.*

7.3.9 CIRCUITOS VIRTUALES MULTIPROTOCOLOS

Un circuito virtual simple a un host puede traer tráfico de múltiples protocolos, como lo muestra la figura 7.21. Una declaración del comando *x.25 map* contiene varias direcciones de protocolos mapeados en una dirección X.121 asociados con el host destino.

FIGURA 7.21



Cada uno de los protocolos soportados puede mapear a un destino de host. Como las cargas de tráfico son generadas por múltiples protocolos de ruteo sobre un VC, combinando con SVCs, como se describió anteriormente, puede mejorar la tasa de transferencia.

7.3.10 CONFIGURANDO X.25

Cuando se selecciona X.25 como protocolo WAN, se deben fijar parámetros de interfaz apropiados, incluyendo:

- Definir la encapsulación X.25 (DTE es por defecto).
- Asignar una dirección X.121 (usualmente provisto por el proveedor de servicios).
- Definir las declaraciones de mapeo para asociar las direcciones X.121 con las direcciones del protocolo de alto nivel.

Otras tareas de configuración pueden ser desempeñadas para controlar la tasa de transferencia y garantizar la compatibilidad con el proveedor de la red X.25.

X.25 es un protocolo de flujo controlado. Los parámetros de flujo controlado por defecto deben corresponder en ambos lados del enlace. La mala correspondencia causada por configuraciones inconsistentes puede resultar en severos problemas de red.

Ambos lados del enlace X.25 (DTE y DCE) deben estar de acuerdo en un número de parámetros, incluyendo encapsulación y mapeo de direcciones. Ellos también deben estar de acuerdo en los números de VC y su propósito.

Los estándares X.25 ordenan que el tamaño de la ventana por defecto de dos paquetes y un tamaño de paquete por defecto de 128 bytes deban estar disponibles. El tamaño de paquete más grande (por ejemplo, 512 o 1024) son comúnmente utilizados en Estados

Unidos y Europa. El tamaño del paquete arriba puede ser permitido por algunos proveedores de red.

Los siguientes comandos pueden ser utilizados para configurar parámetros de interfaz en un ruteador:

- *encapsulation x.25*
- *x.25 address*
- *x.25 map*

7.3.10.1 COMANDO *ENCAPSULATION X.25*

Se utiliza el comando *encapsulation x.25* para especificar el estilo de encapsulación – DTE o DCE- a ser usado en una interfaz serial. Un ejemplo de configuración es:

Router(config-if)#*encapsulation x.25*
Router(config-if)#*encapsulation x.25 dce*

El ruteador puede ser un DTE; típicamente, ésta es la configuración cuando el PDN es utilizado para transportar varios protocolos. El ruteador también puede ser configurado como un DCE el cual es típico cuando un ruteador actúa como un Switch X.25. DTE está por defecto.

7.3.10.2 COMANDO *X.25 ADDRESS*

El comando *x.25 address* define la dirección X.121 del ruteador local (una dirección por interfaz). El valor especificado debe corresponder con la dirección designada por el PDN. El formato de este comando es:

Router(config-if)#*x.25 address* direccion X.121

7.3.10.3 COMANDO *X.25 MAP*

El comando *x.25 map* provee una conversión de direcciones de alto nivel a direcciones X.25. El comando correlaciona las direcciones de capa de red a las direcciones X.121 de host a host. El formato del comando es:

Router(config-if)#*x25 map* protocolo direccion direccion X.121 [opciones]

donde los parámeros son los siguientes:

- protocolo: Selecciona el tipo de protocolo. Los protocolos soportados son IP, XNS, DECnet, IPX, Apple Talk, Vines, Apollo, Bridge clns.
- dirección: Especifica la dirección del protocolo.

- dirección X.121: Especifica la dirección de protocolo y la dirección X.121 juntos deben especificar la red completa de mapeo de protocolo a X.121.
- opciones (opcional): Modifica la conexión. Una opción comúnmente utilizada es *broadcast*. La opción *broadcast* causa que el Cisco IOS Software direccione algunos broadcast enviados a través de esta interfaz a la dirección X.121 específica.

La siguiente declaración *x25 map* es utilizada para comunicarse con un host que entiende múltiples protocolos con un VC simple. Esta comunicación requiere la encapsulación de protocolos múltiples definido por RFC 1356.

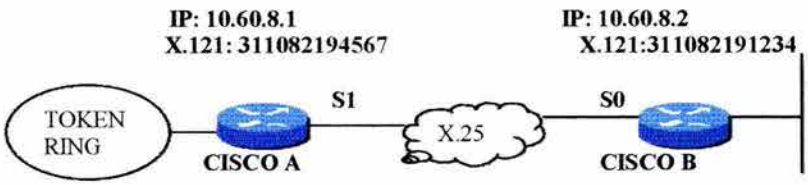
Router(config-if)#*x25 map* protocolo dirección [protocolo2 direccion 2]* direccion X.121 [opciones]

El signo * significa que un máximo de nueve direcciones de protocolos de red puede ser asociados con un host destino en un comando de configuración simple.

7.3.11 EJEMPLO DE CONFIGURACIÓN X.25

En la figura 7.23, dos ruteadores X.25 son configurados para conectar oficinas remotas.

FIGURA 7.23




```
interface serial 1
  encapsulation x25
  x25 address 311082194567
  ip address 10.60.8.1  255.255.248.0
  x25 map ip 10.60.8.2 311082191234 broadcast
```

```
interface serial 1
  encapsulation x25
  x25 address 311082191234
  ip address 10.60.8.2  255.255.248.0
  x25 map ip 10.60.8.2 31108219567 broadcast
```

Para el ruteador A en la figura 7.23, los detalles de la configuración son los siguientes:

- encapsulation x25: Fija la encapsulación en la interfaz serial 1 a X.25
- x25 address 311082194567: Establece la dirección X.121 de Serial 1.
- ip address 10.60.8.1 255.255.240.0: Especifica un protocolo de capa 3 y la dirección que se asocia con la dirección X.121 de la interfaz.
- x25 map ip 10.60.8.2 311082191234 broadcast: Mapea una dirección IP a una dirección X.121 para el host (serial 0) el cual está en el final de la conexión X.25. La opción *broadcast* direcciona la interfaz para enviar la información de ruteo a sus vecinos sobre X.25.

El ruteo IP en el ruteador A reenvía datagramas destinados para la subred 10.60.8.0 a la interfaz serial 1. El mapeo de interfaz identifica el destino a la nube X.25. Esta es una configuración típica, el ruteador A trata de establecer un SVC al ruteador B utilizando una dirección fuente X.121 y una dirección destino X.121 de 311082191234 cuando éste envía paquetes a la red 10.60.8.2.

Sobre el recibo de la solicitud, el ruteador B identifica la dirección IP remota de la dirección fuente X.121 y acepta la conexión. Después que el SVC es conectado, cada ruteador utiliza éste como un enlace punto a punto para su destino.

7.3.12 TAREAS ADICIONALES DE CONFIGURACION

Puede ser necesario llevar tareas de configuración adicionales para que el ruteador trabaje correctamente con el proveedor de servicios de red. Los parámetros cruciales son:

- Rango de Circuito Virtual: Comienza, autentifica y termina
- Tamaño de paquetes por defecto: Entrada y salida
- Tamaño y módulo de ventana

Esos parámetros deben de ser definidos pero no es necesario configurarlos directamente porque ellos dependen de los parámetros por defecto utilizados por el proveedor de servicios.

7.3.13 CONFIGURANDO RANGOS DE CIRCUITOS VIRTUALES X.25

Arriba de 4,095, los circuitos virtuales pueden ser configurados en una interfaz y cada punto de una conexión X.25 debe estar de acuerdo en el rango de circuitos disponibles que están siendo utilizados. La siguiente tabla resume los comandos de configuración para la asignación del número de circuito virtual. El rango completo de circuitos virtuales puede ser asignado a PVCs, SVCs o la combinacion de ambos dependiendo de los requerimientos, los SVCs son los más comúnmente utilizados.

TIPO DE CIRCUITO VIRTUAL	RANGO	POR DEFECTO	COMANDOS
PVCs	1-4095		x25 pvc circuit
SVCs:			
Entrate solamente	1-4095	0	x25 lic circuit
DCE iniciado	1-4095	0	x25 hic circuit
Dos caminos[52]	1-4095	1	x25 ltc circuit
		1024	x25 htc circuit
Saliente solamente	1-4095	0	x25 loc circuit
DTE iniciado	1-4095	0	x25 hoc circuit

Un número de límite alto y bajo debe ser configurado para definir el rango. Si ambos rangos del límite son ceros, el rango es inutilizable

Los números del circuito deben ser asignados de modo que un rango entrante venga antes de un rango de dos caminos, los cuales vienen antes de un rango saliente. Algunos PVCs deben tomar un número de circuitos que viene antes de algun rango SVC. El siguiente esquema de numeración lista el orden apropiado para esas asignaciones de números de circuitos virtuales:

1_PVC <(lic_hic)<(hc_ht)<(loc_hoc)_4095

Las siguientes decodificaciones pueden ser utilizadas para interpretar el esquema de numeración:

- *lic*- número de circuito entrante más bajo
-
- *hic*- número de circuito entrante mas alto
- *ltc*- número de circuitos de dos caminos más bajo
- *htc*- número de circuito de dos caminos más alto
- *loc*- número de circuito saliente más bajo
- *hoc*- número de circuito saliente más alto

El siguiente ejemplo fija los rangos de circuitos virtuales de 5 a 20 para llamadas entrantes solamente (de DTE y DCE) y 25 a 1024 para llamadas entrantes o salientes. También especifica circuitos no virtuales para llamadas salientes (de DTE a DCE).

x25 lic 5
x25 hic 20
x25 ltc 25

X.25 ignora algunos eventos en un número de circuito virtual no asignado en un rango de circuito virtual al circuito virtual fuera de rango como un error de protocolo. El administrador de red especifica los rangos de circuitos virtuales para la conexión X.25. Para una operación correcta, el DTE y el DCE deben tener rangos idénticos configurados.

7.3.14 CONFIGURANDO TAMAÑOS DE PAQUETES X.25

Los siguientes comandos son utilizados para configurar el tamaño de paquetes X.25:

- *x25 ips*
- *x25 ops*

Estos comandos fijan tamaños de paquetes de entrada y salida por defecto, respectivamente. Los valores de entrada y salida deben corresponder a menos que la red soporte transmisiones asimétricas. El formato de los comandos es:

Router(config-if)#*x25 ips* bytes
Router(config-if)#*x25 ops* bytes

donde **bytes** se refiere al tamaño del paquete máximo asumido por circuitos virtuales que no negocian un tamaño. Los valores soportados son: 16, 32, 64, 128, 256, 512, 1024, 2048 y 4096. El valor por defecto es 128 bytes.

Si las estaciones de una conexión X.25 llegan a tener un conflicto en el número máximo de paquetes de circuitos virtuales, el circuito virtual deja de funcionar.

Los paquetes son enviados a través de la red X.25 que excede el tamaño del paquete especificado requiere que el ruteador fragmente el paquete en paquetes más pequeños. El reensamblaje de paquetes ocurre cuando el ruteador los recibe, este proceso consume ciclos de CPU en ambor ruteadores.

7.3.15 CONFIGURANDO LOS PARAMETROS DE VENTANA X.25

X.25 utiliza ventanas deslizantes para el control de flujo. Una ventana grande permite que más paquetes sean transmitidos.

Los siguientes comandos son utilizados para configurar el tamaño de ventana deslizante:

- *x25 win*
- *x25 wout*
- *x.25 modulo*

Se utilizan los comandos *x25 win* y *x25wout* para fijar los tamaños de ventanas entrantes y salientes por defecto. El tamaño de ventana especifica el número de paquetes que son recibidos/enviados a enviar/recibir un reconocimiento. Ambos puntos del enlace X.25 debe utilizar el mismo tamaño de ventana por defecto. El formato de estos comandos es:

Router(config-if)#*x25 win* paquetes
Router(config-if)#*x25wout* paquetes

donde el parámetro **paquetes** especifica el tamaño de ventana del paquete. Los posibles valores para el rango de tamaño de ventana de una a una menos que el módulo.

El comando *x25 modulo* especifica el modulo de enumeración de paquetes. Esto afecta al número máximo de tamaño de ventana. Por ejemplo, el *modulo 8* es ampliamente utilizado y permite tamaños de ventana de circuito virtual arriba de 8 (utilizando una secuencia de 0 a 7) paquetes. El modulo *128* es raro pero permite tamaños de ventana de circuito virtual arriba de 128 (utilizando una secuencia de 0 a 127) paquetes.

El formato del comando es:

Router(config-if)#*x25 modulo* modulus

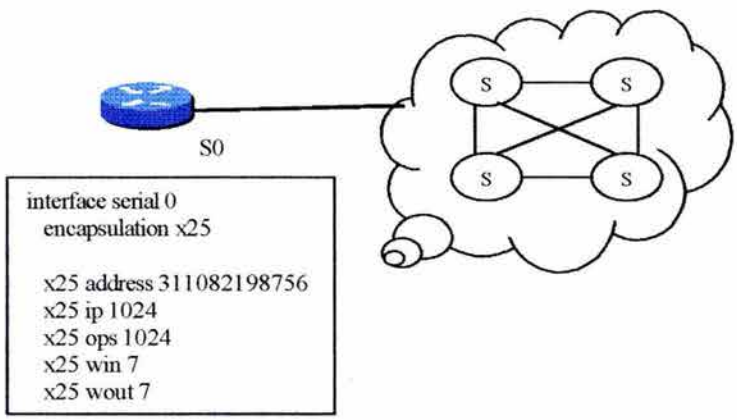
donde el parámetro **modulus** puede ser 8 o 128

Ambos puntos del enlace deben utilizar el mismo módulo.

7.3.16 EJEMPLO DE CONFIGURACION ADICIONAL X.25

La figura 7.24 muestra una configuración de la interfaz Serial 0. El tamaño del paquete no puede ser soportado por todos los PDNs.

FIGURA 7.24



Una dirección X.121 es asignada a la interfaz Serial 0. El paquete de entrada y salida, tamaños de ventana y el número máximo de circuitos virtuales por algún protocolo son también definidos.

En la figura 7.24 los siguientes comandos han sido especificados:

- *x25 address 31108218756*: Especifica la dirección de la interfaz.
- *X25 ips/ops 1024*: Fija el tamaño del paquete de entrada y salida a 1024 para corresponder los valores definidos para la conexión de red.
- *X25 win/wont 7*: Fija el tamaño de paquete de entrada y salida a 7 para corresponder los valores definidos por la conexión de la red.

7.3.17 CONFIGURANDO UN RUTEADOR COMO UN SWITCH

El ruteador puede ser configurado para tráfico switcheado X.25 sobre una conexión TCP como lo muestra la figura 7.25, X.25 sobre TCP es llamado XTO.

FIGURA 7.24

El comando para configurar un PVC XOT es:

Router(config-if)# *x.25 pvc* numero1 *tunnel* direccion *interface serial* entero *pvc* numero2 [opciones]

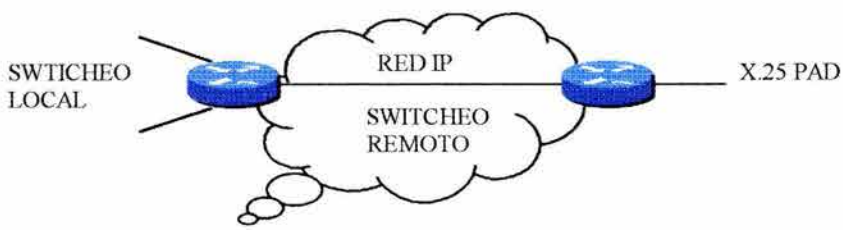
Las opciones del comando son **packet size** *in out* y **window size** *in out*; ellos permiten valores de control de flujo de PVC a ser definidos si ellos difieren de los valores por defecto de las interfaces.

En este modo, la columna vertebral de la red abarca ruteadores de switcheado de paquetes. Pocos dispositivos X.25 se conectan con otros dispositivos a través de la columna vertebral de la red.

7.3.18 X.25 LOCAL Y SWITCHEO XOT

El tráfico X.25 puede ser ruteado localmente entre puertos seriales. En este caso, las declaraciones de ruteo estático mapean direcciones X.121 a puertos seriales. El ruteador permite interfaces X.25 conectadas a diferentes puertos para hacer conexiones SVC, una capacidad la que es llamada *Switcheo X.25 Local* (mostrado en la figura 7.26). Un ruteador configurado como un switch XOT provee de una mejora significante en la tasa de transferencia sobre el equipo de switcheo X.25 tradicional.

FIGURA 7.26



El switcheo X.25 remoto permite interfaces X.25 conectadas a diferentes ruteadores para establecer SVC y PVC. El switcheo X.25 remoto es llevado a cabo por un tuneleo de los establecimientos de llamadas X.25 y el tráfico de datos entre los ruteadores en una conexión TCP.

El formato del comando es:

Router(config-if)#*x25 route* [#position] direccion x.121 [patron *cud*] *interface* tipo número

donde los parámetros especifican lo siguiente:

- *#position (opcional)*: Un valor posicional que especifica el número de línea en la tabla donde la entrada tomo lugar.
- *direccion x.121*: Patrón de dirección destino X.121.
- *patron CUD (opcional)*: Patrón Call User Data (CUD) el cual es un entero ASCII imprimible
- *tipo numero*: El número de la interfaz destino tal como *Serial 0*.

7.3.19 MONITOREANDO X.25

Se utiliza el comando *show interfaces* para desplegar el estado y la información del contador acerca de una interfaz. En la figura 7.27, la interfaz Serial tiene su tipo de encapsulación configurada para X.25.

FIGURA 7.27

```
Router#show interfaces

Serial0 is up, line protocol is up
   Hardware is MK5025
   Internet address is 183.8.128.129, subnet mask is 255.255.255.128
   MYU 1500 bytes, BW 56Kbit, DLY 20000 usec, rely 255/255, load 1/255
   Encapsulation X25, loopback not set
   LAPB DCE, state CONNECT, modulo 8, k 7, N1  12048 N2  20
         T1 3000, interface outage (partial T3) 0, T4 0
         VS 1, VR 1 Remote VR 1, Retransmissions 0
         IFrames 1728559/1639143 RNRs 0/0 REJs 0/0 SAMB/Es 3/2 FRMRs 0/0 DISCs 0/0
X25 DCE, address 311012345678, state RI, modulo 8, Timer 0
         Defualts: cisco encapsulation, idle 0, nvc 1
            input/output window sizes 2/2, packet sizes 128/128
         Timers: T10 60, T11 180, T12 60, T13 60, TH 0
         Channels: Incoming-only none, two way 1-1024, Outgoing-only none
         RESTARTs 3/3 CALLs 244+235/266+262/0+0 DIAGs 0/0
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interfaces" counters never
Output queue 0/40, 0 drops; input queue 2/75, 0 drops
Five minute input rate 0 bits/sec, 3 packets/sec
Five minute output rate 0 bits/sec, 3 packets/sec
      3370943 packets input, 1133 76062 bytes, 0 no buffer
       Received 1971 broascast, 0 runts, 0 giant
       57 input errors, 57 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
--more--
```

Los comandos *show* adicionales incluyen los comandos *show x25 map* y *showx25vc*.

7.4 CONFIGURANDO FRAME RELAY

Esta sección describe la operación de Frame Relay y cubre configuración para interfaces y subinterfaces físicas

7.4.1 DESCRIPCION DE FRAME RELAY

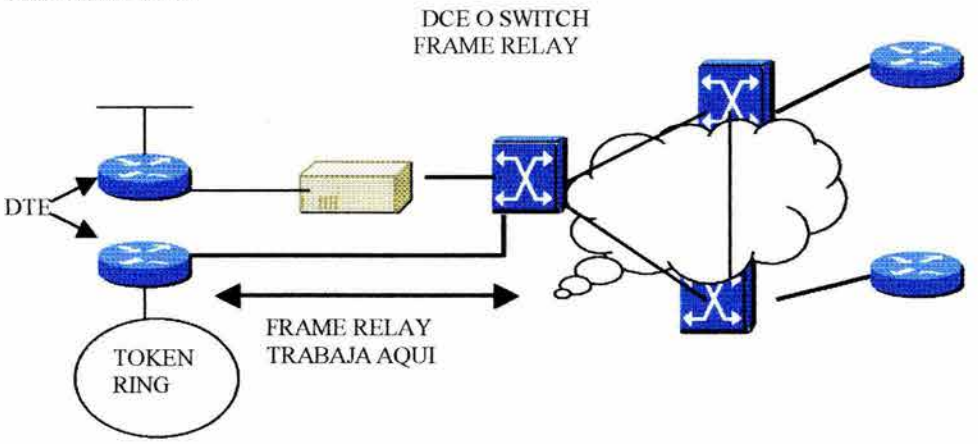
Frame Relay es un estándar de CCITT y American National Standars Institute (ANSI) que define el proceso de envío de datos sobre una red de datos pública. Este es un protocolo de nueva generación y es un protocolo de capa 2 que provee un alto desempeño y eficiencia. Confía en las capas superiores para corrección de errores y control de flujo.

Como muestra la figura 7.28 Frame Relay define el proceso de interconexión entre CPE (también conocido como DTE), tal como un ruteador y el equipo de acceso de switcheo local del proveedor de servicios (también llamado DCE).

Esto no define la manera en que los datos son transmitidos en la nube del proveedor de servicios de Frame Relay.

Frame Relay provee de medios para multiplexar varias conversaciones lógicas de datos (referidos como Circuitos Virtuales) sobre un enlace de transmisión física simple por asignación a cada par de DTEs. El equipo de switcheo del proveedor de servicios constituye de una tabla de mapeo de identificadores de conexión en puertos de salida. Cuando un frame es recibido, el dispositivo de switcheo analiza el identificador de conexión y entrega del frame al puerto de salida asociado. La ruta completa al destino es establecida antes del envío de primer frame.

FIGURA 7.28



Con ANSI T1.617 y ITU Q.933 (capa 3) y Q.922 (capa 2), Frame Relay ahora soporta SVCs. Se necesita determinar si el carrier[52] soporta SVCs antes de implementarlos.

7.4.2 TERMINOLOGIA FRAME RELAY

La terminología asociada con Frame Relay puede ser relativamente nueva. Hay que tener presente que los términos utilizados por el proveedor de servicios Frame Relay, incluyendo un glosario Frame Relay, hacen referencia al Foro Frame Relay en Internet en *www.frforum.com/4000/4000index.html*. La figura 7.29 identifica los términos que son utilizados más frecuentemente cuando se habla de Frame Relay

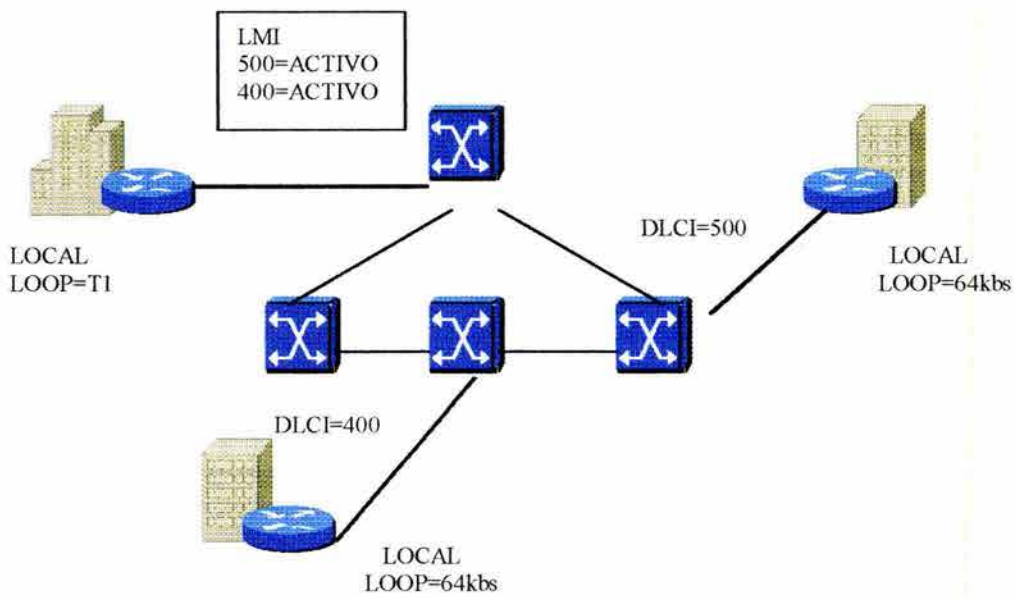
7.4.2.1 RANGO DE ACCESO LOCAL

La velocidad del reloj (velocidad de puerto) de la conexión (local loop) a la nube Frame Relay es el rango de acceso local. Este es el rango en el cual los datos viajan fuera de la red.

7.4.2.2 DATA-LINK CONNECTION IDENTIFIER (DLCI)

El DLCI es un número que identifica el circuito lógico entre el CPE y el switch Frame Relay (FR). El switch FR mapea el DLCI entre cada par de ruteadores para crear un PVC. Los DLCIs son una significancia local en que el identificador hace referencia en el punto entre el ruteador local y el switch FR al cual está conectado.

FIGURA 7.29



7.4.2.3 LOCAL MANAGEMENT INTERFACE (LMI)

El LMI es un estándar de señalización entre el dispositivo CPE y el switch FR que es el responsable para el manejo de la conexión entre dispositivos. LMI incluyen soporte para:

- Un mecanismo de keepalive, el cual verifica que el dato esté correcto.
- Un mecanismo multicast, el cual provee un servidor de red con DLCI local.
- Un direccionamiento multicast el cual da DLCI locales más que una significancia local de red Frame Relay.

Aunque el LMI es configurable, el ruteador trata de autosensar o reconocer el tipo de LMI que el switch FR utiliza para enviar una o más solicitudes del estado del switch FR. El switch FR responderá por si mismo con el último tipo de LMI recibido. Tres tipos de LMI son soportados:

- *cisco*: Tipo de LMI definido en común por Cisco, StrataCom, Northern Telecom, y DEC.
- *ANSI*: Anexo D definido por ANSI T.617.
- *q933a*: ITU-T Q.933 Anexo A.

7.4.2.4 COMMITTED INFORMATION RATE (CIR)

El CIR es el rango en bits por segundo que el switch FR fija y es utilizado para transferir datos. El rango es usualmente promediado sobre un periodo de tiempo referido como el *Committed Rate Measurement Interval (Tc)*. (El término MIR para Measurement Interval es utilizado en lugar de CIR por al menos un vendedor de Frame Relay).

7.4.2.5 SOBRESATURACION

Cuando la suma de los CIR en todos los circuitos virtuales que llegan a un dispositivo excede la velocidad de la línea de acceso, la conexión Frame Relay se dice que está sobresaturada. Esto puede ocurrir cuando la línea de acceso puede soportar la suma del CIR que rompen con las capacidades del circuito virtual. Si la sobresaturación ocurre, los paquetes son perdídos.

7.4.2.6 COMMITTED BURST (Bc)

El Committed Burst es el número máximo de bits que la red Frame Relay fija para la transferencia durante el *Committed Rate Measurement Interval (Tc)*.

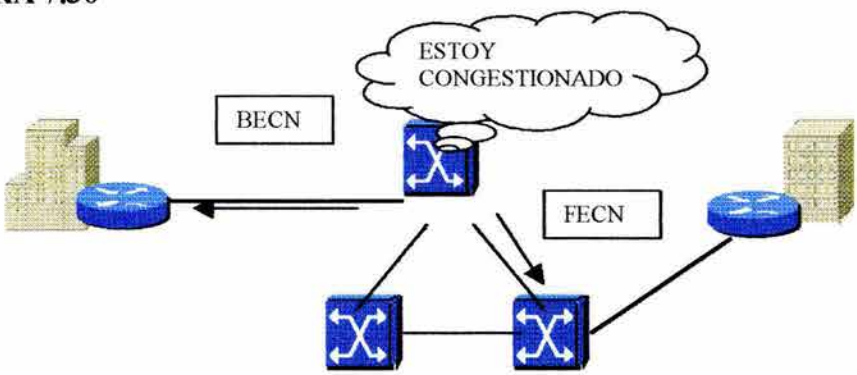
7.4.2.7 EXCESS BURST

El Excess Burst es el número máximo de bits que el switch FR intentará fijar para transmitir más allá del CIR

7.4.2.8 FORWARD EXPLICIT CONGESTION NOTIFICATION (FECN)

Cuando el switch FR reconoce congestión en la red, éste fija el bit FECN en el límite del paquete de Frame Relay para el dispositivo destino, como lo muestra la figura 7.30

FIGURA 7.30



7.4.2.9 BACKWARD EXPLICIT CONGESTION NOTIFICATION (BECN)

Cuando el switch FR reconoce congestión en la red, éste fija el bit BECN en el ruteador fuente diciéndole a éste que reduzca el rango en el cual se envían los paquetes.

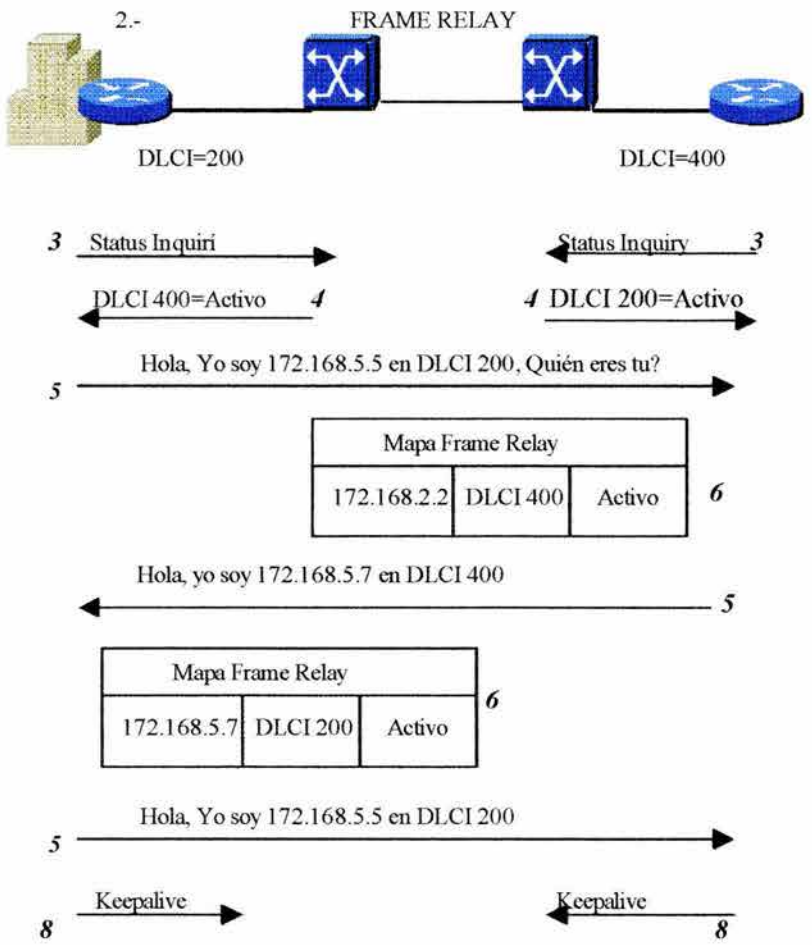
7.4.2.10 DISCARD ELIGIBILITY (DE) INDICATOR

Cuando el ruteador detecta congestión en la red, éste fija el bit DE en el tráfico sobresaturado. Si la red experimenta congestión, primero descarta esos paquetes con el bit DE fijo.

7.4.3 OPERACIÓN DE FRAME RELAY

Frame Relay es un protocolo de capa 2 que describe la manera en que el dispositivo DTE se comunica con el switch FR. La figura 7.31 ilustra la manera en que la operación de Frame Relay trabaja.

FIGURA 7.31



Los siguientes pasos muestran la manera en la cual el protocolo Frame Relay opera:

1.- Se ordena el servicio de Frame Relay a un proveedor de servicios.
2.- Cada ruteador, conectado directamente o a través de un CSU/DSU, se conecta a un switch FR y un DLCI es asignado.
3.- Cuando el ruteador CPE es habilitado, manda un mensaje de *Status Inquiri* al switch FR. El mensaje notifica el estado del ruteador y pregunta al switch FR por el estado de la conexión de otros ruteadores remotos.
4.-Cuando el switch FR recibe la solicitud, éste responde con un mensaje de estado que incluye el DLCI de los ruteadores remotos a los cuales el ruteador local puede enviar datos.
5.- Para cada DLCI activo que un ruteador puede alcanzar, el ruteador envía un paquete de solicitud de Inverse ARP introduciéndose él mismo y preguntando a cada ruteador remoto para identificarse con respuesta.
6.- Para cada DLCI para el cual el ruteador recibe un mensaje Inverse ARP, el ruteador creará una entrada de mapa en su tabla de Frame Relay que incluye su propio DLCI y las direcciones de capa de red de los ruteadores remotos, así como el estado de la conexión. Hay que notar que el DLCI es el que está configurado localmente en el ruteador y no el

DLCI que los ruteadores remotos utilizan. Tres posibles estados de conexión aparecen en la tabla Frame Relay:

- Estado activo: Indica que la conexión está activa y que los ruteadores pueden intercambiar datos.
- Estado inactivo: Indica que la conexión local al switch FR está trabajando pero la conexión de los ruteadores remotos al switch FR no está trabajando.
- Estado suprimido: Indica que el LMI no esta siendo recibido del switch FR o no hay servicio entre el ruteador CPE y el switch FR.

Sin Inverse ARP no está trabajando o los ruteadores remotos no soportan éste, se nesecita configurar las rutas de los ruteadores remotos.
7.- Cada 60 segundos los ruteadores intercambian mensajes Inverse ARP.
8.-Cada 60 segundos (esto es configurable) el CPE envía un mensaje Keepalive al switch FR. El propósito de éste mensaje es verificar que el switch FR esté aún activo.

7.4.4 CONFIGURANDO FRAME RELAY

Una configuración básica de Frame Relay asume que se quiere configurar Frame Relay en una o más interfaces fisicas y que el LMI y el Inverse ARP son soportados por los ruteadores remotos. En este tipo de ambiente, el LMI notifica al ruteador acerca de los DLCI disponibles. La figura 7.32 ilustra configuraciones para esta situación.

Se utilizan los siguientes pasos para una configuración básica Frame Relay en los ruteadores:

1.- Seleccionar la interfaz y entrar en el modo de configuración global.
2.- Configurar una dirección de red, por ejemplo una dirección IP.
3.- Seleccionar el tipo de encapsulación utilizado para encapsular el tráfico de datos. El formato del comando de encapsulación es el siguiente:

Router(config-if)#*encapsulation frame-relay [cisco|ietf]*

donde *cisco* es por defecto. Se utiliza *cisco* si se conecta a otro ruteador Cisco; se utiliza *ietf* si se conecta a un rutador que no sea Cisco.
4.- Si se utiliza el Cisco IOS Release 11.1 o superiores, se especifica el tipo de LMI utilizado en el switch FR:

Router(config-if)#*frame-relay lmi-type [ansil|cisco|q9433]*

donde *cisco* es por defecto.
5.- Configurar el ancho de banda del enlace el Kilobits por segundo.

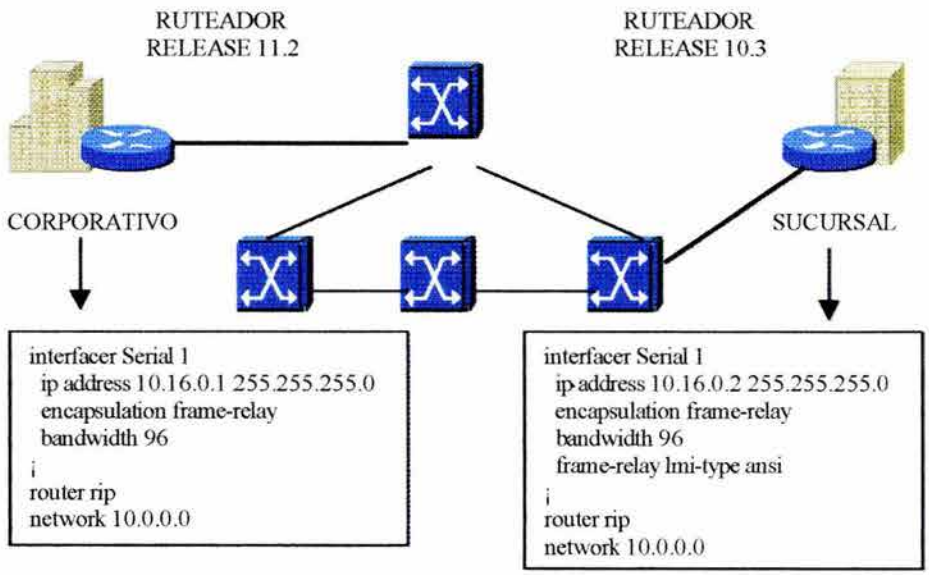
Router(config-if)#*bandwidth* kilobits

Este comando afecta la operación de ruteo para protocolos tales como IGRP y EIGRP porque éstos son utilizados para definir la métrica del enlace. Sin este comando, EIGRP asume que el ancho de benda es 1.544 Mbps (T1). Este comando también es la base para estadísticas tal como la utilización del ancho de banda.
6.- Si Inverse ARP está deshabilitada, se habilita. Inverse ARP está habilitada por defecto. El formato de este comando es:

Router(config-if)#*frame-relay inverse arp [protocolo] [dlci]*

Los protocolos soportados incluyen IP, IPX, Apple Talk, DECnet, Vynes y XNS. El parámetro *dlci* identifica el DLCI en la interfaz local con la cual se quiere intercambiar mensajes Inverse ARP

FIGURA 7.32



7.4.5 COMANDO DE CONFIGURACION OPCIONAL

Normalmente Inverse ARP es usado para solicitar la dirección de protocolo del próximo salto para una conexión específica. Las respuestas a Inverse ARP son incorporadas en una tabla de dirección-DLCI. Esta tabla es entonces usada para ruteo de tráfico de salida. Cuando Inverse ARP no es soportado por el ruteador remoto, cuando se configura OSPF sobre Frame Relay o cuando se quiere controlar el tráfico broadcast cuando se utiliza ruteo, se debe definir la tabla dirección-DLCI estáticamente. Esas entradas estáticas se refieren a mapeos estáticos los cuales son implementados con el comando *frame-relay map*. La forma de este comando es:

Router(config-if)#*frame relay map protocolo direccion protocolo dlci [broadcast] [ietf|cisco|[payload-compress packet-by-packet]*

donde los parámetros y palabras clave tienen los siguientes significados:

- *protocolo*: Define los protocolos soportados o control de enlace logico.
- *dirección de protocolo*: Define la dirección de capa de red de la interfaz destino del ruteador.
- *dlci*: Define el DLCI local utilizado para conectar a la dirección del protocolo remoto.
- *broadcast(opcional)*: Reenvía un broadcast a esta dirección cuando el multicast no es habilitado. Esto se utiliza si se quiere que el ruteador mande actualizaciones de ruteo. Si no se habilita se deben definir rutas estáticas.
- *ietf|cisco (opcional)*: Se selecciona el tipo de encapsulación a utilizar.
- *payload-compress packet-by-packet*: Utilizando STAC, un método de compresión propietario de Cisco.

Otros comandos opcionales pueden ser utilizados con Frame Relay para tratar con tablas de ruteo y keepalives.

Por ejemplo, si se utiliza EIGRP se puede fijar el porcentaje de ancho de banda configurado a utilizar por el tráfico de ruteo EIGRP. El porcentaje por defecto es 50%. Notar que la sintaxis para los comandos varía, dependiendo de si se configura por EIGRP para IP, IPX o Apple Talk. La sintaxis IP es como sigue:

Router (config-if)#*ip bandwidth-percent eigrp as-number porciento*

donde *as-number* es un numero de sistema autónomo y *porciento* es el porcentaje de ancho de banda EIGRP que se puede utilizar. Recordar que el total de ancho de banda es derivado de lo que fue configurado utilizando el comando *bandwidth* o el defecto que es 1.544 Mbps.

Se puede extender o reducir el intervalo en el cual la interfaz del ruteador envía Keepalives al switch FR. El tiempo por defecto es 10 segundos. La forma del comando es:

Router(config-if)#*keepalive numero*

donde *numero* es el intervalo en segundos.

Si un LMI no es utilizado en la red o se hace una prueba back-to-back entre ruteadores, se necesita especificar el DLCI para cada interfaz local utilizando el siguiente comando:

Router(config-if)# *frame-relay local-dlci numero*

donde *número* es el DLCI dela interfaz a ser utilizado.

7.4.6 VERIFICANDO LA OPERACIÓN FRAME RELAY

Después de configurar Frame Relay se puede verificar que la conexión esté activa utilizando los siguientes comandos *show*:

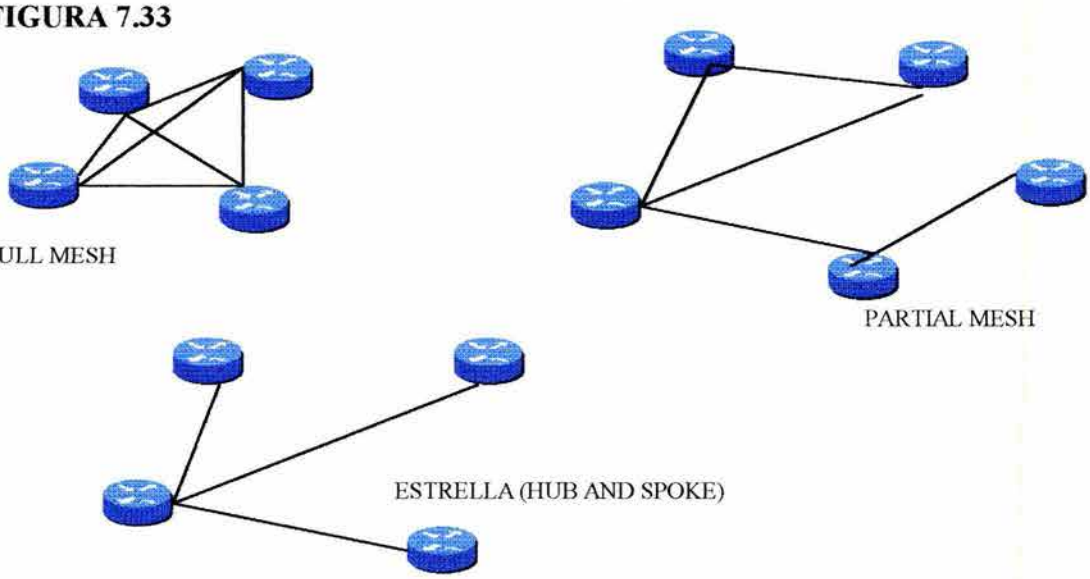
- *show interfaces serial:* Despliega información acerca de DLCI multicast, el DLCI utilizado en Frame Relay configurado en interfaz serial y el LMI DLCI utilizado para la interfaz local de administración.
- *show frame-relay pvc:* Despliega información de cada conexión configurada así como estadísticas de tráfico. Este comando también es útil para una vista del número de paquetes BECN y FECN recibidos por el ruteador.
- *show frame-relay map:* Despliega direcciones de capa de red y los DLCI asociados para cada destino remoto.
- *show frame-relay lmi:* Despliega estadísticas de tráfico LMI. Por ejemplo, esto muestra el número de mensajes de estado intercambiados entre el ruteador local y el switch FR.

7.4.7 SELECCIONANDO UNA TOPOLOGIA DE FRAME RELAY

Frame Relay permite conectar sitios remotos en una variedad de caminos como lo muestra la figura 7.33. Ejemplos de topologías son:

- Topología de estrella
- Topología Full-mesh
- Topología Partial-mesh

FIGURA 7.33



7.4.7.1 TOPOLOGIA DE ESTRELLA

Una topología de estrella, también conocida como *configuración Hub and Spoke*, es la topología de red Frame Relay más popular. En esta topología los sitios remotos se conectan a un sitio central que generalmente provee de un servicio o aplicación. Esta es la topología menos cara porque requiere menos PVCs que las otras topologías. En este escenario, el ruteador central provee una conexión multipunto porque se utiliza una interfaz simple para interconectar múltiples PVCs.

7.4.7.2 TOPOLOGIA FULL-MESH

En la topología Full-Mesh todos los ruteadores tienen circuitos virtuales a todos los destinos. Este método es costoso y provee conexiones directas desde cada sitio a todos los otros sitios y permite redundancia. Por ejemplo, dados tres ruteadores, A, B y C. Si el enlace entre los ruteadores A y B está caido, el ruteador A todavía puede alcanzar el ruteador B por medio del ruteador C.

7.4.7.3 TOPOLOGIA PARTIAL-MESH

En la topología Partial-Mesh no todos los sitios tienen acceso directo con el sitio central. Dependiedo de los patrones de tráfico en la red se necesitará tener PVCs adicionales conectados a sitios remotos que tienen requerimientos de un alto tráfico de datos.

7.5 ACCESIBILIDAD Y RECURSOS DISTRIBUIDOS PARA FRAME RELAY

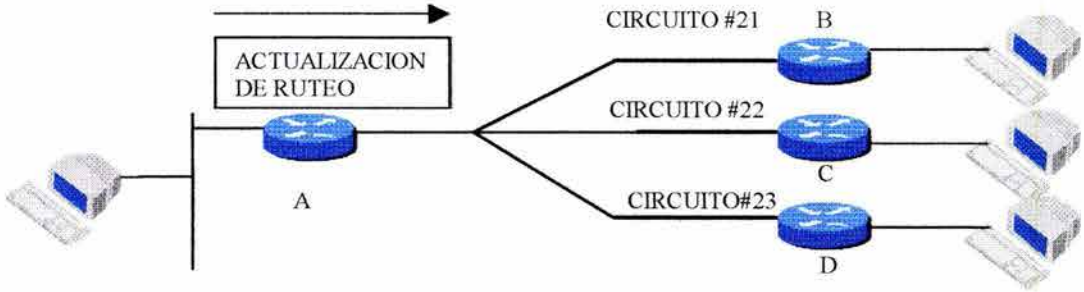
En algunas de la posibles topologías, cuando una interfaz simple debe ser utilizada para interconectar múltiples sitios, se debe hacer frente a los retos de accesibilidad debido a la naturaleza de *Nonbroadcast Multiaccess (NBMA)* de Frame Relay.

Por defecto, una red Frame Relay provee conectividad NBMA entre sitios remotos. Depediendo en la topología, los broadcasts de actualizaciones de ruteo recibidos por un ruteador no pueden ser reenviados a todas las localizaciones.

Vamos a considerar el diseño Frame Relay de la figura 7.34. *Split Horizon*[53] reduce los loops de ruteo por no permitir una actualizacion de ruteo recibida en una interfaz física para ser reenviada a través de la misma interfaz física. Como resultado, si el ruteador B en la figura 7.34, envía una actualización al ruteador A el cual conecta PVCs múltiples sobre una interfaz física simple, el ruteador no puede reenviar ese broadcast a través de la misma interfaz a los otros ruteadores remoto C y D.

Para superar este problema de accesibilidad, el ruteador debe repetir el broadcast para cada conexión activa, que es la distribución del tráfico de broadcast que puede llevarse a cabo sólo por el envío del mismo mensaje a cada conexión virtual. Este método requiere de una asignación de recursos considerables en el ruteador.

FIGURA 7.34



Los broadcast no son un problema si hay un solo PVC en una interfaz física como en un tipo de configuración punto a punto.

La cantidad de tráfico de broadcast y el número de circuitos virtuales a cada ruteador deben ser evaluados durante la fase de diseño de una red Frame Relay. La sobrecarga de tráfico, tales como actualizaciones de ruteo, puede afectar la entrega de datos críticos, especialmente cuando la ruta de entrega contiene enlaces de bajo ancho de banda (56Kbps).

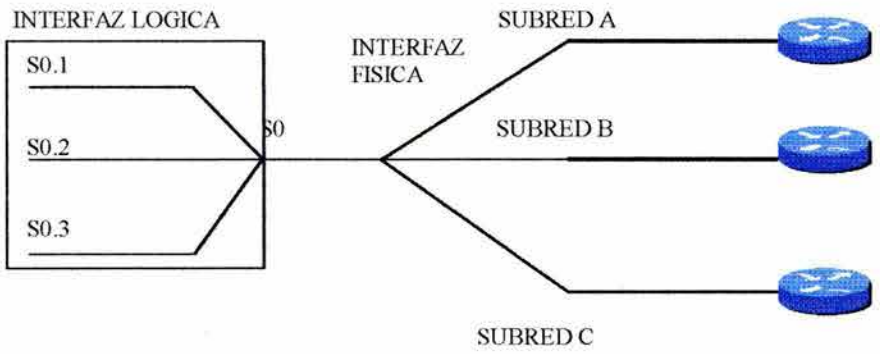
7.6 RESOLVIEDO LA ACCESIBILIDAD Y RECURSOS DISTRIBUIDOS: SUBINTERFACES

La respuesta simple para resolver los puntos de accesibilidad parece que es deshabilitar el Split Horizon. Dos problemas existen con esta solución. Primero, sólo IP permite deshabilitar Split Horizon; IPX y Apple Talk no. (Cuando una interfaz es configurada con *encapsulation frame-relay*, Split Horizon está deshabilitado para IP y habilitado para IPX y Apple Talk por defecto).

El segundo problema es que deshabilitar Split Horizon incrementa las posibilidades de que haya loops de ruteo.

Para habilitar el reenvío de broadcast de actualizaciones de ruteo, se puede configurar el ruteador con interfaces asignadas lógicamente llamadas *subinterfaces*. Las subinterfaces son subdivisiones lógicas de una interfaz física, como lo muestra la figura 7.35. En ambientes de ruteo de Split Horizon, las actualizaciones de ruteo recibidos en una subinterfaz pueden ser renviadas a otra subinterfaz. En la configuración de una subinterfaz cada circuito virtual puede ser conectado como una conexión punto a punto el cual permite que la subinterfaz actúe como una línea dedicada.

FIGURA 7.35



Se pueden configurar subinterfaces para soportar los siguientes tipos de conexiones:

- Punto a punto: Una simple subinterfaz es utilizada para establecer una conexión PVC a otra interfaz fisica o subinterfaz. en un ruteador remoto. En este caso, las interfaces están en la misma subred y cada interfaz tendria un DLCI. Cada conexión punto a punto está en su propia subred. En este ambiente los broadcast no son un problema porque los ruteadores son un punto a punto y actúan como una linea dedicada.
- Multipunto: Una subinterfaz simple es utilizada para establecer múltiples conexiones PVC para múltples interfaces fisicas o subinterfaces en ruteadores remotos. En este caso, todas las interfaces participantes estarán en la misma red y cada interfaz tendrá su DLCI local. En este ambiente, como la subinterfaz actúa como un NBMA de red Frame Relay, el tráfico broadcast está conforme a la regla Split Horizon.

7.7 CONFIGURANDO SUBINTERFACES

Para configurar subinterfaces en interfaces fisicas utilizar los siguientes pasos:

1.- Seleccionar la interfaz en la cual se quiere crear subinterfaces y entrar en el modo de configuración de interfaz.
2.- Remover alguna dirección de red asignada a la interfaz fisica. Si la interfaz fisica tiene una dirección, los frames no serán recibidos por subinterfaces locales.
3.- Configurar la encapsulación Frame Relay.
4.- Seleccionar la interfaz que se quiere configurar. El formato de este comando es:

```
Router(comfig-if)#interface serial numero.numero subinterfaz [multipunto|punto a
punto]
```

donde los parámetros y palabras clave son los siguientes:

- *.número subinterfaz*: Número de la subinterfaz en el rango de 1 a 4294967293. El número de interfaz que precede del (.) debe corresponder con el número de interfaz el cual ésta subinterfaz pertenece.
- *multipunto*: Se selecciona esta opción si se quiere que el ruteador reenvíe broadcast y actualizaciones de ruteo que son recibidos. También se selecciona si que quiere ruteo IP y si se quiere que todos los ruteadores estén en la misma subred.
- *punto a punto*: Se selecciona esta opción si no se quiere que el ruteador reenvíe broadcast o tablas de ruteo y si se quiere que cada uno de los ruteadores punto a punto tengan sus misma subred.

Se debe especificar Punto a Punto o Multipunto porque no hay uno por defecto.
5.- Configurar una dirección de red en la subinterfaz. Si la subinterfaz es punto a punto y se está utilizando IP se puede utilizar el comando *ip unnumbered*[54]:

Router(config-if)#*ip unnumbered interfaz*

Si se utiliza este comando, es recommendable que la interfaz numerada sea la interfaz loopback[55]. El enlace Frame Relay no trabajará si este comando está apuntando a otra interfaz que no está en completa operación y la interfaz loopback es menos probable que falle. La interfaz loopback es una dirección que representa el dispositivo mismo.
6.- Si se configura la subinterfaz como punto a punto o como multipunto con Inverse ARP habilitado, se debe configurar el DLCI local para la subinterfaz a distinguir de la interfaz física. Se utiliza el siguiente comando:

Router(config-if)#*frame-relay interface-dlci número de DLCI*

donde *número de DLCI* define el numero DLCI local enlazada a la subinterfaz. Este es sólo el camino para enlazar un LMI derivado de PVC a una subinterfaz porque el LMI no conoce acerca de subinterfaces.

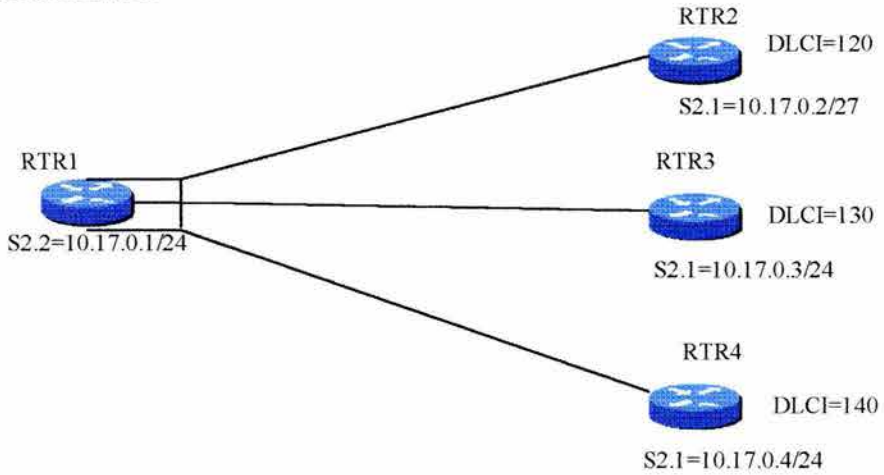
Este comando no es requerido para subinterfaces multipunto configurado con mapeos de rutas estáticas. No utilizar este comando en interfaces físicas.

7.8 EJEMPLO DE CONFIGURACIÓN DE SUBINTERFACES MULTIPUNTO

Considerar la red mostrada en la figura 7.36.

La configuración de salida en la figura 7.37 muestra la manera en que se configuran las subinterfaces multipunto.

FIGURA 7.36



Específicamente las subinterfaces de la figura 7.36 han estado configuradas en la interfaz S2.2 del ruteador del sitio central. Con este tipo de configuraciones, la subinterfaz toma las mismas características Frame Relay de una interfaz física, es decir, cada subinterfaz es un NBMA y es sujeto a la operación de Spli Horizon. La ventaja, sin embargo, es que se necesita una sola dirección de red.

FIGURA 7.37

```
<Output Omitted>
!
interface Serial2
   no ip address
!
interface Serial2.2 multipoint
   ip address 10.17.0.1 255.255.255.0
   bandwidth 64
   frame-relay map ip 10.17.0.2.120 broadcast
   frame-relay map ip 10.17.0.2.130 broadcast
   frame-relay map ip 10.17.0.2.140 broadcast
!
router rip
network rip
   network 10.0.0.0
<Output Omitted>
```

7.9 EJEMPLO DE CONFIGURACION DE SUBINTERFACES PUNTO A PUNTO

Considerar la configuración de subinterfaces punto a punto mostrada en la figura 7.38. La figura 7.40 muestra la configuración para esta red Frame Relay.

FIGURA 7.38

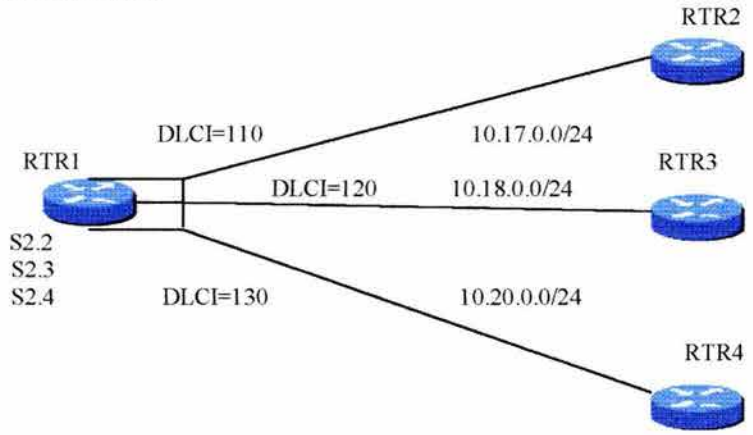
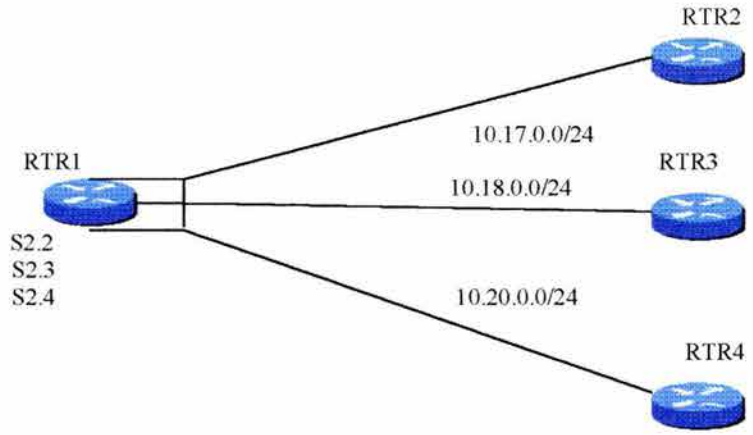


FIGURA 7.39



La figura 7.40 muestra la configuración para el ruteador 2 de la figura 7.38

FIGURA 7.40

```
<Output Omitted>
!
interface Serial2
   no ip address
!
interface Serial2.1 point-to-point
   ip address 10.17.0.2 255.255.255.0
   bandwidth 64
   frame-relay interface-dlci 110
!
router rip
network rip
   network 10.0.0.0
<Output Omitted>
```

```
p1r2#show frame-relay map
Serial2.1 (up): point-to point dlci, dlci
110 (0x64, 0x1840), broadcast status defined, active

p1r2#show ip route
<Output Omitted>

      10.0.0.0/24 is subnetted, 3 subnet
R       10.18.0.0[120/1] via 10.17.0.1, 00:00:04, Serial2.1
C         10.17.0.0 is directly connected, Serial2.1
R       10.20.0.0[120/1] via 10.17.0.1, 00:00:04, Serial2.1
```

La figura 7.42 muestra la manera de configurar subinterfaces punto a punto utilizando el comando *ip unnumbered*.

Cuando se utiliza el comando *ip unnumbered* recordar lo siguiente:

- La interfaz no puede estar en estado *no shut*. La interfaz debe estar en completa operación.
- Para garantizar que la interfaz más estable es referenciada, es recomendable que se pueda configurar una interfaz loopback con una dirección IP y hacer referencia a esa interfaz.

FIGURA 7.41

```
<Output Omitted>
!
interface Serial0
   ip address 100.4.2.1 255.255.255.255
!
ip address 172.7.2.9 255.255.255.255
   no fair-queue
   clockrate 56000
!
interface Serial2
   no ip address
   encapsulation frame-relay
!
!
interface Serial 2.2 point-to-point
    ip unnumbered Serial1
    bandwidth 64
    frame-relay interfec-dlci 220
!
interface Serial 2.3 point-to-point
    ip unnumbered Serial0
    bandwidth 64
    frame-relay interfec-dlci 230
!
<Output Omitted>
!
router rip
network 10.0.0.0
```

CONCLUSIÓN

Como ya sabemos, el Internet está creciendo muy rápido y las redes manejan aplicaciones robustas que demandan un ancho de banda considerable, por consiguiente, se requiere de equipo más robusto para soportar tales aplicaciones.

La pequeñas y medianas empresas ya empiezan a utilizar este tipo de aplicaciones en sus conexiones de punto a punto o multipunto utilizando tecnologías como lo son Frame Relay, ISDN o PPP, por nombrar algunas y no olvidemos la convergencia de voz, datos y video.

La convergencia de voz, datos y video no es más que el transporte de paquetes de voz, datos y video sobre el mismo medio físico formándose así una red muy completa con una gran relación de costo-beneficio porque la empresa ahorra en llamadas de larga distancia y tendrá su información controlada, segura y a la mano para cuando se necesite, por todo esto una empresa puede ser más productiva.

Los ruteadores son equipos adecuados para realizar las tareas antes mencionadas. En este documento se revisó los componentes, el funcionamiento y configuración de los ruteadores para los diferentes protocolos y ambientes de redes utilizando las tecnologías WAN. También se describieron algunas de esas tecnologías WAN.

Cisco Systems ofrece certificaciones y especializaciones para vender, diseñar, instalar y poner a punto sus soluciones. Cabe mencionar que las empresas que solicitan este tipo de soluciones o servicios buscan proveedores certificados o especializados en la soluciones de Cisco y Cisco ofrece todo tipo de certificaciones y especializaciones para poder vender, instalar y configurar sus soluciones y productos y ese respaldo por parte de Cisco para los proveedores les da a los clientes finales la tranquilidad y la confianza de saber que la gente la cual está ofreciendo las soluciones de Cisco son gente calificada y certificada para esto.

BIBLIOGRAFIA

- Wendell Odom, CCIE #1624, CCNA Exam Certification Guide, Edición 2, Año 2000, pp. 500, Cisco Systems, INC.

OTRAS FUENTES

- Curso Multimedia Cisco Bussiness Essentials: Networking Fundamentals, Cisco Systems, INC.

- Corporate Headquarters, Software Configuration Guide For Cisco 3600, Cisco Systems, INC.

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rip.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ospf.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ppp.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/x25.htm

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm