



Universidad de San Carlos de Guatemala  
Facultad de Ingeniería  
Escuela de Mecánica Eléctrica

**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE FIBRA ÓPTICA PDH  
(JERARQUÍA PLESIÓCRONA)**

**Edwin Alfonso León Lossi**

Asesorado por el Ing. Luís Eduardo Duran Córdoba

Guatemala, septiembre de 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**DISEÑO E IMPLEMENTACIÓN DE UNA RED DE FIBRA ÓPTICA PDH  
(JERARQUÍA PLESIÓCRONA)**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA  
FACULTAD DE INGENIERÍA  
POR

**EDWIN ALFONSO LEÓN LOSSI**

ASESORADO POR EL ING. LUIS EDUARDO DURAN CORDOVA  
AL CONFERÍRSELE EL TÍTULO DE  
**INGENIERO ELECTRÓNICO**

GUATEMALA, SEPTIEMBRE DE 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



### **NÓMINA DE JUNTA DIRECTIVA**

|            |                                    |
|------------|------------------------------------|
| DECANO     | Ing. Murphy Olympo Paiz Recinos    |
| VOCAL I    | Inga. Glenda Patricia García Soria |
| VOCAL II   | Lic. Amahán Sánchez Álvarez        |
| VOCAL III  | Ing. Julio David Galicia Celada    |
| VOCAL IV   | Br. Kenneth Issur Estrada Ruiz     |
| VOCAL V    | Br. Elisa Yazminda Vides Leiva     |
| SECRETARIA | Inga. Marcia Ivonne Véliz Vargas   |

### **TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO**

|            |  |
|------------|--|
| DECANO     | Ing. Sydney Alexander Samuels Milson   |
| EXAMINADOR | Ing. Gustavo Adolfo Villeda Vásquez    |
| EXAMINADOR | Ing. Marvin Marino Hernández Fernández |
| EXAMINADOR | Ing. Julio Cesar Solares Peñate        |
| SECRETARIO | Ing. Pedro Antonio Aguilar Polanco     |

## **HONORABLE TRIBUNAL EXAMINADOR**

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

### **DISEÑO E IMPLEMENTACIÓN DE UNA RED DE FIBRA ÓPTICA PDH (JERARQUÍA PLESIÓCRONA),**

tema que me fuera asignado por la Dirección de la Escuela de Mecánica Eléctrica, con fecha 24 de enero de 2005.

Edwin Alfonso León Lossi

## **ACTO QUE DEDICO A:**

**Dios**

**Mis Padres**

Carlos Alfonso León Toledo

Ana Angélica Lossi Fajardo

**Mis Abuelos**

Ángel Lossi González (Q.E.P.D)

Margarita Fajardo Cabrera (Q.E.P.D)

Domingo Alfonso León Blas (Q.E.P.D)

Margarita del Carmen Toledo Cruz (Q.E.P.D)

**Mis Hermanos**

Jessica Paola León Lossi

Nancy Margarita León Lossi

## **DEDICATORIA**

### **Dios**

Por darme la fortaleza suficiente para superar y aprender de los obstáculos que se han presentado en mi vida.

### **A mis padres**

Por ser las personas que más admiro y que guiaron mis pasos para hacer de mi un hombre de bien, y de los cuales estoy orgulloso de representar lo mejor.

### **Mi país**

Guatemala, tierra labrada con el sudor y esfuerzo de cada hermano guatemalteco.

### **Mi universidad**

San Carlos de Guatemala, mi Alma Mater de conocimiento y sabiduría

### **Mi facultad**

Ingeniería, aulas impregnadas de saber, en donde dejo vida y esperanza, y me llevo sabiduría.

### **A mis amigos**

Ese grupo de personas especiales que me tendieron una mano desinteresada y que siempre estuvieron allí cuando los necesité.

## ÍNDICE GENERAL

|   |              |
|---|--------------|
| <b>ÍNDICE DE ILUSTRACIONES</b>                        | <b>IX</b>    |
| <b>GLOSARIO</b>                                       | <b>XV</b>    |
| <b>RESUMEN</b>  | <b>XIX</b>   |
| <b>OBJETIVOS</b>                                      | <b>XXI</b>   |
| <b>INTRODUCCIÓN</b>                                   | <b>XXIII</b> |
| <br>  |              |
| <b>1 CONCEPTOS BÁSICOS DE REDES DE DATOS</b>          | <b>1</b>     |
| 1.1 Introducción                                      | 1            |
| 1.2 Ancho de banda                                    | 1            |
| 1.3 Arquitectura de redes                             | 4            |
| 1.4 Interfaces y servicios                            | 7            |
| 1.4.1 Servicios orientados y no orientados a conexión | 8            |
| 1.5 Primitivas de servicio                            | 10           |
| 1.6 Modelos de referencia                             | 11           |
| 1.6.1 El modelo de referencia OSI                     | 11           |
| 1.6.2 El modelo de referencia TCP/IP                  | 14           |
| 1.7 Tipos de redes                                    | 17           |
| 1.7.1 Redes de área local                             | 18           |
| 1.7.1.1 Topologías de las LAN                         | 18           |
| 1.7.2 Redes de área extendida (WAN)                   | 22           |
| 1.7.2.1 Transmisión de datos en redes WAN             | 26           |
| 1.8 Elementos de interconexión                        | 31           |

|   |           |
|---|-----------|
| 1.8.1 Concentrador (HUB)                              | 32        |
| 1.8.2 Puentes   | 33        |
| 1.8.3 Conmutador                                      | 34        |
| 1.8.3.1 Lan virtual                                   | 36        |
| 1.8.4 Enrutador                                       | 37        |
| 1.9 Factores que afectan el diseño de una red         | 39        |
| <b>2 PROTOCOLOS DE RED</b>                            | <b>41</b> |
| 2.1 Introducción                                      | 41        |
| 2.1.1 Funciones básicas de un protocolo               | 41        |
| 2.2 Protocolos de redes LAN                           | 43        |
| 2.2.1 Técnica de acceso CSMA Y CSMA/CD                | 45        |
| 2.2.2 CSMA/CD (Ethernet /IEEE802.3)                   | 47        |
| 2.2.3 <i>Token Ring</i> /IEEE 802.5                   | 51        |
| 2.2.4 Interfaz de fibra distribuida (FDDI)            | 54        |
| 2.3 Protocolos de redes WAN                           | 56        |
| 2.3.1 Fundamentos de TCP/IP                           | 56        |
| 2.3.2 Puertos y <i>sockets</i>                        | 56        |
| 2.3.2.1 Puertos                                       | 57        |
| 2.3.2.2 <i>Socket</i>                                 | 58        |
| 2.3.3 Protocolo de datagramas de usuario              | 60        |
| 2.3.3.1 Formato del datagrama UDP                     | 61        |
| 2.3.3.2 Interfaz de programación de aplicación de UDP | 63        |
| 2.3.4 Protocolo de control de transmisión (TCP)       | 63        |
| 2.3.4.1 El principio de las ventanas                  | 63        |
| 2.3.4.2 El principio de ventanas aplicado a TCP       | 66        |



|           |   |    |
|-----------|---|----|
| 2.3.5     | Establecimiento de la sesión en TCP               | 69 |
| 2.3.6     | Formato del segmento TCP                          | 70 |
| 2.3.7     | IP ( <i>Internet Protocol</i> )                   | 71 |
| 2.3.7.1   | Asignación de direcciones y segmentación de redes | 72 |
| 2.3.7.2   | Direcciones de IP                                 | 72 |
| 2.3.7.3   | Subredes  | 75 |
| 2.3.7.4   | Máscara de subred                                 | 77 |
| 2.3.7.5   | Tipos de segmentación                             | 80 |
| 2.3.7.5.1 | Segmentación estática                             | 81 |
| 2.3.7.5.2 | Segmentación con máscara de longitud variable     | 82 |
| 2.3.8     | <i>Frame Relay</i>                                | 82 |
| 2.3.8.1   | Dispositivos de <i>Frame Relay</i>                | 84 |
| 2.3.8.2   | Circuitos virtuales                               | 85 |
| 2.3.8.2.1 | Circuitos virtuales conmutados                    | 86 |
| 2.3.8.2.2 | Circuitos virtuales permanentes                   | 87 |
| 2.3.8.3   | Identificador de conexión de enlace               | 87 |
| 2.3.8.4   | Mecanismos de control de congestión               | 88 |
| 2.3.8.4.1 | Elegibilidad para descarte                        | 89 |
| 2.3.8.4.2 | Chequeo de error                                  | 89 |
| 2.3.8.5   | Interfaz administrativa local (LMI)               | 89 |
| 2.3.8.6   | Formato de la trama de <i>Frame Relay</i>         | 90 |
| 2.3.8.6.1 | Trama de <i>Frame Relay Standard</i>              | 91 |
| 2.3.8.6.2 | Formato de la LMI                                 | 93 |
| 2.4       | Conceptos básicos de enrutamiento                 | 94 |
| 2.4.1     | Componentes del enrutamiento                      | 94 |
| 2.4.1.1   | Determinación de la trayectoria                   | 95 |
| 2.4.1.2   | Conmutación de paquetes                           | 96 |

|  |            |
|--|------------|
| 2.4.2 Algoritmos de enrutamiento                         | 97         |
| 2.4.2.1 Objetivos de diseño                              | 97         |
| 2.4.3 Tipos de algoritmos                                | 99         |
| 2.4.3.1 Estático y dinámico                              | 99         |
| 2.4.3.2 Algoritmo se una sola ruta o de múltiples rutas  | 100        |
| 2.4.3.3 Plano versus Jerárquico                          | 100        |
| 2.4.3.4 Cliente inteligente versus enrutador inteligente | 101        |
| 2.4.3.5 Estado de conexión versus vector distancia       | 102        |
| 2.4.4 Métricas de enrutamiento                           | 102        |
| <b>3 TECNOLOGÍAS DE TRANSPORTE DIGITAL</b>               | <b>105</b> |
| 3.1 Introducción   | 105        |
| 3.2 Sincronismo  | 106        |
| 3.2.1 Relojes imperfectos                                | 109        |
| 3.2.2 Fluctuación de fase                                | 110        |
| 3.2.3 Deslizamiento de trama                             | 112        |
| 3.2.3.1 Justificación positiva                           | 114        |
| 3.2.3.2 Justificación positiva/nula/negativa             | 114        |
| 3.2.4 Métodos de sincronización de red                   | 115        |
| 3.3 Jerarquías de multiplexación PDH                     | 117        |
| 3.3.1 Primer orden jerárquico trama digital de 2048 kbps | 118        |
| 3.3.1.1 Lógica de alineamiento de trama                  | 119        |
| 3.3.2 Tramas de orden superior                           | 122        |
| 3.3.2.1 Trama digital de 8448 kbps                       | 122        |
| 3.3.2.2 Ordenes jerárquicos superiores                   | 123        |
| 3.3.3 Proceso de justificación                           | 123        |
| 3.4 Fundamentos de SDH                                   | 125        |

|  |     |
|--|-----|
| 3.4.1 Multiplexión de SDH  | 127 |
| 3.4.2 La trama SDH   | 129 |
| 3.4.3 Jerarquía de la señal SDH  | 130 |
| 3.4.4 Sincronización   | 131 |
| 3.4.4.1 Compensación de sincronía en SDH                               | 133 |
| 3.4.5 Mapeo de tributario asíncronos en la trama STM-1                 | 135 |
| 3.5 Principios básicos de ATM  | 140 |
| 3.5.1 Características principales de ATM                               | 141 |
| 3.5.1.1 Ausencia de control de flujo<br>y chequeo de error nodo a nodo | 141 |
| 3.5.1.2 Operación orientada a conexión                                 | 142 |
| 3.5.1.3 Funciones de la cabecera                                       | 143 |
| 3.5.1.4 Campo de información relativamente pequeño                     | 144 |
| 3.5.2 Conexiones virtuales - Canales virtuales -<br>Caminos virtuales  | 144 |
| 3.5.2.1 Caminos virtuales  | 146 |
| 3.5.3 Conmutación  | 146 |
| 3.5.4 Formato básico de la celda                                       | 147 |
| 3.5.4.1 Formato de cabecera de ATM                                     | 148 |
| 3.5.4.2 Campos de las celdas de ATM                                    | 149 |
| 3.5.5 Modelo de referencia ATM   | 150 |
| 3.5.5.1 La capa física de ATM  | 151 |
| 3.5.5.2 Capas de adaptación de ATM                                     | 152 |
| 3.5.5.3 Capas ATM de adaptación ALL2                                   | 152 |
| 3.5.5.4 Capa de adaptación AAL 3/4                                     | 153 |
| 3.5.5.5 Capa de adaptación AAL5  | 155 |
| 3.5.6 Direccionamiento de ATM  | 155 |
| 3.5.6.1 Modelo de direccionamiento de subred                           | 155 |
| 3.5.6.2 Formato NSAP   | 155 |

|   |     |
|---|-----|
| 3.5.6.3 Campos de la dirección ATM  | 157 |
| 3.5.7 Conexiones de ATM   | 158 |
| 3.6 Evolución de la conmutación multicapa en el Internet                          | 159 |
| 3.6.1 Separación de los componentes de envío y control                            | 160 |
| 3.6.2 Algoritmo de intercambio de etiquetas                                       | 161 |
| 3.6.3 IP Sobre ATM  | 164 |
| 3.6.4 Alternativas de conmutación de múlticapa<br>para el modelo de IP sobre ATM  | 168 |
| 3.6.5 Similitudes entre las soluciones<br>de conmutación multicapa                | 169 |
| 3.6.6 Diferencias fundamentales entres<br>las soluciones de conmutación multicapa | 172 |
| 3.6.6.1 Modelo manejado por datos   | 172 |
| 3.6.6.2 Modelo manejado por control   | 173 |
| 3.6.7 Conmutación de etiquetas múltiprotocolo MPLS                                | 174 |
| 3.6.7.1 Funcionamiento de MPLS  | 176 |
| 3.6.7.2 Construcción de un una red MPLS   | 177 |
| 3.6.8 Distribución de etiquetas en MPLS   | 180 |
| 3.6.8.1 Control de distribución de etiquetas                                      | 182 |
| 3.7 Evolución de la trasmisión en fibra óptica                                    | 188 |
| 3.7.1 Desarrollo de la tecnología DWDM  | 189 |
| 3.7.2 Funciones de un sistema DWDM  | 191 |
| 3.7.2.1 Multiplexores y demultiplexores   | 193 |
| 3.7.2.2 Técnicas de multiplexión y demultiplexion                                 | 195 |
| 3.7.2.3 Multiplexores de adición y sustracción                                    | 198 |
| 3.7.3 Interfaces de DWDM  | 199 |

## **4 DISEÑO DE LA RED**

|         |   |     |
|---------|---|-----|
| 4.1     | Introducción  | 201 |
| 4.2     | Consideraciones globales de diseño                          | 205 |
| 4.2.1   | Pasos para el diseño de red                                 | 208 |
| 4.2.2   | Objetivo de la red  | 209 |
| 4.3     | Necesidades de la red                                       | 210 |
| 4.4     | Estudio de tráfico  | 212 |
| 4.5     | Descripción de la solución                                  | 216 |
| 4.5.1   | Parámetros Administrativos                                  | 219 |
| 4.5.2   | Parámetros de interfaces Tramadas y no tramadas             | 220 |
| 4.5.3   | Interfaces no tramadas                                      | 224 |
| 4.5.4   | Enrutamiento y Punteo Concurrente.                          | 231 |
| 4.5.5   | Enrutamiento y Punteo Integrado (IRB)                       | 232 |
| 4.6     | Métodos de evaluación financiera en Evaluación de Proyectos | 238 |
| 4.6.1   | Método del valor actual neto                                | 239 |
| 4.6.2   | Método de la Tasa Interna de Retorno (TIR)                  | 241 |
| 4.6.3   | Análisis financiero de la propuesta                         | 241 |
| 4.6.3.1 | Análisis Financiero Proyecto 1                              | 242 |
| 4.6.3.2 | Análisis económico del proyecto 2                           | 243 |
| 4.6.3.3 | Comparación de los dos proyectos                            | 244 |

|                        |     |
|------------------------|-----|
| <b>CONCLUSIONES</b>    | 247 |
| <b>RECOMENDACIONES</b> | 249 |
| <b>BIBLIOGRAFÍA</b>    | 251 |

## ÍNDICE DE ILUSTRACIONES

### FIGURAS

|   |    |
|---|----|
| 1. Topología de Bus   | 20 |
| 2. Topología de anillo  | 21 |
| 3. Topología de estrella  | 21 |
| 4. Ejemplo de una red CSMA/CD   | 47 |
| 5. Tramas de los estándares IEEE 802.3 y CSMA/CD                                | 49 |
| 6. Topología de anillo  | 51 |
| 7. Estructura de la trama de Pase<br>y la de información para <i>Token Ring</i> | 52 |
| 8. Diagrama de conexión de las interfaces DAS                                   | 54 |
| 9. Falla de una interfaz DAS  | 55 |
| 10. Demultiplexión UDP basada en puertos  | 61 |
| 11. Formato del datagrama UDP   | 62 |
| 12. Mensajes utilizados en el principio de ventanas básico                      | 64 |
| 13. Estado inicial de la ventana  | 64 |
| 14. Secuencia de envío y acuse  | 65 |
| 15. Deslizamiento de ventana al recibir un acuse                                | 65 |
| 16. Estado de los mensajes de TCP durante la transferencia de datos             | 67 |
| 17. Saludo de tres vías al iniciar una sesión de transferencia                  | 69 |
| 18. Secuencia de finalización de sesión de TCP                                  | 70 |
| 19. Formato de la trama TCP   | 70 |
| 20. Clases de direcciones IP  | 74 |
| 21. Representación binaria de las partes que componen la dirección IP           | 78 |
| 22. Asignación de dirección usando máscaras de subred                           | 80 |

|   |     |
|---|-----|
| 23. Elementos de una red <i>Frame Relay</i>                             | 84  |
| 24. Trama de <i>Frame Relay Standard</i>                                | 91  |
| 25. Formato de la LMI   | 93  |
| 26. Método de transmisión asíncrono                                     | 107 |
| 27. Transmisión Síncrona  | 107 |
| 28. Tiempo de bit determinada por el reloj                              | 108 |
| 29. Desviación en fase de una señal                                     | 110 |
| 30. Variación de fase entre dos señales                                 | 111 |
| 31. Rangos de frecuencia de Jitter y Wander                             | 111 |
| 32. Lectura de datos desde memoria de entrada con reloj propio          | 112 |
| 33. Variación de frecuencias continuada                                 | 113 |
| 34. Justificación positiva/nula/negativa                                | 115 |
| 35. Métodos de sincronización de una red digital                        | 115 |
| 36. Multitrama para la señal E1 a 2048 kb/s y T1 a 1544 kb/s            | 119 |
| 37. Lógica utilizada para reconocer la palabra de alineamiento de trama | 120 |
| 38. Trama y proceso de justificación en PDH                             | 121 |
| 39. Trama STM-1   | 128 |
| 40. Multiplexión de señales STM 1                                       | 128 |
| 41. Encabezado básico de la trama STM-1                                 | 129 |
| 42. Red de comunicación típica basada en capas                          | 130 |
| 43. Estructura jerárquica de la distribución de la señal de reloj       | 132 |
| 44. Bytes puntero marcando el inicio de la cabecera de POH del VC4      | 133 |
| 45. Nodo SDH con frecuencias de entrada y salida diferente              | 135 |
| 46. Mapeo de tributarios en una trama STM-1                             | 135 |
| 47. Multiplexor de ATM  | 140 |
| 48. VCI y VPI de ATM  | 144 |
| 49. Red ATM   | 145 |
| 50. Conmutador ATM  | 146 |
| 51. Formato básico de la celda ATM                                      | 147 |



|  |     |
|--|-----|
| 52. Formatos de celda de ATM   | 148 |
| 53. Modelo de referencia ATM   | 150 |
| 54. AAL1 prepara la celda para transmisión   | 152 |
| 55. Formatos de dirección ATM.   | 157 |
| 56. Descripción de las capas de control y envío                                      | 160 |
| 57. Camino conmutado por etiquetas   | 161 |
| 58. Topología física ATM y topología lógica IP superpuesta                           | 165 |
| 59. Modelo Funcional IP sobre ATM  | 166 |
| 60. Integración de un enrutador IP y un conmutador<br>ATM en un conmutador multicapa | 169 |
| 61. Sistema funcional de MPLS  | 175 |
| 62. Encabezado de etiqueta   | 175 |
| 63. Red IP clásica   | 177 |
| 64. Asignación de etiquetas por un LER   | 178 |
| 65. Flujo de datos en una red MPLS   | 179 |
| 66. Red ejemplo de MPLS  | 182 |
| 67. Control independiente  | 182 |
| 68. Control ordenado   | 183 |
| 69. DOD  | 184 |
| 70. Tablas de conexión cruzada creadas por los enrutadores                           | 184 |
| 71. Tablas internas de LSR   | 186 |
| 72. WDM de dos canales   | 190 |
| 73. Evolución de DWDM  | 191 |
| 74. Plano esquemático funcional de DWDM  | 192 |
| 75. Sistema de multiplexión y demultiplexión unidireccional                          | 194 |
| 76. Sistema Full Duplex DWDM.  | 194 |
| 77. Multiplexor óptico por refracción  | 195 |
| 78. Multiplexor por rejilla difractora   | 196 |
| 79. Enrutador óptico   | 196 |

|  |     |
|--|-----|
| 80. Multiplexor de filtro de película delgada  | 197 |
| 81. Multiplexor de adición y sustracción   | 198 |
| 82. Funciones del transpondedor  | 199 |
| 83. Diagrama de flujo para la implementación y actualización de una red                                | 203 |
| 84. Modelo de referencia TCP/IP  | 204 |
| 85. Diagrama de flujo para el diseño de una red  | 209 |
| 86. Gráfica de tráfico de Sanarate   | 213 |
| 87. Gráfica de tráfico de Teculután  | 214 |
| 88. Gráfica de tráfico de Pasabien   | 215 |
| 89. Gráfica de tráfico de Morales  | 215 |
| 90. Gráfica de tráfico de Chiquimula   | 216 |
| 91. Proceso de encapsulación de la información   | 217 |
| 92. Topología de la red  | 218 |
| 93. Pantalla de asignación de interfaces   | 220 |
| 94. Pantalla de configuración de reloj   | 221 |
| 95. Pantalla de configuración interfaz E1  | 222 |
| 96. Pantalla de configuración de bits de entramado interfaz E1   | 222 |
| 97. Pantalla de configuración interfaz óptica  | 223 |
| 98. Pantalla de configuración de bits de entramado interfaz óptica                                     | 223 |
| 99. Pantalla de configuración modulo base VCM  | 224 |
| 100. Pantalla de configuración de señales de control modulo Puente                                     | 224 |
| 101. Pantalla de configuración de los lazos de prueba internas Puente                                  | 225 |
| 102. Parámetros <i>Frame Relay</i> e IP de la interfaz puente  | 225 |
| 103. Márgenes de potencia de las interfaces ópticas  | 226 |
| 104. Disposición física de las interfaces ópticas  | 227 |
| 105. Asignación de las ranuras de tiempo de los circuitos<br>en la interfaz G.703 del nodo de Sanarate | 229 |
| 106. Dirección de la señal de sincronización   | 229 |
| 107. Gráfica de comportamiento del VPN   | 240 |

## TABLAS

|   |     |
|---|-----|
| I. Direcciones de subred                                  | 79  |
| II. Órdenes jerárquicos plesiócronicos                    | 121 |
| III. Contenedores de SDH                                  | 136 |
| IV. Tabla de conmutación ATM                              | 147 |
| V. Tablas de LER  | 179 |
| VI. LIB   | 180 |
| VII. Base de datos FEC                                    | 187 |
| VIII. FEC a NHLFE   | 187 |
| IX. NHLFE   | 187 |
| X. Resumen parámetros administrativos                     | 220 |
| XI. Tabla resumen de asignación de interfaces y circuitos | 228 |
| XII. Criterios de aceptación y rechazo                    | 239 |
| XIII. Desglose de gastos actuales                         | 242 |
| XIV. Flujo de caja proyecto 1                             | 242 |
| XV. Costos iniciales del proyecto                         | 243 |
| XVI. Cálculo de depreciaciones                            | 243 |
| XVII. Flujo de caja proyecto 2                            | 244 |
| XVIII. Tabla resumen comparativo de ambos proyectos       | 245 |



## GLOSARIO

|                        |  |
|------------------------|--|
| <b>ATM</b>             | Modo de Transferencia Asíncrona o <i>Asynchronous Transfer Mode</i> (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.                            |
| <b>Bit</b>             | Es el acrónimo de <i>Binary digit</i> . (dígito binario). Un bit es un dígito del sistema de numeración binario  |
| <b>Byte</b>            | Se describe como la unidad básica de almacenamiento de nformación, generalmente equivalente a ocho bits, pero el tamaño del byte depende del código de caracteres o código de información en el que se defina, también llamado octeto.                 |
| <b><i>Backbone</i></b> | Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al <i>backbone</i> (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas. |
| <b>Conmutación</b>     | Mecanismo por el cual los paquetes o mensajes son enviados entre diferentes sistemas centrales sin que exista un ruta previamente establecida.   |

**Decibel** Se denomina decibelio a la unidad empleada en Acústica y Telecomunicación para expresar la relación entre dos potencias, acústicas o eléctricas.

**Enrutamiento** Mecanismo por medio del cual se selecciona una ruta para que un mensaje llegue de la fuente al destino.

**Frecuencia** Es un término empleado en física para indicar la velocidad de repetición de cualquier fenómeno periódico. Se define como el número de veces que se repite un fenómeno en la unidad de tiempo.

***Frame Relay*** Tecnología de transmisión de datos que consiste en la conmutación de unidades de datos de tamaño variable denominadas tramas.

**IP** Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. La versión actual es IPv4 mientras que ya esta en desarrollo la versión 6 (IPv6). También se refiere a las direcciones de red Internet (IP Address).

**MAC** En redes de computadoras Media Access Control address cuyo acrónimo es MAC es un identificador físico -un número, único en el mundo, de

48 bits- almacenado en fábrica dentro de una tarjeta de red o una interfaz usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de Internet.

### **Métricas**

Método mediante el cual un protocolo de enrutamiento determina que una ruta es mejor que otra. Esta información se almacena en tablas de enrutamiento. Las métricas incluyen ancho de banda, costo de la comunicación, retardo, número de saltos, carga, MTU, costo de ruta, y confiabilidad. A menudo denominada simplemente métrica.

### **Protocolo**

Se le llama protocolo de red o protocolo de comunicación al conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red. En este contexto, las entidades de las cuales se habla son programas de computadora o automatismos de otro tipo, tales y como dispositivos electrónicos capaces de interactuar en una red.

### **Plesiocrono**

Plesiocrono se origina del griego plesio ("cercano" o "casi") y cronos ("reloj"), el cual significa que dos ojos están cercanos uno del otro en tiempo, pero no exactamente el mismo. Contrasta con isocronos, el cual significa "mismo reloj".

**PDH**

La Jerarquía Digital Plesiócrona, conocida como PDH (Plesiochronous Digital Hierarchy), es una tecnología usada en telecomunicación para transportar grandes cantidades de información mediante equipos digitales de transmisión que funcionan sobre fibra óptica, cable coaxial o radio de microondas.

**SDH**

Synchronous Digital Hierarchy Estandar europeo que define una serie de tasas y formatos normalizados que se transmiten usando señales sobre fibra óptica. SDH es similar a SONET, con una tasa básica de 155,52 Mbps, diseñado en STM1

**TCP**

*Transmission Control Protocol*. Especificación software que empaqueta y desempaqueta los datos recibidos y enviados en paquetes, gestiona la transmisión de éstos por la red comprueba los errores.



## RESUMEN

La competencia combinada con la gran demanda y las exigencias de los consumidores han forzado a las empresas a mantenerse siempre actualizados y de buscar soluciones óptimas en la utilización de los recursos, en este sentido las telecomunicaciones son un aspecto que cada día cobra mayor importancia en el funcionamiento de una empresa, y a ido evolucionando poderse adaptar a las necesidades siempre crecientes de prestación de servicios.

En un principio las necesidades de una empresa eran nada más el simple hecho de compartir recursos de oficina, como por ejemplo, un centro de impresión, para lo que la solución aplicada consistía en la utilización de medios removibles de la maquina como por ejemplo los discos flexibles, el proceso consistía en guardar el o los documentos a compartir en uno de estos medios para luego transportarlos hasta su destino, a estas redes se les llamo "redes a pie", con este método existía la posibilidad de duplicidad de documentos y de perdida de información. Con el advenimiento de maquinas con más capacidad de procesamiento y de almacenamiento, con la respectiva alza en los precios se hizo necesario una manera de centralizar las operaciones en estos equipos de alto rendimiento, de allí fue donde nacieron las redes de área local en sus diferentes variantes en tecnología, variantes que describo en el primer capítulo de este trabajo de graduación.

Ahora la tarea consistía en comunicar a estos segmentos aislados de la empresa, para poder compartir información en un tiempo real o por lo

menos prudencial, para desarrollar transacciones. La primera aproximación para resolver este tipo de problema fue utilizar la red de telefonía convencional esto solucionó por un tiempo la situación , pero al crecer las necesidades de ancho de banda de las aplicaciones nuevos sistemas de comunicación debieron ser implementados, mismos que describo en los capítulos dos y tres del presente trabajo.

El proceso de diseño e implementación de una red requiere de diversas etapas que muy a menudo son pasadas por alto, ya sea por inexperiencia de las personas o por negligencia, en el último capítulo del presente trabajo de graduación, presento algunos lineamientos y procedimientos para el análisis de los diferentes factores que afectan un diseño de red.

## OBJETIVOS

### General

Desarrollar los criterios generales necesarios para el diseño e implementación de una red de transporte de datos, atendiendo a los factores de coste, prestaciones y necesidades específicas de acuerdo al tipo de servicios y aplicaciones que sean requeridas por los usuarios de la red.

### Específicos

1. Obtener conocimientos de elementos básicos en lo que respecta al diseño de redes de transmisión y distribución de datos como son: Las diferentes topologías de las redes, Protocolos de red, elementos activos de una red y tipos de servicios que puede proporcionar una red dependiendo de su infraestructura.
2. Desarrollar criterios de planificación y estructuración de las redes en general, a su vez conocer los tipos de protecciones que debe tener una red para asegurar un servicio continuo y por último los alcances que puede tener y debe tener una red.
3. Compartir la experiencia adquirida durante el proceso de diseño e implementación de una red de datos real donde se tuvo la oportunidad de aplicar los conocimientos adquiridos y aprender nuevos conceptos que intervienen dentro del diseño, planeación y ejecución de un proyecto.



## INTRODUCCIÓN

Considero que no hay mejor experiencia para un profesional que la adquirida con la practica, mediante la cual puede poner a prueba sus capacidades natas y las aprendidas como estudiante dentro de las aulas de la universidad, debido a esto decidí basar mi trabajo de graduación en un proyecto real, en el cual participe activamente en el diseño e implementación, para poder explicar el porque de las decisiones que tomamos a la hora de la implementación tuve que explicar en los primeros tres capítulos los diferentes factores que intervienen en la selección de una solución factores que deben se deben balancear para poder tener una solución optima, tanto técnica como económica.

En el primer capítulo aparecen conceptos básicos de las redes de datos, los objetivos principales de una red no importando si es de área local o de área extendida, lo procesos que intervienen en la comunicación del la información desde que es enviada de la estación de un usuario hasta que alcanza su destino, conceptos importantes que fijan las limitantes de desempeño de las redes como lo es el ancho de banda, la arquitectura sobre la cual se basa una red para poder funcionar y poder adaptarse a los cambios de las exigencias de las nuevas aplicaciones. Como todas las cosas en la ingeniería deben poder ser modeladas y las redes de telecomunicación no son excepción dentro de este capítulo también incluimos una breve explicación de los modelos que son utilizados para la descripción del funcionamiento de una red, por último se explica el funcionamiento de los diferentes dispositivos de interconexión que son bloques fundamentales

sobre los cuales descansa el funcionamiento de una red, dando criterios básicos de donde y porque se utiliza cada uno de ellos.

Sin excepción todas las cosas necesitan de reglas y parámetros para poder funcionar, por eso, en el segundo capítulo explico algunos de los protocolos de red mas implementados en la actualidad, no importando para que tipo de red, las funciones de un protocolo invariablemente son: segmentación y reconstrucción, encapsulación, control de conexión, entrega ordenada, control de flujo y control de error.

Aunque todos los protocolos realizan las mismas operaciones la selección correcta del protocolo de red es importante debido a que dependiendo de la selección los elementos de red deberán ser adquiridos con la capacidad de soportar dicho protocolo esto incluye a los elementos de interconexión como a los elementos clientes de la red, esto se aplica a las redes en general, varios de los factores más importantes dentro de la decisión del protocolo a implementar es la escalabilidad, la interoperabilidad con otra tecnologías, y el factor económico, esto por mencionar algunos.

En la actualidad una de las necesidades imperante para cualquier tipo de empresa es la estar comunicada, las necesidades de cada empresa varían desde una simple conexión telefónica a Internet, hasta tener canales dedicados de varios megabytes de ancho de banda entre sus sucursales y sus oficinas principales, en orden de satisfacer la necesidades de las empresas los proveedores de servicios de telecomunicaciones han tenido que desarrollar técnicas de transmisión de datos que puedan adaptarse dinámicamente a los volúmenes de transferencias de datos de las empresas en general, y es de esas técnicas de transmisión de las cuales hablaremos en el tercer capítulo de este trabajo, exploraremos varias de las tecnologías ya

establecidas y otras, que están ganando terreno en lo que al transporte de datos se refiere.

Si no se toma el tiempo para planificar una red, la interconexión mediante el uso de cualquier tipo de protocolo puede provocar complicaciones no previstas debido a posibles fallas de diseño, por este motivo en el cuarto capítulo analizamos los lineamientos mínimos que debemos tomar en cuenta a la hora de analizar y proponer un diseño para implementar una red por primera vez o sustituir un diseño que ya está en funcionamiento, en nuestro caso, presentamos un diseño para sustituir un sistema de interconexión a través de un proveedor de servicios aun sistema de interconexión basado en infraestructura propia, analizando tanto los aspectos técnicos como económicos.





# 1 CONCEPTOS BÁSICOS DE REDES DE DATOS

## 1.1 Introducción

Las redes de datos tienen como objetivo principal, hacer posible el intercambio de información a varios usuarios o estaciones de trabajo, para poder entender los procesos que hacen posible que este objetivo se cumpla, debemos poseer conocimientos teóricos básicos de todos los factores que intervienen en las diferentes etapas que pasa la información desde que es transmitida y es recibida y entregada al usuario final, en esencia este capítulo trata de cubrir la mayoría de estos aspectos para que el lector pueda comprender los capítulos que preceden a este.

## 1.2 Ancho de banda

La comprensión del concepto de ancho de banda es de suma importancia dentro del contexto de las comunicaciones ya que dentro de un enlace, el ancho de banda es una de las limitaciones más importantes para tener en cuenta dependiendo del medio que se este usando para transmitir. Podemos definir el ancho de banda como sigue: El ancho de banda es el rango entre dos frecuencias determinadas, utilizado para un propósito específico. Para nuestros propósitos debemos considerar el ancho de banda, como el rango de frecuencias dentro de las cuales las características de desempeño de un elemento específico esta por encima de un límite determinado. Para filtros, atenuadores, amplificadores, línea de transmisión, y otros elementos tanto

activos como pasivos, estos límites están definidos por la caída de 3 decibeles por debajo de la potencia promedio dentro de la ancho de banda, o debajo del nivel establecido a una frecuencia de referencia.

Antes de continuar hablando tenemos que definir ciertas unidades básicas que nos ayudarán a comprender de forma fácil el concepto de ancho de banda, la primera de estas unidades es la unidad más pequeña de información en un sistema digital de transmisión de información esta unidad es el bit con sus diferentes múltiplos como el byte que es un octeto de bits, el killobit que es un millar de bits, el megabit que es un millón de bits, ETC. Otra unidad que debe ser tomada en cuenta es la unidad de tiempo que en nuestro caso es el segundo. De manera que si tratáramos de describir la cantidad de información que fluye en un período DETERMINADO de tiempo, podríamos utilizar las unidades "bits por segundo" para describir este flujo.

Si permanecemos dentro del dominio de los sistemas binarios, la primera aproximación que tendremos del ancho de banda es de un bit por hertz de ancho de banda. Esta aproximación apenas da cabida a problemas nominales de canal como respuesta a amplitud y frecuencia, distorsión de fase, y ruido. Como se puede apreciar esta primera aproximación de ancho de banda es demasiado rustico. H. Nyquist de los laboratorio Bell esencialmente propuso que la transmisión libre de errores debía tener una tasa de dos bits por cada hertz de ancho de banda, este es llamado comúnmente la a tasa de Nyquist o el ancho de banda de *Nyquist*. En otras palabras si nosotros tenemos un ancho de banda de 1000Hz, en teoría podríamos transportar 2000 bps sin ningún error. Por otra parte Claude Shannon, también de los laboratorios Bell,

sostenía la teoría de que la capacidad de transmisión del canal se relaciona con el ancho de banda ideal para la transmisión sin errores, de la siguiente forma:

### **Ecuación 1**

$$C=W\log_2(1+S/N)$$

Donde S/N es relación de señal a ruido, W es el ancho de banda y C es la capacidad del canal. Muy a menudo escucharemos del límite de Shannon en referencia a la fórmula de arriba. Como ya hemos mencionado uno de los mayores problemas en el canal de transmisión es la distorsión de fase. En su mayoría este efecto del canal el que nos restringe a alcanzar el límite de Shannon. En un canal de ancho de banda limitado mientras la tasa de bits se incrementa más allá de cierto punto, la interferencia intersímbolo empieza a cobrar más importancia en la tasa de error de bits. Todo esto considerando que la transmisión se hace en banda base.

Existe otro concepto importante que debería haber tenido en cuenta: el *rendimiento*. El rendimiento generalmente se refiere al ancho de banda real medido, en un momento específico del día, usando rutas específicas de la red de datos, mientras se descarga un archivo específico. Desafortunadamente, por varios motivos, el rendimiento a menudo es mucho menor que el ancho de banda digital máximo posible del medio que se está usando. Algunos de los factores que determinan el rendimiento y el ancho de banda son los siguientes:

- dispositivos de conexión
- tipo de datos que se transfieren
- topología
- cantidad de usuarios

- computador del usuario

Al diseñar una red, es importante tener en cuenta el ancho de banda teórico. La red no será más rápida que lo que los medios permiten. Al trabajar con redes reales, deberá medir el rendimiento y decidir si éste es adecuado para el usuario.

### **1.3 Arquitectura de redes**

Para poder explicar lo que es la arquitectura de redes vamos a utilizar la historia de lo que al final nos impulsa a crearlas, la historia del ordenador o computador, en un principio el diseño de una computadora era tan compleja que cada vez que se diseñaba un nuevo modelo, todo tenía que ser rediseñado única y exclusivamente para este nuevo modelo con esto no se consideraba la interoperabilidad con otros modelos ya que los objetivos que se perseguían eran el correcto y eficiente funcionamiento del nuevo ordenador.

IBM lanzó al mercado una nueva clase de computador que en realidad era una familia de computadoras que compartían la misma arquitectura, esta establecía parámetros de funcionamiento compatibles con todos los modelos de la familia, esto permitía que todos los modelos de la familia, que comprendían una gama diversa de tamaño y poder de procesamiento, pudieran correr las mismas aplicaciones y el mismo sistema operativo. Esta arquitectura llamada Sistema 360 ha ido evolucionando hasta llegar a la arquitectura ESA/390 que es la que actualmente se utiliza en los grandes servidores IBM modernos.

Las primeras redes de computadoras tuvieron unos inicios muy similares a los primeros computadores: Las redes y los protocolos se diseñaban pensando en el hardware a utilizar en cada momento, sin tener en cuenta la evolución previsible, ni la interconexión y compatibilidad con equipos de otros fabricantes. Muchas veces al evolucionar los equipos de red sucedió la misma situación que para los ordenadores, y era que para cada uno de estos nuevos elementos debían ser reescritos los protocolos de comunicación, y en la mayoría de los casos el código escrito para los protocolos anteriores resultaba inútil y no podía ser reutilizado.

El inconveniente de la falta de compatibilidad entre protocolos se solucionó de forma parecida a la que se había hecho con las computadoras. Cada fabricante elaboró su propia arquitectura de red, que permitía independizar las funciones y el software del hardware concreto utilizado. De esta forma cuando se quería cambiar algún componente sólo la función o el módulo afectado tenía que ser sustituido. La primera arquitectura de redes fue anunciada por IBM en 1974, a esta arquitectura se le denominó SNA (*Systems Network Architecture*). La arquitectura SNA se basa en la definición de siete niveles o capas, cada una de las cuales ofrece una serie de servicios a la siguiente, la cual se apoya en esta para implementar los suyos, y así sucesivamente. Las ideas básicas del modelo de capas son las siguientes:

1. La capa  $n$  ofrece una serie de servicios a la capa  $n+1$ .
2. La capa  $n$  sólo 've' los servicios que le ofrece la capa  $n-1$ .
3. La capa  $n$  en un determinado sistema solo se comunica con su homóloga en el sistema remoto (comunicación de igual a igual o 'peer-to-peer'). Esa 'conversación' se efectúa de acuerdo con una serie de reglas conocidas como protocolo de la capa  $n$ .

La comunicación entre dos capas adyacentes en un mismo sistema se realiza de acuerdo con una interfaz. La interfaz es una forma concreta de implementar un servicio y no forma parte de la arquitectura de la red. Una arquitectura de red no queda bien definida hasta que las funciones de sus capas son descritas a detalle por ejemplo deben ser descritos los servicios que prestan a las capas superiores, los protocolos que utilizan para hablar con sus iguales en el modelo, al conjunto de estos protocolos se les llama pilas de protocolo como por ejemplo la pila de protocolos de TCP.

La misión de un modelo de capas es simplificar considerablemente la tarea de cada una de las entidades, que sólo tiene que preocuparse de una pequeña parte de todo el mecanismo. En esencia se trata de aplicar a la resolución de problemas un mecanismo tal que divide las tareas de comunicar a dos clientes en tareas más pequeñas y más simples aliviando un poco la complejidad que pueda tener este proceso.

Cuando un sistema desea enviar un mensaje a un sistema remoto normalmente la información se genera en el nivel más alto; conforme va descendiendo se producen diversas transformaciones, por ejemplo adición de cabeceras, de colas, de información de control, la fragmentación en paquetes más pequeños si es muy grande (o más raramente la fusión con otros si es demasiado pequeño), etc. Todas estas operaciones se invierten en el sistema remoto en las capas correspondientes, llegando en cada caso a la capa correspondiente en el destino un mensaje igual al original.

## 1.4 Interfaces y servicios

Debido a su importancia vamos a estudiar con más detalle que es un servicio. Empezaremos con algunas definiciones.

Llamaremos entidad a los elementos activos en cada capa. Una entidad puede ser un proceso, un componente hardware, o una combinación de ambos. Una computadora puede tener una o varias entidades en cada capa (por ejemplo una computadora con dos tarjetas de conexión a LAN).

Llamaremos entidades iguales o entidades pares ('peer entities' en inglés) a dos entidades diferentes que pertenecen a la misma capa; generalmente estarán en diferentes máquinas, pero podrían estar en la misma.

Las entidades de la capa  $n$  implementan los servicios que utiliza la capa  $n+1$ . En este caso la capa  $n$  actúa como el proveedor del servicio y la capa  $n+1$  es el usuario del servicio. El uso que la capa  $n$  haga de los servicios de la capa  $n-1$  es algo que no afecta ni incumbe a la capa  $n+1$ .

Los servicios están disponibles en los SAPs (*Service Access Points*). Los SAPs de la capa  $n$  son los puntos donde la capa  $n+1$  puede acceder a los servicios ofertados. Cada SAP de cada entidad de la capa  $n$  tiene una dirección que le identifica de forma única en toda la red.

Denominamos interfaz al conjunto de reglas que gobiernan el intercambio de información entre capas. En una comunicación la entidad de la capa  $n+1$

intercambia una IDU (Interface Data Unit) con la entidad de la capa n a través del SAP. La IDU esta formada por una SDU (Service Data Unit) e información de control. La SDU es la información que se transmite a la entidad equivalente (peer) en el lado contrario, y de allí a la capa n+1 a través de su SAP. La información de control es necesaria como su nombre indica para que la capa n haga correctamente su trabajo, pero no es parte de los datos mismos. En la especificación de una arquitectura solo es necesario describir la estructura de la SDU, pero no la de la IDU; ésta se describe en la interfaz, que puede ser distinta para cada implementación.

Para transferir la SDU (Service Data Unit) la entidad de la capa n puede tener que fragmentarla en varias PDUs (Protocol Data Units). Cada PDU llevará una cabecera que permitirá a la entidad de la capa n en el otro lado ensamblar de nuevo la SDU correctamente.

#### **1.4.1 Servicios orientados y no orientados a conexión**

Como se ha descrito anteriormente en el modelo SNA la capa n utiliza los servicios de la capa n-1 para poderse comunicar con su capa igual en el lado de destino, según el funcionamiento de cada uno de estos servicios se puede distinguir dos tipos de servicios y son: Los servicios orientados a conexión y los no orientados a conexión a continuación mencionaremos las diferencias entre ambos servicios.

Servicio orientado a conexión también llamado CONS por sus siglas en ingles tiene dentro de sus funciones de comunicación el establecimiento de un canal el envío de los datos o información y por último el cierre del canal



que en un principio abrió. Dicho canal es conocido como circuito virtual, dentro de las clases de circuitos virtuales se reconocen dos tipos uno de ellos el circuito virtual permanente PVC y el circuito virtual conmutado SVC.

El circuito virtual permanente está establecido todo el tiempo que la red está operativa. Mientras que los circuitos conmutados se establecen y terminan a petición del usuario, normalmente cuando hay paquetes que se quieren transmitir. Una vez establecido el VC el camino físico que van a seguir los datos está determinado; los paquetes deben ir todos por él desde el origen al destino, y llegar en el mismo orden con el que han salido. Dado que el VC establece de forma clara el destino, los paquetes no necesitan contener su dirección.

En el servicio no orientado a conexión la forma de establecer la comunicación es menos rigurosa ya que en este tipo de servicios, cuando una entidad tiene información que transmitir sencillamente la envía en forma de paquetes, confiando que estos llegaran a su destino de alguna manera, no se establece previamente un VC ni otro tipo de canal de comunicación punto a punto ; los paquetes pueden ir por caminos físicos diversos, y deben incluir cada uno la dirección de destino. Los paquetes deben ser almacenados por nodos intermedios de la red, y reenviados mas tarde. Aunque lo normal es que lleguen en el mismo orden con que han salido, esto no esta garantizado como ocurría en el servicio orientado a conexión debido al almacenamiento en nodos intermedios y a la diversidad de caminos físicos posibles. A los paquetes enviados en un servicio no orientado a conexión se les denomina datagramas, ya que cada paquete viaja hacia su destino de forma completamente independiente de los demás como si fuera un telegrama. En cualquiera de los dos tipos de servicio antes mencionados es posible que se produzca pérdida de información; también puede ocurrir que el tiempo de envío del paquete, también llamado retardo o latencia sea demasiado grande o fluctúe dentro de un amplio

rango debido a la carga o congestión en la red. En algunos casos se requiere una entrega fiable, es decir que se garantice la entrega de los paquetes, o un retardo garantizados, o sea no superiores a un determinado valor. Por ejemplo si transferimos un archivo, normalmente dividiéndolo en múltiples paquetes, necesitaremos un servicio fiable en la entrega, pero podemos tolerar un retardo más o menos grande; por el contrario la voz, o el vídeo (imagen en movimiento) toleran un pequeño porcentaje de pérdidas, pero requieren un retardo reducido y constante. Cuando al establecer una comunicación se solicita un nivel mínimo para alguno de éstos parámetros se dice que se requiere una calidad de servicio (llamada QoS, Quality of Service). No todos los protocolos o redes ofrecen la posibilidad de negociar calidades de servicio; en estos casos el protocolo simplemente aprovecha los medios disponibles lo mejor que puede, intentando evitar las congestiones y situaciones críticas en lo posible, y repartir los recursos entre los usuarios de manera mas o menos equilibrada; esta estrategia se denomina del 'mejor esfuerzo' (o también 'best effort'). Como ejemplos de redes con QoS podemos citar ATM, como ejemplos de redes 'best effort' podemos mencionar TCP/IP (la Internet) y Ethernet.

## **1.5 Primitivas de servicio**

Como hemos visto, en el modelo de capas, cada capa ofrece sus servicios a la siguiente y cada una de las capas es independiente de la otra. El servicio se define por un conjunto de operaciones u órdenes que la capa superior puede mandar a la capa inferior. Dicho conjunto de operaciones se denomina primitivas.

## **1.6 Modelos de referencia**

Vamos a hablar ahora con cierto detalle de las dos arquitecturas de redes más importantes en la actualidad, correspondientes a los modelos OSI (*Open Systems Interconnection*) y TCP/IP (*Transmission Control Protocol/Internet Protocol*). Conviene destacar que la arquitectura es una entidad abstracta, más general que los protocolos o las implementaciones concretas en que luego se materializan éstos. Típicamente para cada capa de una arquitectura existirán uno o varios protocolos, y para cada protocolo habrá múltiples implementaciones. Las implementaciones cambian continuamente; los protocolos ocasionalmente se modifican o aparecen otros nuevos que coexisten con los anteriores o los dejan anticuados; sin embargo una vez definida una arquitectura ésta permanece esencialmente intacta y muy raramente se modifica.

### **1.6.1 El modelo de referencia OSI**

Mas o meno al mismo tiempo en que el proyecto del gobierno Estados Unidos DARPA se estaba desarrollando y que eventualmente llego a ser lo que se conoce como TCP/IP y el Internet, un estándar alternativo estaba siendo desarrollado por la CCITT y la ISO.

El estándar resultante fue el modelo de referencia OSI , que define un modelo de comunicación de siete capas. Cada capa del modelo de referencia provee un conjunto de funciones a la capa superior, y a la vez, basa su funcionamiento en las funciones de la capa inferior. Aunque los mensajes solamente pueden pasar de forma vertical a través de la pila de

capas del modelo, desde un punto de vista lógica , cada capa se comunica directamente con su capa par en su destino.

El modelo OSI ofrece un esquema por capas para el diseño de redes. Algunas de esta capas pueden no utilizarse de manera uniforme en la implementación de un protocolo dado, pero el modelo OSI se desglosa de tal forma que cualquier función de una red puede estar representada por una de sus siete capas o niveles. Cuando se envía un paquete de un cliente a otro de una red se pasa desde la aplicación; se les aplica el modelo; atraviesan el medio o soporte como una señal eléctrica u óptica que representan unos y ceros individuales, y luego se vuelven a trasladar al modelo del lado del receptor en todo este proceso, cada capa que tiene un protocolo aplicable añade al paquete un encabezamiento , que identifica el modo en que el protocolo deberá ría procesar el paquete en el otro lado de la comunicación. Este proceso recibe el nombre en encapsulado. Al llegar al destino, el paquete volverá a ser procesado por el modelo, de modo que se eliminarán los encabezamientos de protocolos añadidos.

En el momento en que el paquete llega a la aplicación, lo único que queda son los datos, es decir, la carga útil.

Seguidamente se estudiarán en detalle las características específicas de cada una de las distintas capas y los procesos adicionales de los que es responsable.

- **Aplicación** (capa 7) La capa de aplicación es la capa del modelo OSI más cercana al usuario; suministra servicios de red a las aplicaciones del

usuario. Esta capa es responsable de la comunicación directa con la propia aplicación, permite escribir las aplicaciones con poco código de red. En vez de ello, la aplicación informa al protocolo de la capa de aplicación de lo que necesita y es responsabilidad de dicha capa de aplicación traducir la petición a algo que la pila de protocolos sea capaz de entender.

- **Presentación** (capa 6) La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. Dicho de otra manera esta es responsable del formateo del un paquete: compresión, encriptación decodificación y correspondencia de paquetes. Si se recibe, por ejemplo un correo electrónico y el texto está encriptado, será un problema de capa de presentación.
- **Sesión** (capa 5) Como su nombre lo implica, la capa de sesión establece, administra y finaliza las sesiones entre dos clientes que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. Esto lo logra asegurándose que la aplicación del otro extremo tenga configurados los parámetros correctos para establecer una aplicación bidireccional con la aplicación fuente.
- **Transporte** (capa 4) La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Según el protocolo que se use esta capa puede ser responsable de la detección y recuperación de errores, del establecimiento y terminación de sesiones en la capa de transporte, del multiplexado, de la fragmentación y del control de flujo.

- **Red** (capa 3) La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de clientes que pueden estar ubicados en redes geográficamente distintas.
- **Enlace** (capa2) La capa de enlace de datos proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico y del control de la NIC. Según el protocolo de que se trate, puede realizar también el control de flujo. Esta capa añade también la FCS, que ofrece cierta capacidad de detección de errores.
- **Física** (capa 1) La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física

### 1.6.2 El modelo de referencia TCP/IP

En 1969 la agencia ARPA (*Advanced Research Projects Agency*) del Departamento de Defensa de los Estados Unidos inició un proyecto de interconexión de computadoras mediante redes telefónicas. Al ser un proyecto desarrollado por militares en plena guerra fría un principio básico de diseño era que la red debía poder resistir la destrucción de parte de su infraestructura, de forma que dos nodos cualesquiera pudieran seguir comunicados siempre que hubiera alguna ruta que los uniera. Esto se consiguió en 1972 creando una red de conmutación de paquetes denominada ARPAnet, la primera de este tipo que operó en el mundo. La conmutación de paquetes unida al uso de topologías

malladas mediante múltiples líneas punto a punto dio como resultado una red altamente fiable y robusta.

La ARPAnet fue creciendo paulatinamente, y pronto se hicieron experimentos utilizando otros medios de transmisión de datos, en particular enlaces por radio y vía satélite; los protocolos existentes tuvieron problemas para ínter operar con estas redes, por lo que se diseñó un nuevo conjunto o pila de protocolos, y con ellos una arquitectura. Este nuevo conjunto se denominó TCP/IP (*Transmission Control Protocol/Internet Protocol*) nombre que provenía de los dos protocolos más importantes que componían la pila; la nueva arquitectura se llamó sencillamente modelo TCP/IP, los nuevos protocolos fueron especificados por vez primera por Cerf y Kahn en un artículo publicado en 1974. A la nueva red, que se creó como consecuencia de la fusión de ARPAnet con las redes basadas en otras tecnologías de transmisión, se la denominó Internet.

La aproximación adoptada por los diseñadores del TCP/IP fue mucho más pragmática que la de los autores del modelo OSI. Mientras que en el caso de OSI se emplearon varios años en definir con sumo cuidado una arquitectura de capas donde la función y servicios de cada una estaban perfectamente definidas, y solo después se planteó desarrollar los protocolos para cada una de ellas, en el caso de TCP/IP la operación fue a la inversa; primero se especificaron los protocolos, y luego se definió el modelo como una simple descripción de los protocolos ya existentes. Por este motivo el modelo TCP/IP es mucho más simple que el OSI. También por este motivo el modelo OSI se utiliza a menudo para describir otras arquitecturas, como por ejemplo la TCP/IP, mientras que el modelo TCP/IP nunca suele emplearse para describir otras arquitecturas que no sean la suya propia.

En el modelo TCP/IP se pueden distinguir cuatro capas:

La capa cliente -red

La capa Internet

La capa de transporte

La capa de aplicación

Pasemos a describirlas brevemente.

- **La Capa de aplicación** (capa 4). Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece mas acertada. La capa de aplicación contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios
- **Capa de transporte** (Capa 3). Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos protocolos: el TCP (Transmission Control Protocol) ofrece un servicio fiable, con lo que los paquetes (aquí llamados segmentos) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un host rápido sature a un receptor más lento. Ejemplos de protocolos de aplicación que utilizan TCP son el SMTP (Simple Mail Transfer Program, correo electrónico) y el FTP (File Transfer Protocol).
- **Capa de Internet** (capa2). Esta capa es el 'corazón' de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de encaminar los paquetes de la forma más conveniente para



que lleguen a su destino, y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada. A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para cada una intervienen en la descripción del modelo, la capa internet define aquí un formato de paquete y un protocolo, llamado IP (Internet Protocol), que se considera el protocolo 'oficial' de la arquitectura.

- **La Capa Cliente-red (Capa 1)** Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el host a la red por medio de algún protocolo que permita enviar paquetes IP. Podríamos decir que para el modelo TCP/IP esta capa se comporta como una 'caja negra'. Cuando surge una nueva tecnología de red (por ejemplo ATM) una de las primeras cosas que aparece es un estándar que especifica de qué forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente

## 1.7 Tipos de redes

Antes de definir los diferentes tipos de redes de datos, debemos definir el concepto de red de datos con este nombre definiremos al conjunto de elementos que funcionan como una carretera transportando datos de la estación de un usuario a la estación de otro.

Existen en general dos tipos de redes de datos : Redes de área local LAN por sus siglas en ingles y las redes de área extendida WAN. También por sus siglas en ingles. Los dos tipos difieren por el área de cobertura y otras características que explicaremos con más detalle en apartados siguientes.

### **1.7.1 Redes de área local**

Las redes de área local (LAN) están definidas por la IEEE como sigue “ Una red de comunicación que interconecta una variedad de elementos (p.e., computadores personales, estaciones de trabajo, impresoras, etc.) que pueden transmitir datos sobre un área limitada, típicamente dentro de un edificio.

Dentro del medio de transmisión para este tipo de red podemos encontrar par de cobre, cable coaxial, fibra óptica y radio. La implementación de los sistemas de cable coaxial se esta debilitando a favor de la instalación de par trenzado de alta calidad. Las redes inalámbricas son las más recientes en este tipo de redes.

Las ratas de datos pueden variar de 1 Mbps a 100Mbps. Factores como la rata de datos, el número de elementos conectados, el espaciamiento de estos elementos y la extensión de estas dependen de:

- El medio de transmisión empleado,
- La técnica de transmisión ( p.e., banda base o banda ancha),
- El protocolo de acceso de la red; y
- La incorporación de elementos tales como repetidores, concentradores, puentes, enrutadores.

La mayoría de las LAN operan sin algoritmos de corrección de error con BER especificados en el rango de  $1 \cdot 10^{-8}$  a  $1 \cdot 10^{-12}$  o mejor.

La aplicación más común de una LAN es el interconectar terminales de datos y otros recursos de procesamiento, donde todos los elementos residen en un solo edificio o complejo de edificios, y usualmente estos recursos tienen un mismo propietario.

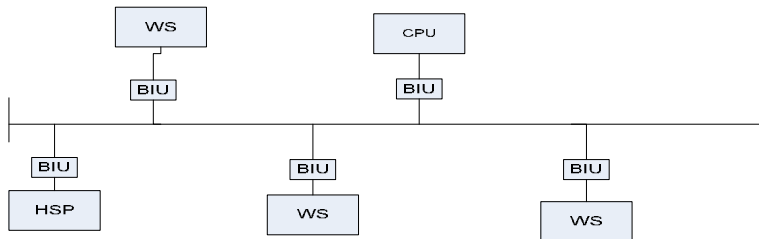
Una LAN permite compartir eficientemente los costos de operación de equipos de alto costo como son, medios de almacenamiento en masa, computadores centrales e impresoras de alta velocidad. El hecho de compartir recursos es probablemente tan importante para una LAN como el hecho de que esta sirva como enlace para la red interna de la compañía.

Hay dos técnicas genéricas de transmisión utilizadas por las LAN: Banda base y Banda ancha. La transmisión en banda base puede ser definida como la aplicación de la banda base directamente al medio de transmisión. La transmisión de banda ancha en este contexto, en cuando la banda base del elemento de datos es trasladada en frecuencia para alojarla en una frecuencia definida en el espectro de radiofrecuencia. Este tipo de transmisión requiere la utilización de un modem para llevar a cabo dicha traslación. La transmisión en banda base usualmente también requiere algún tipo de elemento para acondicionar la señal.

### 1.7.1.1 Topologías de las LAN

Existen tres tipos básicos de topologías de LAN: bus, anillo y estrella. Estas son ilustradas en la figura junto con la red de árbol, que es una red derivada de la topología de bus convencional.

**Figura 1. Topología de Bus.**



BIU: interfaz de banda base

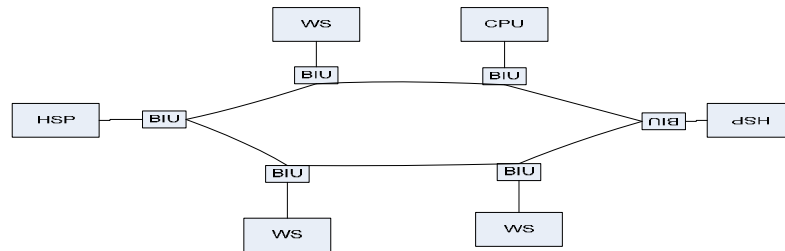
WS: estación de trabajo

HSP: impresora de alta velocidad

CPU: unidad central de proceso.

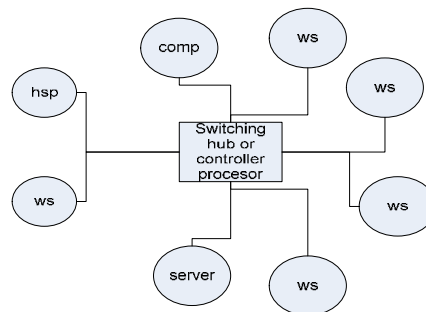
La topología de bus es aquella donde el medio de transmisión es un único medio donde los usuarios se adhieren por medio de una conexión directa, originalmente el medio de transmisión era cable coaxial, en la actualidad el cable coaxial se está reemplazando por el par trenzado.

**Figura 2. Topología de anillo.**



Un anillo es simplemente un bus que está doblado sobre sí mismo. El tráfico de un usuario fluye en una dirección del anillo, esta sería la configuración básica de la topología de anillo por otro lado la otra configuración incluye un segundo anillo donde el tráfico fluye en la dirección contraria. Este concepto de anillo con tráfico contrario mejora la confiabilidad en el caso de que una estación falle o un corte en medio de transmisión del anillo.

**Figura 3. Topología de estrella.**



Una red en estrella como la mostrada tiene en el centro de la misma un elemento de conmutación. Este puede ser un elemento de conmutación de datos, este puede ser un concentrador conmutador. Los usuarios pueden estar conectados, dos a la vez, tres a la vez, todos a la vez, segmentados en familias temporales de usuarios, dependiendo de la configuración del

conmutador en ese momento. En este caso cada usuario esta conectado en general de forma punto a punto.

### **1.7.2 Redes de área extendida (WAN)**

Las redes de área extendida proveen un conectividad sobre una extensión mucho mayor que sus contrapartes las redes de área local. Las velocidades de transferencia de datos en las WAN hasta hace poco eran muy baja. Una de las principales razones es que en muchos casos la conexión a una WAN es a través de una línea de la PSTN ya sea análoga o digital.

Como fue visto con anterioridad las LAN posee capacidades de comunicación dentro de un área y un grupo de usuarios relativamente pequeño, una WAN no solo tiene la capacidad de cubrir el globo sino que incluso puede cubrir el espacio exterior, además pueden tener acceso a ella una gran y diversa cantidad de usuarios (P.Ej. La Internet).

Con estos conceptos en mente ¿ Cuales serian los conceptos claves que deberíamos entender para hacer que este sistema pueda cumplir con nuestras expectativas en servicio? Pensemos un poco y hagamos una lista de requerimientos de una red de datos tales que logren una comunicación fiable. Esta lista tendría más o menos estos requerimientos:

- Los mensajes de datos debe tener una gran probabilidad de llegar a su destino intacto y libre de errores.
- Pueden haber problemas de urgencia. Con esto queremos decir que tan pronto después de la transmisión un mensaje de datos alcanzara su destino.
- El destino debe estar preparado par recibir y entender el mensaje.

En el primer punto, el mensaje debe llegar a su destino, intervienen varios factores por ejemplo ¿Como es que el mensajes es enrutado de manera que llegue a su destino? En la telefonía convencional la señalización realiza esta función. Esta establece un circuito, mantiene la conectividad durante la llamada y luego la corta cuando uno o ambos subscriptores corta la comunicación. Con la comunicación de datos las mismas funciones deben ser llevadas a cabo. Una forma de conectividad es llamada Orientada a Conexión , donde, un circuito en realidad es conectado entre los puntos que desean comunicarse, se transmite la información y por último se corta o desconecta el circuito. La otra forma de transmitir información es por medio de la creación de una trama la cual después de ser creada debe hallar su camino hasta su o sus destinos. A esto en la en el mundo de las comunicaciones se le conoce como servicio no orientado a conexión, en este caso en el encabezado del mensaje se encuentra la información de enrutamiento del mismo, en muchos casos un mensaje esta compuesto de varias tramas, en ese caso cada una de las tramas tiene un campo añadido con la información de dirección de destino y a veces también posee la dirección de remitente u origen. En ambos casos los campos son de 8 bits, expandibles en cantidades similares de 8 bits.

Tres preguntas claves vienen a la mente cuando se analiza esta situación y son las siguientes:

1. ¿Qué parte de la cabecera de la trama puede ser reconocida fácilmente como dirección destino y/o como dirección fuente?
2. ¿Qué capacidad de direccionamiento tiene el campo de dirección? En otras palabras ¿cuantas direcciones diferentes pueden ser acomodadas en un campo de 8 bits?

3. ¿Una vez que un enrutador, un puente inteligente, reconoce los límites del campo de direcciones, como sabe a donde enrutar la trama?

Ahora veamos las respuestas.

¿Qué parte del encabezado de la trama puede ser identificado fácilmente como campo de direcciones tanto de origen como de destino? Una familia de protocolos gobierna la operación de una red particular de datos. Nuestro interés ahora es en los protocolos de capa dos y tres del modelo OSI. Una cosa que puede hacer y hacerlo muy bien un procesador es contar bits, y grupos de 8 bits, los cuales llamamos octetos. Una red en especial utiliza un protocolo en particular de capa dos. Debido a esto el procesador conoce de antemano donde están los límites de una trama, debido a que este está diseñado para cumplir con los requerimientos de este protocolo específico o por lo menos dentro de su programación puede soportarlo. Sin embargo con algunos protocolos de capa dos puede existir el problema de que las tramas son de largos variables. En este caso es obvio que el microprocesador debe ser notificado de esta situación en un campo específico de la trama. Cuando es así la información del largo de la trama está contenida en un subcampo dentro del campo de control de la trama. Así que para responder a esta pregunta 1, el procesador digital sabe de antemano que octeto u octetos contienen la información de la dirección simplemente contando desde el octeto único de comienzo de trama. Esto lo sabe de antemano porque dentro de la programación suministrada al procesador está exactamente como debe manejar el protocolo.

¿Cuál es la capacidad de direccionamiento de un campo de direcciones? Dejaremos que cada dirección consista de una secuencia binaria de 8 o 16 bits. Para una secuencia de 8 bits cuántas combinaciones tenemos la respuesta es  $2^n$  donde  $n$  es el número de bits en una secuencia particular, en



nuestro caso  $n$  es 8 por lo tanto tenemos una cantidad de 256 direcciones disponibles, si se usa un direccionamiento extendido, por ejemplo cuando usamos dos octetos para la dirección destino, a veces el bit menos significativo del primer octeto es reservado para notificar al procesador que espere un segundo octeto dedicado a la dirección de destino. Ahora solo tenemos 7 bits en el primer octeto y ocho del segundo octeto sumando todos los bits tendríamos 15 bits para el direccionamiento y contaríamos con 32,768 direcciones.

¿Cómo hace un enrutador o un nodo conmutador de datos para enrutar hacia una dirección particular? Simple, buscando en una tabla. Ahora esta tabla puede contener algunos valores fijos, o valores que pueden ser actualizados de forma manual o dinámica. Aquí debemos tener en cuenta tres posibles opciones:

- Un nodo / enrutador es añadido o quitado de una red.
- Nuevos patrones de enrutamiento son establecidos; y otros descontinuados y
- Congestión, degradación de ruta/nodo y/o fallas.

Todos estos temas serán tratados con más profundidad en el capítulo 2 en el espacio dedicado a TCP/IP.

En cuanto a la urgencia de un mensaje podemos mencionar lo siguiente. Existen varias familias de mensajes de datos que tienen una importancia baja o ninguna real, en cuanto a la urgencia con que deben ser entregados. Por ejemplo un archivo contable que incluyen la nomina, pueden requerir tiempos de 24 o 48 horas para su entrega. En este caso porque no usar el sistema postal como medio de comunicación, en cambio cuando se verifica

una tarjeta de crédito tiene requerimiento más alto en lo que a velocidad de transacción se refiere. Por lo general la mayoría de las transacciones tiene requerimientos de tiempo de entrega bajo es decir son urgentes.

Una de las razones para la implementación de Frame Relay es baja latencia. Llamemos latencia al tiempo que toma completar una transacción a un mensaje de datos. Existe cuatro causas por las cuales se incrementa el tiempo de transacción y son las siguientes:

1. Retardo de propagación
2. El numero de intercambios de mensajes requeridos para completar una transacción
3. Requerimientos de tiempo y procesamiento y
4. Secundariamente, la calidad del circuito.

Por último, el destino debe estar preparado para recibir y entender un mensaje de datos. Esto no es más que una cuestión de compatibilidad, el receptor del mensaje debe ser compatible con el transmisor y nodos intermedios. No podemos tener un extremo transmitiendo en ASCII y en el otro un receptor que solo entienda EDCDIC. Esta compatibilidad puede extenderse a través de la siete capas del modelo OSI. Por ejemplo, frame relay esta basado solamente en las capas 1y2 del modelo OSI, y es responsabilidad del usuario proveer la compatibilidad necesaria de las capas superiores. Ahora que hemos visto los puntos principales de la comunicación a través de una WAN veremos alguna forma de transmisión de este tipo de redes.

#### **1.7.2.1 Transmisión de datos en redes WAN.**

Dado que cualquier usuario puede solicitar un acceso a las redes que operan las compañías telefónicas, a éstas se las denomina redes públicas de

datos (PDN, *Public Data Networks*). Cuando se desea interconectar computadoras o redes locales ubicadas a cierta distancia es preciso normalmente utilizar los servicios de alguna de esas redes públicas. Dichos servicios pueden clasificarse de acuerdo con el tipo de conexión que ofrecen, permanente o temporal, y con el tipo de circuito, real o virtual.

**Líneas dedicadas** La solución mas simple para una red es el circuito real permanente, constituido por lo que se conoce como líneas dedicadas o líneas alquiladas (*leased lines* en inglés); está formado por un enlace punto a punto permanente entre los computadoras o enrutadores que se desean unir. Una línea dedicada es únicamente un medio de transmisión de datos a nivel físico, todos los protocolos de niveles superiores han de ser suministrados por el usuario. Normalmente no es posible contratar una línea dedicada de una velocidad arbitraria, existen unas velocidades prefijadas que son las que suelen ofrecer las compañías telefónicas y que tienen su origen en la propia naturaleza del sistema telefónico. El precio de una línea dedicada es una cuota fija mensual que depende de la velocidad y de la distancia entre los dos puntos que se unen. La cuota es independiente del uso (corresponde por tanto con lo que se conoce como 'tarifa plana').

En las líneas dedicadas la capacidad contratada está reservada de forma permanente en todo el trayecto. Su costo es elevado y por tanto su instalación generalmente sólo se justifica cuando el uso es elevado (al menos tres o cuatro horas al día). Por este motivo las líneas dedicadas no suelen utilizarse en casos en que se necesita una conexión esporádica, por ejemplo una oficina que requiere conectarse unos minutos al final del día para transferir unos archivos, o un usuario doméstico que se conecta a Internet en los ratos de ocio.

**Conmutación de circuitos.** La conmutación de circuitos supone una utilización más óptima de los recursos que las líneas dedicadas, ya que la conexión extremo a extremo sólo se establece durante el tiempo necesario. Para la transmisión de datos mediante conmutación de circuitos se utiliza la misma red que para la transmisión de la voz, mediante módems o adaptadores apropiados. Genéricamente se la denomina Red Telefónica Conmutada (RTC) o PSTN (Public Switched Telephone Network) y comprende en realidad tres redes diferentes: la red de telefonía básica (RTB) también llamada POTS (Plain Old Telephone Service); Está formada por las líneas analógicas tradicionales y por tanto requiere el uso de módems; la máxima velocidad que puede obtenerse en este tipo de enlaces es de 33.6 Kb/s, salvo el caso en que la transmisión se origine en un acceso RDSI, en cuyo caso puede obtenerse una velocidad máxima de 56 Kb/s.

La Red Digital de Servicios Integrados (RDSI) también llamada ISDN (Integrated Services Digital Network). Está formada por enlaces digitales hasta el bucle de abonado, por lo que el circuito es digital de extremo a extremo. La velocidad por circuito (también llamado canal) es de 64 Kb/s, pudiendo con relativa facilidad agregarse varios canales en una misma comunicación para obtener mayor ancho de banda.

Dado que hasta fechas recientes el único sistema de RTC era la RTB a menudo se utilizan ambos términos indistintamente para indicar la red telefónica analógica. Para evitar confusiones conviene usar el término RTB al referirse a la red telefónica analógica, y reservar el término RTC para referirnos al conjunto de todas las redes conmutadas existentes. En el caso de la RTC cualquier par de usuarios puede comunicar entre sí siempre que conozca su dirección o número de teléfono, por lo que podemos ver la RTC como una gran nube a la

que se conectan multitud de usuarios. Una vez establecido un circuito entre dos abonados la función que desempeña para los protocolos de nivel superior es equivalente a la de una línea dedicada.

Es posible la interconexión entre computadoras de redes diferentes (RDSI, RTB o GSM); en cuyo caso la velocidad de transmisión será igual a la más lenta de las conexiones implicadas; en algunos casos puede ser necesario disponer de equipos específicos o contratar servicios especiales.

**Conmutación de paquetes.** Con la conmutación de circuitos hemos avanzado en el aprovechamiento de la infraestructura. Sin embargo nos encontramos aún con tres inconvenientes: En ocasiones no podremos establecer la conexión por no haber circuitos libres, salvo que contratemos un número de circuitos igual al máximo número posible de conexiones simultáneas, lo cual sería muy costoso. Que un circuito se esté utilizando no garantiza que se esté aprovechando el ancho de banda que tiene asignado. Para evitar estos inconvenientes se crearon redes en las que el usuario puede mantener una única conexión física a la red, y sobre ella varios circuitos virtuales con equipos remotos. De esta forma podemos dotar a nuestra computadora central de varios circuitos virtuales, con lo que siempre va a encontrar un circuito libre sobre el cual establecer la conexión. Al mantener un solo enlace físico el costo de las interfaces, módems, etc., es fijo e independiente del número de circuitos virtuales utilizados. Lógicamente al tener el computadora central que atender a todas las conexiones por el mismo enlace físico sería conveniente (aunque no necesario) incrementar la velocidad de este. Como previsiblemente muchas oficinas querrán conectar más o menos a la misma hora sería conveniente ampliar el enlace del servidor para evitar congestión en horas pico.

Para poder definir circuitos virtuales es preciso disponer de equipos inteligentes en la red que puedan hacer la distribución de los paquetes en función de su destino. Por esto a las redes que permiten crear circuitos virtuales se las denomina redes de conmutación de paquetes, y en cierto sentido podemos considerarlas como la evolución de las redes de conmutación de circuitos. Existen dos tipos de redes de conmutación de paquetes, según ofrezcan servicios orientados a conexión o no orientados a conexión (envío de datagramas). La primera red de conmutación de paquetes que existió fue ARPAnet, pero como no era orientada a conexión no se adaptaba bien a un servicio de compañía telefónica. Para facilitar la facturación las redes públicas de conmutación de paquetes suelen ofrecer servicios orientados a conexión en el nivel de red. Actualmente hay tres tipos de redes públicas de conmutación de paquetes orientadas a conexión estandarizadas: X.25, *Frame Relay* y ATM. Las tres representan implementaciones bastante completas de los tres primeros niveles del Modelo de Referencia OSI, y tienen muchos puntos en común.

La subred de una red de conmutación de paquetes se constituye mediante conmutadores unidos entre sí por líneas dedicadas. La distribución de los conmutadores y la forma como éstos se interconectan, es decir la topología de la red, es algo que decide el proveedor del servicio y que fija la carga máxima que la red podrá soportar en lo que se refiere a tráfico entre conmutadores; la topología fija también la fiabilidad de la red, es decir cuan resistente será a fallos; por ejemplo una red mallada será muy fiable y tendrá una gran disponibilidad, ya que en caso de avería de un enlace o conmutador será fácil encontrar un camino alternativo. En X.25, *Frame Relay* y ATM existe el concepto de circuito virtual (VC), que puede ser de dos tipos: conmutado o SVC (*Switched Virtual Circuit*) y permanente o PVC (*Permanent Virtual Circuit*).

El conmutado se establece y termina a petición del usuario, mientras que el permanente tiene que ser definido por el proveedor del servicio, mediante configuración en los conmutadores a los que se conectan los equipos implicados, normalmente mediante modificación contractual con el cliente. En cierto modo podemos considerar los PVCs como 'líneas dedicadas virtuales' mientras que los SVCs son como conexiones RTC 'virtuales'.

## 1.8 Elementos de interconexión

Una red puede ser tan simple como dos usuarios compartiendo información a través de un *diskette* o tan compleja como la Internet que tenemos hoy. La Internet esta constituida por miles de redes interconectadas a través de elementos llamados concentradores o repetidores (hub), puentes, enrutadores y conmutadores. Estos elementos son los bloques de construcción con los cuales se forman las redes y cada uno realiza una función específica en el proceso de entregar la información que fluye en la red, existen algunos puntos que deben ser considerados para decidir cual de los elementos anteriormente mencionados se adecua mejor a la implementación deseada y son los siguientes:

- **La complejidad de la aplicación.** Si los requerimientos solamente es la extensión de la red para acomodar más usuarios, entonces un puente dará la talla para la aplicación.
- **Los requerimientos de desempeño.** Con el advenimiento de las aplicaciones de multimedia, más ancho de banda es requerido para hacer estas funciones disponibles para los usuarios. En este caso un

Conmutador sería una mejor opción que un concentrador para construir este tipo de red.

- **Requerimientos específicos de un negocio o empresa.** Algunas veces, una necesidad específica requiere un control más granular de quien puede acceder a cierta información. En este tipo de situación un enrutador puede ser requerido para desempeñar un control más sofisticado del flujo de información.
- **Costo y operación.** Algunos de los elementos descritos anteriormente necesitan cierto nivel de experiencia para poderlos operar, por ejemplo un puente es mucho más sencillo de operar que un enrutador. Por último, el costo es un criterio importante de decisión. Cuando todos los elementos pueden hacer el trabajo, el que tenga menor costo usualmente es el que será seleccionado

Los elementos de conexión funcionan en diferentes capas del modelo OSI, y es importante saber a que nivel trabajan para poder hacer la decisión de su uso.

### 1.8.1 Concentrador (HUB)

Un concentrador es un elemento de conexión, al cual todas las estaciones de trabajo están físicamente conectadas, así todas ellas están agrupadas dentro de un dominio común denominado segmento de red.

Un concentrador funciona a nivel de la capa física del modelo OSI, este meramente regenera las señales eléctricas que produce una estación de trabajo, y es conocido también como repetidor. Es un elemento compartido, lo que significa que si todos los usuarios están conectados a un concentrador



de 10Mbps, entonces todos los usuarios comparten el mismo ancho de banda de 10Mbps. Con la consecuencia de que entre más usuarios sean conectados en el mismo, el ancho de banda promedio efectivo tiende a bajar. El número de concentradores que se pueden usar es también determinado por la tecnología escogida.

### **1.8.2 Puentes**

Un puente es un elemento de conectividad que funciona en la capa de enlace del modelo OSI. La tarea primaria de un puente es interconectar dos segmentos de red para que puedan intercambiar información entre ellos.

Un puente básicamente guarda un paquete proveniente de un puerto, y cuando le es requerido, lo envía a través de otro puerto, por lo tanto se puede decir que es un elemento de Guarda y envía (*Store and Forward*). Cuando un puente envía información, este solo inspecciona dentro de un paquete la información de la capa de enlace. Así un puente es más eficiente que un enrutador que es un elemento de capa tres. Las razones para usar un puente puede ser cualquiera de las siguientes:

- Para acomodar mas usuarios en una red En redes como token ring solo permiten 254 clientes dentro de un segmento de red, y cualquier ordenador adicional por fuerza tendría que estar en otro segmento de red.
- Para mejorar el desempeño de una red. Un puente puede ser utilizado para separar una red en dos segmentos, así la interferencia, como las

colisiones, pueden ser contenidas dentro de un cierto grupo de usuarios, permitiendo al resto comunicarse entre ellos sin problemas.

- Para extender la longitud de una red

Tecnologías como Ethernet especifican ciertas distancias máximas para una LAN. Un puente es una excelente herramienta para extender la distancia así más estaciones pueden ser conectadas.

- Para mejorar la seguridad

Con un puente se puede implementar lo que es llamado un filtro de MAC, esto es, permitir selectivamente que solamente tramas provenientes de ciertas estaciones puedan pasar a través de él en ambos sentidos. De esta manera le permite al administrador de la red controlar acceso a cierta información o usuarios.

- Para conectar redes de diferentes tecnologías

Debido a que hay una variedad de razones para usar un puente, los puentes son clasificados en varias categorías por las funciones que estos desempeñan:

- **Puente transparente.** Un puente transparente es aquel que envía tráfico entre las redes LAN adyacentes y es desconocida por las estaciones. La existencia de este, de allí, es transparente. Un puente transparente construye una tabla de direcciones MAC de las estaciones que le sirve para decidir si envía un paquete. Cuando el puente recibe un paquete, este revisa su tabla para ver la dirección destino del paquete, si este está en el mismo segmento de LAN de donde viene el paquete entonces este no es reenviado, sin embargo si

la dirección es para un segmento distinto al de donde fue generado entonces si se reenvía , si la dirección no esta en la tabla entonces, paquete es reenviado a todas las interfaces con excepción de donde provino el paquete. Este tipo de puente se utiliza en las redes Ethernet.

- **Puente de fuente enrutada.** Un puente de fuente enrutada es usada en las redes de Token Ring donde el la estación que envía la información decide el camino a tomar para llegar a su destino. Antes de enviar información alguna, una estación debe decidir el camino que la información debe tomar. La estación hace esto enviando lo que se conoce como una trama de exploración y forma el camino o ruta en base a la información recibida del destino.
- **Puente transparente de fuente enrutada.** Este tipo de puente es aquel que hace el enrutamiento de fuente, cuando tramas con información de enrutamiento es recibida y hace de puente transparente cuando las tramas no poseen este tipo de información.. Este puente reenvía las tramas de forma transparente sin ninguna conversión a la interfaz de salida, mientras las que poseen información de enrutamiento son restringidas al dominio, de esta forma los paquetes si información de ruteo pueden alcanzar otro puente de fuente enrutada y LAN puenteadas de forma transparente, mientras la tramas con enrutamiento de fuente son limitadas solamente al fuente con fuente enrutada y la LAN con enrutamiento de fuente.

Otra forma de clasificar a los puentes es en locales y remotos. Mientras los puentes locales conectan dos segmentos de red dentro del mismo edificio los puentes remotos funcionan en pares y conectan segmentos de redes distantes.

### 1.8.3 Conmutador.

Un conmutador funciona al mismo nivel de capa con respecto al modelo de referencia OSI que un puente de hecho un conmutador puede ser considerado como un puente de varios puertos, mientras un puente maneja tráfico entre dos segmentos de red, el conmutador posee muchos puertos, y maneja el tráfico entre esos puertos.

La gran diferencia entre un puente y un conmutador es que el puente realiza sus tareas a través de software, mientras que el conmutador realiza esta función a través de implementaciones de hardware. Debido a esto un conmutador es más eficiente que un puente, y usualmente cuesta más. Mientras que la generación antigua de conmutadores solamente pueden trabajar en el modo de guardar y enviar, existen algunos conmutadores que ofrecen modos diferentes de operación por ejemplo existe un método en cual un paquete empieza a ser enviado sin haber recibido el paquete completo esto mejora grandemente el rendimiento del conmutador. Un conmutador que posee la capacidad de procesamiento, para manejar el total del ancho de banda requerido por todos los puertos es considerado como no obstructivo que es un factor importante en el proceso de escoger un conmutador.

Los conmutadores son implementados para particionar un segmento de red en segmentos más pequeños, así el tráfico de difusión puede ser reducido y más clientes pueden comunicarse al mismo tiempo. Esto es llamado micro segmentación, e incrementa el ancho de banda de la red en general sin hacer un gran cambio en la estructura.

### **1.8.3.1 Lan virtual**

Con las necesidades del usuario por ancho de banda incrementándose cada día, se requiere de más segmentación y los segmentos de red en los puertos del conmutador se hacen más pequeños hasta que solamente pueden alojar a un usuario. Debido a esto más funciones deben ser añadidas al conmutador una de las cuales es llamada LAN virtual (VLAN). Esta función consiste en un agrupamiento lógico de estaciones que comparten las mismas características. En un principio, las estaciones eran agrupadas por puertos en el conmutador, esto es, las estaciones conectados a ciertos puertos pertenecían al mismo grupo. Esto es llamado una VLAN basada en puertos, este tipo de arreglo es estático debido a que el administrador debe planificar el modo de agrupar las estaciones programarlo en el conmutador y después ponerlo en funcionamiento. Después se mejoro la forma de agrupamiento así los conmutadores pueden hacerlo no por el puerto donde están conectados sino por que protocolo de red utilizan, tales como IP o IPX esto es llamado VLAN de protocolo o PVLAN.

### **1.8.4 Enrutador**

Como se menciona anteriormente, un enrutador funciona en la capa tres del modelo OSI, la capa de red. Un enrutador inspecciona la información del paquete pertinente a la capa de red y reenvia el paquete basado en ciertas reglas, debido a que este elemento de red necesita inspeccionar más información de un paquete es normal que deba poseer una capacidad de procesamiento mayor al de cualquiera de los otros elementos de red antes mencionados aunque diferentes en la forma en que inspeccionan el paquete

el enrutador y el puente obtienen el mismo objetivo: el reenviar información a un destino designado. Un enrutador es un elemento muy importante en una red IP, esto debido a que es elemento de enlace entre diferentes grupos de redes llamados subredes IP. Todos los clientes en una red IP tienen un identificador único llamada dirección IP, a esta dirección la forman dos partes la primera llamada número de red y el segundo es el número de cliente, los clientes que están en diferentes subredes solamente pueden ser conectados a elementos intermediarios, el enrutador, antes de poderse comunicar entre sí. En este caso el enrutador es llamado la puerta de salida por defecto.

La razón por la cual usar un enrutador son las mismas por las cuales se usa un puente, debido a que el enrutador inspecciona más información dentro de un paquete que un puente, este posee cualidades más poderosas en el sentido de tomar decisión basadas en la información de red y protocolo tales como la dirección IP. Con la introducción de nuevos y más potentes procesadores un enrutador puede inspeccionar un paquete más allá de la capa de red, este tipo de enrutadores pueden desempeñar funciones tales como bloquear la capacidad de ciertos usuarios a utilizar ciertas funciones tales como FTP o TELNET. Cuando un enrutador realiza esta función se dice que está haciendo filtrado.

Un enrutador también es utilizado para conectar oficinas remotas a oficinas centrales, en ese escenario, usualmente el enrutador colocado en la oficina remota tiene un puerto que conecta a la LAN local, y uno que se conecta con un servicio de banda ancha, tal como una conexión ISDN. En la oficina central por lo general existe un enrutador de más alta capacidad para recibir los enlaces de varios de los enrutadores remotos.

## 1.9 Factores que afectan el diseño de una red

El diseño de una red es más que meramente planear usar el último grito de la moda en lo que corresponde a tecnología. Un buen diseño de red toma en cuenta muchos factores como los siguientes:

- **Tamaño** Al final el tamaño si importa, el hecho de diseñar una LAN para una pequeña oficina con unos cuantos usuarios, es diferente que hacer una para una compañía grande con miles de de usuarios. Al construir una LAN pequeña un diseño plano es usualmente utilizado, donde todos los elementos de conexión estarían conectados entres sí. Para una compañía o empresa grande un diseño jerárquico seria la mejor aproximación al problema
- **Geografía.** La localización geográfica de los sitios que necesitan estar conectados son importantes dentro del diseño de una red , el proceso de selección para elegir la tecnología y equipo correctos para una conexión remota es un proceso delicado, especialmente los que son de naturaleza lejana. Las tarifas, la mano de obra local, calidad de servicio de los proveedores de servicios son criterios importantes.
- **Tipos de aplicaciones.** Los tipos de aplicaciones utilizadas determinan el ancho de banda requerido. Mientras que una transacción basada en texto puede requerir unos cuantos Kbps de ancho de banda, un archivo de ayuda con videos con explicaciones puede requerir unos 1.5 Mbps de ancho de banda.
- **Tolerancia a fallas.** En una red de “misión critica”, el desempeño puede no ser un criterio de tanto peso mas no así la tolerancia a fallas. De este tipo de red se espera un servicio ininterrumpido y la

redundancia es requerida tanto a nivel de hardware como a nivel de servicio. En este aspecto muchas funciones deben ser implementadas, tales como redundancia de *hardware*, capacidades de reenrutamiento etc.

- **Estrategia.** Un factor importante es por su puesto una estrategia de red. Sin un plano, uno puede acabar con una red múltiproducos y múltiprotocolos que es difícil de manejar y expandir. Se ha estimado que el 70% del costo de tener en propiedad una red es mantenerla funcionando..
- **Costos.** Una de los elementos que hacen factible un proyecto es el costo. Muchas veces los encargados de red han tenido que desechar una solución técnicamente elegante por un diseño menos sofisticado que a la larga hace el mismo trabajo y a un menor costo.
- **Estándares.** El hecho de escoger equipo que se apega a los estándares es una regla importante a seguir. Los estándares nos dan la habilidad de implantar tecnología reconocida por la industria que es soportada por la mayoría de distribuidores. Esto provee flexibilidad en la elección de equipo, y permite al administrador de la red elegir la solución más efectiva tanto en costo como en funcionalidad.



## 2 PROTOCOLOS DE RED

### 2.1 Introducción

Para obtener el máximo de nuestras redes, ciertas reglas operativas, procedimientos, e interfaces deben ser establecidos. Una red de datos es una gran inversión y nuestro deseo es obtener el mejor resultado de esta inversión. Una forma para optimizar este resultado es la selección de un protocolo operacional. Debemos argumentar que existen múltiples factores involucrados, todos interactuando entre ellos. Entre estos factores están las necesidades que deben ser cumplidas, topología de red y arquitectura, el medio de transmisión seleccionado, el hardware y software que se utiliza para la comunicación y administración de la red, en este capítulo nos enfocaremos en los protocolos operacionales.

En el diccionario de la IEEE la definición de protocolo es la siguiente “un conjunto de reglas que gobiernan unidades funcionales para lograr la comunicación”. Añadiremos interfaces a esta definición para hacerla más general.

#### 2.1.1 Funciones básicas de un protocolo

Hay un número de funciones básicas que un protocolo debe cumplir. Típicamente entre estas están:

- Segmentación y reconstrucción

- Encapsulación
- Control de conexión
- Entrega ordenada
- Control de flujo; y
- Control de error

A continuación una breve explicación de cada una de estas funciones.

- **Segmentación y reconstrucción.** Con segmentación nos referimos a la acción de separar el mensaje de datos en bloques, paquetes, o tramas con un tamaño definido. Cual de los términos se usa depende de la semántica del sistema. Incluso existe un nuevo término denominado celda, usado en ATM y otros sistemas digitales. Reconstrucción es el procedimiento inverso al de Segmentación, debido a que este procedimiento consiste en volver a poner en su posición original los bloques, tramas, o paquetes. El dispositivo que se encarga de hacer la segmentación y reconstrucción en una red de paquetes es llamado PAD (Packet Assembler Disassembler).
- **Encapsulación.** Esta es la acción de añadir un encabezado e información de control antes del paquete e información de paridad, la cual generalmente es puesta después del paquete. Existen tres etapas del control de conexión:
  1. Establecimiento de conexión
  2. Transferencia de datos; y
  3. Finalización de conexión

Algunos de los protocolos más sofisticados también poseen interrupción de conexión y capacidades de recuperación para poder manejar errores y otro tipo de interrupciones

- **Entrega ordenada.** Muy a menudo a los paquetes, tramas, o bloques se les asigna números correlativos para asegurar una entrega ordenada de la información en el lugar de destino. En una red grande con muchos nodos y posibles rutas a un mismo destino, especialmente cuando es operada en modo de transmisión por paquetes, los paquetes pueden llegar de una forma desordenada. Con un plan de numeración único usando una secuencia de numeración simple, el hecho de reordenar un mensaje grande en la estación destino es una tarea simple
- **Control de flujo.** Esto se refiere a la administración del flujo de información de la fuente al destino de la misma de manera que las memorias de buffer no se rebalsen, pero manteniendo la capacidad máxima de transporte de todos los elementos que intervienen en la transferencia de datos.
- **Control de error.** Esta es una técnica que permite la recuperación de paquetes perdidos o con errores, existen cuatro funciones que posiblemente estén presentes dentro del proceso del control de error.

1 Numeración de paquetes

2 Octetos incompletos (una secuencia de bits que nos tienen el número adecuado de bits en este caso 8 bits).

3 Detección de error. Usualmente incluye la funcionalidad de corrección de errores

4 Acuse de recibo o confirmación de recibo de una, varias o una serie de paquetes. Esto puede conseguirse devolviendo al

remitente el número de secuencia de envío como una secuencia de recibo.

## 2.2 Protocolos de redes LAN

En este contexto un protocolo es un medio para que todos los usuarios tengan acceso a la LAN de forma equitativa. El acceso puede ser de forma aleatoria o de forma controlada. Hay que tomar en cuenta que el acceso de los usuarios a la LAN es impredecible, y por eso la capacidad de transmisión de la LAN debe ser de forma dinámica en respuesta a esta característica.

Los protocolos de las LAN solo utilizan las capas 1 y 2 del modelo OSI, la capa física y la capa de enlace respectivamente. La capa de enlace se puede subdividir en dos capas más: Control lógico de enlace y control de acceso al medio (MAC). La principal función de la capa 3 del modelo de referencia OSI, llamada, conmutación o red, no son necesarios en este tipo de red. Algunas de las funciones remanentes de la capa 3, que son necesarias son incluidas en la capa 2, las dos subcapas de la capa 2 cumplen cuatro funciones que son:

1. Proveer uno o más puntos de acceso para un servicio (SAP). Un SAP es una interfaz lógica entre dos capas adyacentes.
2. Antes de la transmisión, ensamblar los datos a transmitir dentro de una trama con campos de dirección y de detección de errores.
3. En recepción, desensamblar la trama y realizar el reconocimiento de la dirección y la detección de errores.
4. Controlar las comunicaciones sobre el enlace.

5. Todos los elementos de la primera función y todo lo que tenga que ver con ella son controlados mediante la capa de control lógico de enlace. Las últimas tres de las funciones son manejadas mediante la capa de MAC.

### 2.2.1 Técnica de acceso CSMA Y CSMA/CD

Detección de portadora acceso múltiple (CSMA) es una técnica de acceso a las LAN que típicamente se le ha llamado “escuchar antes de transmitir”, esto nos da una idea del funcionamiento del control del mecanismo. Si el usuario 2 esta transmitiendo, el usuario 1 y todos los demás usuarios “escuchan” que el medio esta ocupado y se abstiene de usarlo. Realmente, cuando un acceso con tráfico censa que el medio esta ocupado se abstiene de transmitir por un periodo de tiempo y luego trata de nuevo. ¿Como se controla este tiempo antes de la retransmisión? Existen tres tipos de control comúnmente usados, estos son llamados algoritmos de persistencia los cuales explicaremos brevemente.

- No persistente. La estación de acceso espera un periodo de tiempo aleatorio y luego intenta la retransmisión.
- 1-Persistente .La estación de acceso sensa el canal hasta que esta desocupado y entonces intenta la retransmisión.
- p-Persistente. La estación de acceso continua sensando el medio hasta que esta desocupado y entonces transmite con una probabilidad preasignada  $p$ . De otra forma se abstiene un tiempo determinado de tiempo después del cual vuelve a retransmitir con una probabilidad  $p$  continúa absteniéndose con una probabilidad  $1-p$ .

La selección del algoritmo depende en la eficiencia deseada en el uso del medio de transmisión y la complejidad del algoritmo y el impacto en los diferentes programas de las unidades de procesamiento de la LAN. Con el algoritmo no persistente, las colisiones son controladas efectivamente porque las dos estaciones que compiten por el medio de transmisión se abstienen de transmitir, muy probablemente con diferentes tiempos de espera. El resultado es la pérdida de tiempo entre transmisiones. El algoritmo 1-Persistente es más eficiente permitiendo a las estaciones transmitir inmediatamente después de transmisión. Sin embargo, si más de dos estaciones compiten por el acceso, la colisión está casi asegurada. También debe ser notado que en CSMA, después de que una estación transmite un mensaje, esta debe esperar por la respuesta o la confirmación de la estación destino. Aquí debemos tener en cuenta el atraso de un viaje de ida y vuelta y además que la estación destino debe competir por el derecho de transmisión en el medio. Otro factor importante es que las colisiones pueden ocurrir solamente cuando más de un usuario empieza su transmisión dentro del tiempo de propagación por eso CSMA es un control de acceso para sistemas de transmisión de paquetes donde el tiempo de duración del paquete es mucho más grande que el tiempo de propagación en el canal.

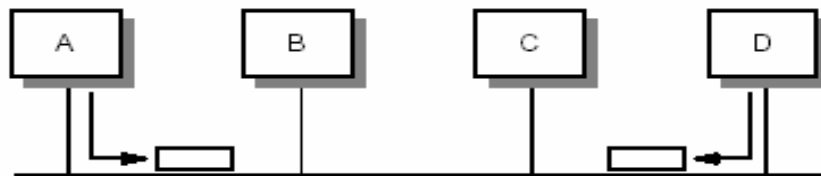
La ineficiencia de CSMA tiene su origen en el hecho de que las colisiones no son detectadas sino hasta que las dos estaciones que transmitieron a la vez terminan su transmisión. En cambio con CSMA/CD que posee detección de colisiones estas pueden ser detectadas en una fase más temprana de la transmisión y esta puede ser abortada, como resultado de esto el tiempo que el canal está inactivo puede acortarse. A este tipo de sistema se le denomina “escuchar mientras transmite”.

### 2.2.2 CSMA/CD (Ethernet /IEEE802.3)

Hoy en día la tecnología más popular en las red LAN es la tecnología Ethernet, es popular debido a que fácil de implementar, y el costo de propiedad es bastante bajo en comparación con otras tecnologías. Además es fácil de monitorear y los productos para este tipo de protocolo son bastante comunes y disponibles.

La tecnología fue inventada por Xerox en 1970 y fue conocido como *Ethernet* V.1 después fue modificado con el consorcio de Intel y Xerox y el nuevo estándar fue llamado *Ethernet* (DIX) V2. Después fue modificado por la IEEE, para ser aceptado como estándar internacional, con modificaciones menores así fue como el IEEE 802.3 fue introducido. El *Ethernet* para LAN es un ejemplo de detección de portadora para acceso múltiple con detección de colisiones, esto es, varios miembros de la misma red transmiten información al azar y retransmiten cuando existe una colisión. Las redes CSMA/CD es el clásico ejemplo de una red broadcast porque todas las estaciones “ven” toda la información que es transmitida en la red.

**Figura 4. Ejemplo de una red CSMA/CD.**



Fuente: *IP Network Design, Segunda edición. IBM.*

En la figura 4 cuando una estación quiere transmitir en la red de datos, primero escucha para saber si alguna otra estación esta transmitiendo en la red. Si la red esta ocupada, espera hasta que la transmisión se detenga para mandar su información en unidades llamadas tramas. Debido a la tamaño de la red la comunicación de un punto a otro dentro de la red puede tomar cierto tiempo uno de los puntos intermedios o inclusive uno de los puntos que intentan comunicarse pueden pensar que el canal esta vacío y transmitir, y es allí donde se produce una colisión y es detectada por todas las estaciones. Cuando una colisión ocurre las dos estaciones involucradas en la colisión dejan de transmitir y esperan un tiempo dado por alguno de los algoritmos de espera antes descritos y luego vuelven a retransmitir sus datos. Como se puede ver la posibilidad de colisión depende de las siguientes condiciones:

- El número de estaciones en la red. Entre más estaciones más posibilidades de colisiones existen.
- El tamaño de la red. Entre *Emás* grande más posibilidades existen de una colisión.
- El largo del paquete. Un paquete más largo requiere un tiempo más grande para ser transmitido, lo cual incrementa las posibilidades de una colisión. El tamaño de la trama en una red *Ethernet* el rango de 64 a 1516 bytes.

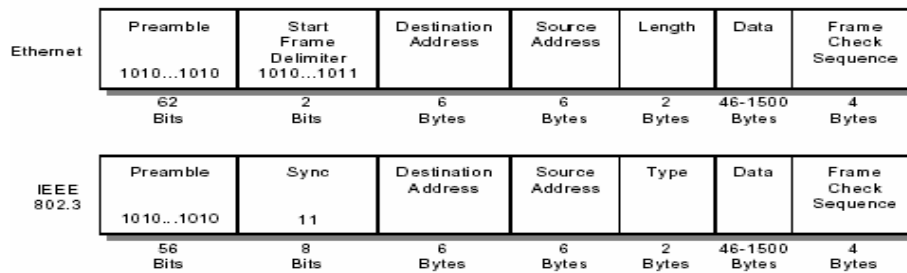
Por lo tanto uno de los aspectos importantes en el diseño de una Lan *Ethernet* es asegura un número adecuado de estaciones por segmento de red, para que el tamaño de la red no exceda lo que el estándar especifica, y que el tamaño de paquete usado también sea el correcto. Mientras que el uso de una trama grande implica que el número de estas para transmitir un paquete es más pequeño, esto aumenta las posibilidades de colisión entre paquetes, por otro lado si se usa un paquete demasiado pequeño esto hace la



posibilidad de una colisión más pequeña pero toma muchas más tramas para poder enviar una misma información.

Fue mencionado que los estándares del *Ethernet* y el IEEE 802.3 no son los mismos. La diferencia está en el formato, lo que significa que las estaciones configuradas con Ethernet no serán capaces de comunicarse con estaciones configuradas con IEEE 802.3 la diferencia entre los formatos es como sigue:

**Figura 5. Tramas de los estándares IEEE 802.3 y CSMA/CD.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Para implementar una red Ethernet, los administradores deben apegarse a ciertas reglas, que están relacionadas con el tipo de medio que este usando.

Ethernet puede ser implementado usando cable coaxial (10 Base 5 o 10Base2), fibra optica(10base F) o UTP categoría 3(10baseT). Esto diferentes medios imponen diferentes restricciones y es importante saberlas. Además Ethernet generalmente sigue la regla 5-4-3. Esto es, en un dominio simple de colisión, solo puede haber cinco segmentos físicos, conectados por 4 repetidores. Ningún par de estaciones pueden estar separadas por más de

tres segmentos. Los otros dos segmentos deben ser segmentos de enlace, esto es, sin ninguna estación ligada a ellos.

A pesar de que se pensó de que la tecnología Ethernet iba a ser reemplazada por tecnologías más modernas sus productos han evolucionado, por ejemplo de la tradicional 10Mbps se evoluciona a la de 100Mbps o Fast Ethernet IEEE 802.3u (Ethernet rápida) La trama utilizada en la FE es la misma que se utilizaba en la Ethernet tradicional por eso resulta fácil de la tecnología antigua a esta nueva tecnología debido a este incremento de velocidad el tamaño de la red debe ser reducido para evitar que la detección de colisiones sea ineficiente. La Gigabit Ethernet o IEEE 802.3z, es 10 veces más rápida que la FE, el entramado utilizado sigue siendo el mismo lo que causa que el tamaño de la red de una forma drástica este tipo de red usualmente se conecta con fibra de longitud de onda corta (1000Base Sx) o con fibras de longitud de onda larga (1000 Base Lx) aunque el estándar para UTP (1000base T) existe.

Generalmente se ha convergido en la opinión de que el máximo ancho de banda utilizable por las Lan Ethernet es alrededor de 40% después del cual el efecto de las colisiones es tan grave que la eficiencia empieza a decrecer.

Ethernet es una buena tecnología para construir una red de bajo volumen y que no posea aplicaciones que demanden una gran cantidad de ancho de banda.

Porque posee un control de acceso sencillo a la red, es simple y proporciona una buena eficiencia en el sentido de entrega de información, sin

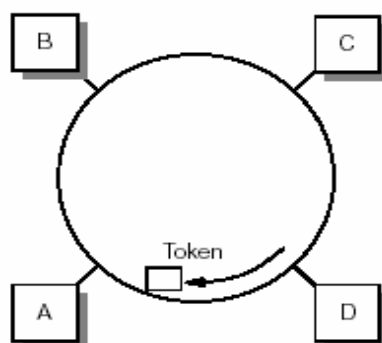
embargo debido a la naturaleza no determinística de las colisiones el tiempo de respuesta en una red de esa naturaleza no puede ser determinado en este caso otro tipo de tecnología debería ser implementado en caso de que fuera necesario conocer este tiempo.

### 2.2.3 *Token Ring* /IEEE 802.5

La tecnología de *Token Ring* (Anillo de Pase) fue inventada por IBM en los setentas es la segunda arquitectura más popular. Soporta velocidades de 1.4 o 16 Mbps. Aunque ya existe una nueva tecnología desarrollada por la IEEE que corre a 100Mbps

Las LAN *token* son claro ejemplo de acceso por medio de un pase, esto es, los miembros de la red pueden transmitir solamente cuando estos tiene en su poder el pase Ya que la transmisión esta regulada por el pase, una red de esta naturaleza no presenta los problemas de colisión de paquetes.

**Figura 6. Topología de anillo.**



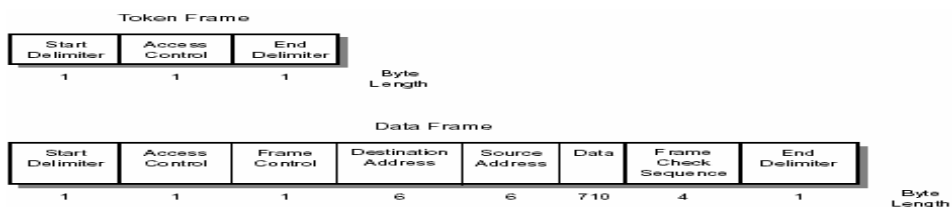
Fuente: *IP Network Design, Segunda edición. IBM.*

Como se muestra en la figura, todas las estaciones están conectadas a manera de un anillo lógico, y el acceso al anillo está controlado por medio de una trama de pase circulante. Cuando la estación A tiene datos que transmitir a la estación D recibe el pase, cambia la información de la trama de control, adhiere la información y la retransmite la trama.

Mientras la trama pasa por la estación B, esa revisa la trama para ver si es para ella, pero como es para D simplemente retransmite la trama y esa acción se repite en la estación C hasta llegar a D. Cuando D recibe la trama, esta copia la información de la trama, ve los bits de reconocimiento de dirección y retransmite la trama modificada en la red de vuelta a A.

Eventualmente A recibe la trama, remueve la información de la misma, y libera una nueva trama de control en el anillo para que otra estación pueda usarlo. El siguiente diagrama muestra los formatos para las tramas de datos y de control o pase.

**Figura 7. Estructura de la trama de Pase y la de información para *Token Ring*.**



Fuente: *IP Network Design, Segunda edición. IBM*

Como se ha descrito, la técnica de pase de control es diferente de la técnica aleatoria de Ethernet, esto hace a la técnica de control de trama de control sea determinística y permita determinar los retardos de la red.

Además de esta diferencia, esta técnica ofrece diagnósticos de la red y auto recuperación tales como:

- Diagnósticos de inserción e inicio de operación del anillo.
- Pruebas de inserción de lóbulos y diagnósticos de falla en los lóbulos en tiempo real.
- Detección de pérdida de señal.
- Monitoreo de las funciones activas y en espera del anillo.
- Detección y reporte de errores de transmisión del anillo.
- Aislamiento de elementos con fallas de manera automáticamente o de forma manual.

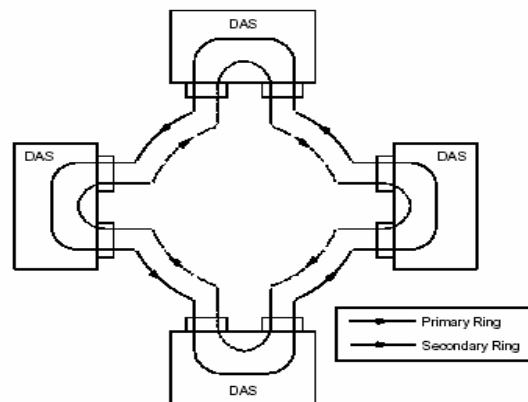
Como era de esperarse los elementos de red con todas estas cualidades resulten siendo más caros que los elementos de Ethernet debido a que cada una de estas funciones están implementada en el micro código de la interfaz.

Este tipo de red es particularmente estable bajo condiciones de mucha carga, el incremento del número de estaciones en la LAN no afecta el desempeño de la red como lo haría con una red Ethernet. Garantiza un acceso justo a todas las estaciones ubicadas en la misma LAN y puede ser equipado con un mecanismo de ocho niveles de priorización. Con propiedades como auto recuperación y auto configuración a nivel eléctrico, las redes de este tipo son las indicadas cuando se busca una red confiable y con tiempos de respuesta predecibles. Redes como los sistemas de manufactura de las fábricas y los sistemas de reservación de las aerolíneas.

## 2.2.4 Interfaz de fibra distribuida (FDDI).

FDDI fue desarrollado a principios de los ochentas diseñado para clientes que requería alta velocidad pero pronto se convirtieron en una alternativa par la implementación de los sistemas centrales de las LAN. De una forma similar a la tecnología de Token Ring esta utiliza una trama de control para la transmisión pero utiliza dos anillos, uno primario y uno secundario, a velocidades de 100Mbps y más. Bajo circunstancias normales solamente se utiliza el anillo principal mientras que el otro esta en espera. FDDI provee de gran flexibilidad en su conectividad y redundancia y ofrece varias maneras de conectar las estaciones, una de las cuales es llamada estación con conexión dual de anillo (DAS).

**Figura 8. Diagrama de conexión de la las interfaces DAS.**

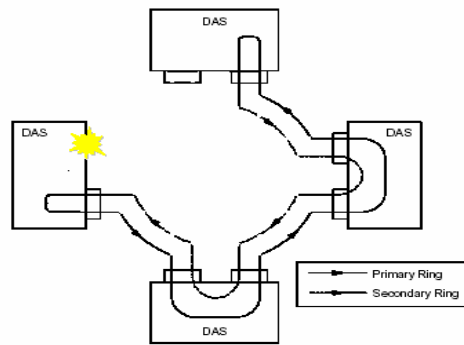


**Fuente:** *IP Network Design, Segunda edición. IBM.*

Todas las estaciones DAS poseen dos puertos disponibles para la conexión a la red como se muestra en la figura 8. En el arreglo anterior, la red consiste en un anillo primario y uno secundario en los cuales los datos fluyen en direcciones contrarias. Bajo condiciones normales, los datos fluyen a través

del anillo primario y el secundario permanece como respaldo. En el caso de una falla de fibra, las dos DAS adyacentes “cierran” sus terminales que están conectadas a las DAS que fallo, ahora la red se convierte en una red de anillo simple y continua operando como se muestra en la figura.

**Figura 9. Falla de una interfaz DAS.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Es fácil de notar la robustez de la configuración de FDDI y apreciar el porque de su uso en redes de gran disponibilidad. Como son de la misma naturaleza que las rede de Token Ring, FDDI ofrece la capacidad de auto recuperación y de seguridad. Debido a que en su mayoría corren sobre cables de fibra óptica, esta no es afectada por eventos electromagnéticos. Debido a su robustez y velocidad, FDDI es el tipo de red preferido para hacer las redes de tráfico principal. Sin embargo con el desarrollo de la tecnología Ethernet de 100Mbps los diseñadores que prefieren ancho de banda en lugar de confiabilidad están migrando sus redes a este tipo de tecnología aún así todavía se pueden hallar este tipo de redes. A los tres tipos de tecnologías vistas hasta ahora se les denomina tecnologías heredadas.

## **2.3 Protocolos de redes WAN.**

En esta parte del capítulo nos dedicaremos a los protocolos y tecnologías de redes WAN la principal diferencia con los protocolos de red LAN es que estos están orientados a una conexión punto a punto mientras que en una LAN los protocolos están orientados a *broadcast*. A pesar de esto comparten algunas características en común que fueron explicadas en el apartado de Funciones Básicas de un Protocolo.

A continuación presentamos las características más importantes de algunos de los protocolos WAN utilizados en la actualidad.

### **2.3.1 Fundamentos de TCP/IP**

Implementado originalmente en los inicios de la década del 70, a experimentado un crecimiento tal que llegado convertirse en la pila de protocolos dominante. Inicialmente diseñado por ARPANET, del departamento de defensa de los Estados Unidos, TCP/IP constituye una de las pocas pilas de protocolos actualmente utilizadas que es completamente independiente del fabricante. Asombrosamente, su desarrollo se ha disparado en tal forma que prácticamente todos los sistemas operativos vigentes hoy reconocen TCP/IP de forma nativa.

### **2.3.2 Puertos y sockets**

Aquí introducimos los conceptos de puerto y socket, los cuales son necesarios para determinar qué proceso local en un cliente dado realmente se



comunica con que proceso, y a cual cliente remoto, usando que protocolo. Si esto suena confuso, consideremos lo siguiente:

- A cada proceso de aplicación es asignado un identificador de proceso, el cual es propenso a ser diferente cada vez que el proceso es iniciado.
- Los identificadores de proceso difieren conforme a la plataforma del sistema operativo en el que están corriendo, debido a esto no son uniformes.
- Un proceso de servidor o servicio puede tener múltiples conexiones a múltiples clientes a la vez, debido a esto los identificadores simples de conexión podrían no ser únicos.

Los conceptos de puerto y socket nos proveen de una herramienta para identificar conexiones de una manera única y uniforme, a la vez que identifica los programas y los clientes que están envueltos en ellas.

### **2.3.2.1 Puertos**

Cada proceso que desea comunicarse con otro proceso se identifica a sí mismo al conjunto de protocolos de TCP/IP por uno o más puertos. Un puerto es un número de 16 bits usado por el protocolo de cliente a cliente para identificar a cuales protocolo de mayor nivel o programa de aplicación debe entregar el mensaje entrante. Existen dos tipos de puertos:

- Bien conocidos: los puertos bien conocidos pertenecen a servidores estándar, por ejemplo Telnet utiliza el puerto 23. La numeración de puertos bien conocidos tiene un rango entre 1 y 1023, hasta el año 1992, el rango entre 256 y 1023 era usado para servidores específicos de UNIX. Así la numeración de los puertos bien conocidos es típicamente es típicamente impar, debido a que los primeros sistemas que usaban el

concepto de puertos requerían pares de puertos conformados por un puerto par y un puerto impar para la operación dúplex. La mayoría de los servidores requieren solamente un puerto con excepción de los servidores de BOOTP, el cual usa dos que son: el 67 y 68. Otro ejemplo es el servidor de FTP que también utiliza dos puertos el 21 y 22.

- Efímeros: los clientes no necesitan de los números de los puertos bien conocidos debido a que ellos inician la comunicación con los servidores y el número de puerto que ellos están usando está contenido en los datagramas de UDP enviados al servidor. A cada proceso de cliente se le asigna un número de puerto mientras el cliente en el que están corriendo lo necesite. La numeración para puertos efímeros tiene valores más grandes que 1023, normalmente en el rango de 1024 a 65,535. Un cliente para utilizar cualquier número asignado a él, mientras la combinación de protocolo de transporte, dirección IP y número de puerto sea única.

La confusión, debida a dos aplicaciones diferentes tratando de usar el mismo puerto en el mismo cliente es evitada mediante la programación de las aplicaciones para que hagan una requisición de un puerto disponible. Debido a esto el número de puerto es asignado dinámicamente.

### **2.3.2.2 Socket**

La interfaz SOCKET es una de varias interfaces de programación de aplicación para los protocolos de comunicación. Diseñada para hacer interfaz genérica de comunicación, las API, fueron introducidas por la 4.2 BSD. Aunque no ha sido estandarizada, se ha convertido en un estándar industrial de facto.

La 4.2 BSD permite dos dominios de comunicación diferentes: espacio Internet y UNIX. La 4.3 BSD ha añadido los protocolos del sistema de redes XEROX (XNS), y la 4.24 BSD añadirá un interfaz extendida para soporte a los protocolos de la ISO.

Consideremos la siguiente terminología:

- Un socket es una forma especial de manejo de archivos, que es usado por un proceso para requerir servicios de red desde el sistema operativo.
- Una dirección de SOCKET es una tríada compuesta de: protocolo, dirección local y proceso local.
- Una conversación es el enlace de comunicación entre dos procesos.
- Una asociación es un conjunto de cinco elementos que especifican a los dos procesos de aplicación que están envueltos en la conexión y consiste de: protocolo, dirección local, proceso local, dirección remota, proceso remoto.
- Una media asociación consiste en los siguientes elementos: protocolo, dirección local, proceso local o protocolo, división remota, proceso remoto. Lo cual especifica cada mitad de la conexión.
- La media asociación es también llamada socket o una dirección de transporte esto es, un socket es un punto final de una comunicación que puede ser nombrada y direccionada en la red.

Dos procesos se comunicaron vías sockets. El modelo de sockets provee a un proceso de una conexión fluida full dúplex a otro proceso, la aplicación no debe preocuparse de manejo de este conexión el manejo es proporcionado por TCP.

El protocolo TCP usa el mismo principio de puertos que protocolo UDP para proveer mutiplexión. Al igual que UDP, TCP utiliza ambas clases de puertos bien conocidos y efímeros cada lado de una conexión TCP tiene un socket que puede ser identificado por medio de la tríada de datos siguientes TCP, dirección IP y número de puerto. Si los dos procesos se están comunicando sobre TCP, ellos tienen una conexión lógica que es identificable de manera única por los dos sockets involucrados en la comunicación. Los procesos de servidores son capaces de manejar a múltiples conversaciones a través de un solo puerto.

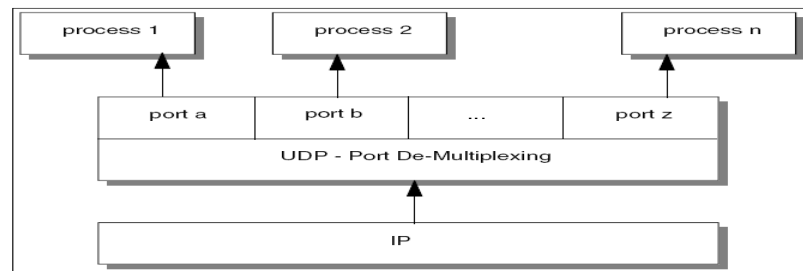
### **2.3.3 Protocolo de datagramas de usuario**

El protocolo de datagramas de usuario el protocolo de transporte no orientado a conexión de la pila TCP/IP . Se encarga del servicio de multiplexado entre aplicaciones que requieren un mínimo de información suplementaria. A diferencia de TCP, UDP carece de mecanismos de recuperación de errores, secuenciación o control de flujo. Su única prestación de encapsulado relacionada con los errores es la inclusión de un total de control capaz de detectar errores en cualquier parte del datagrama, incluida la parte datos por estas características, UDP es un control de eficacia extraordinaria que requieren mucha menos información adicional TCP. Mientras que todos los campos adicionales de TCP hacen que el encabezado TCP sume hasta 200 bits, el encabezado UDP apenas tiene 64 bits.

Además, la sencillez de UDP hace que los equipos del cliente y el servidor tengan que invertir menos recursos en enviar los datos con este protocolo. Sin embargo dado que no es muy fiable, son pocas las aplicaciones que lo usan; las más destacadas son el protocolo de transferencias de archivos trivial TFTP y el sistema de nombre de archivos DNS.

UDP es básicamente una interfaz de aplicación para IP. Como fue mencionado anteriormente, no añade confiabilidad, control de flujo, o recuperación de errores a IP, este simplemente es usado como un multiplexor/demultiplexor para recibir y enviar datagrama, usando los puertos para direccionar los datagramas como se muestran la figura10.

**Figura 10. Demultiplexión UDP basada en puertos.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

UDP provee a una aplicación de un mecanismo para enviar un datagrama a otra. La capa UDP tiene la cualidad de ser extremadamente delgada en consecuencia tiene cabeceras pequeñas, pero requiere que la aplicación tome la responsabilidad de la recuperación de datos y demás procesos de detección de errores. Las aplicaciones que envían datagramas a un cliente necesitan identificar con más precisión su destino, esto es, se requieren parámetros más específicos que la dirección IP, debido a que los datagramas son normalmente dirigidos a ciertos procesos y no al sistema como un todo. UDP se encarga esto usando el concepto de puertos.

### **2.3.3.1 Formato del datagrama UDP**

Cada datagrama de UDP es enviado dentro de un datagrama de IP. Sin embargo el datagrama de IP puede ser fragmentado durante la transmisión, la

implementación de IP de que recibe el datagrama se encargará de debe reensamblarlo antes de presentarlo a la capa UDP. A todas las implementaciones de IP se les exige que acepte datagramas de 576 bytes, lo que significa, que si permitiéramos el tamaño máximo de la cabecera de IP sea de 60 bytes, un datagrama de UDP de 516 bytes es aceptable las implementaciones. Muchas implementaciones aceptarán datagramas mayores, pero esto no está garantizado. El datagrama de UDP tiene un encabezado de 16 bytes esta está descrita en la figura de abajo.

**Figura 11. Formato del datagrama UDP.**

|             |                  |
|-------------|------------------|
| Source Port | Destination Port |
| Length      | Checksum         |
| Data...     |                  |

**Fuente:** *IP Network Design, Segunda edición. IBM.*

Donde:

- Puerto fuente (*Source Port*) : indica el puerto del proceso y envía el datagrama. Este es el puerto al cual da respuestas deben ser direccionadas.
- Puerto destino (*Destination Port*): especifica el puerto del proceso destino en mi cliente destino.
- Largo (*Length*): este campo nos da el largo del datagrama, incluyendo el encabezado.
- Sumario (*Checksum*): indica si el encabezado ha sido dañado en el transito entre la fuente y el destino.

### **2.3.3.2 Interfaz de programación de aplicación de UDP.**

La interfaz de aplicación ofrecida por UDP está escrita en la RFC 768. La cual provee de:

- La creación de nuevos puertos de recibo.
- La operación de recepción que retorna los bytes de data y de indicación de puerto y dirección IP fuente.
- La operación de envío que tiene como parámetros, la data, puertos y direcciones de fuente y destino.

La forma en la que la interfaz se implemente es dejada a la discreción de cada vendedor.

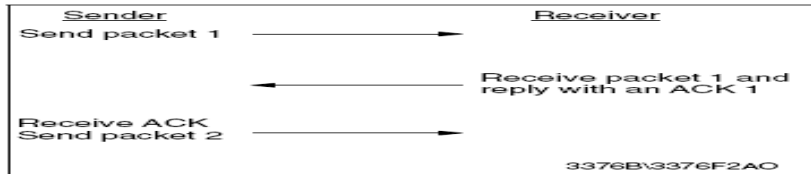
### **2.3.4 Protocolo de control de transmisión (TCP)**

El protocolo de control de transmisión es el protocolo de transporte basado en la conexión de la pila hacia TCP/IP. TCP incluye numerosas funcionalidades no presentes en el UDP. Una de las principales características de TCP es el método de control de flujo y de corrección de errores denominado gestión de ventanas.

#### **2.3.4.1 El principio de las ventanas**

Un protocolo simple de transporte podría usar el siguiente principio: enviar un paquete y entonces esperar a que el receptor acusé de recibo, antes de enviar el siguiente paquete. Si el acuse no es recibido dentro de cierta cantidad de tiempo, retransmite el paquete.

**Figura 12. Mensajes utilizados en el principio de ventanas básico.**



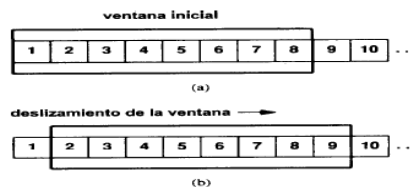
**Fuente:** *IP Network Design, Segunda edición. IBM.*

Mientras que este mecanismo asegura la confiabilidad, sólo utiliza una parte del ancho de banda de la red.

Ahora, consideremos un protocolo donde el transmisor agrupa los paquetes que serán transmitidos, y usa las siguientes reglas:

- El transmisor puede enviar todos los paquetes de toda la ventana sin recibir un acuse de recibo, pero debe empezar un temporizador por cada uno de ellos.
- El receptor debe acusar cada uno los paquetes recibidos, indicando el número de secuencia del último paquete bien recibido.
- El transmisor deben mover su ventana en cada acuse recibido.

**Figura 13. Estado inicial de la ventana.**

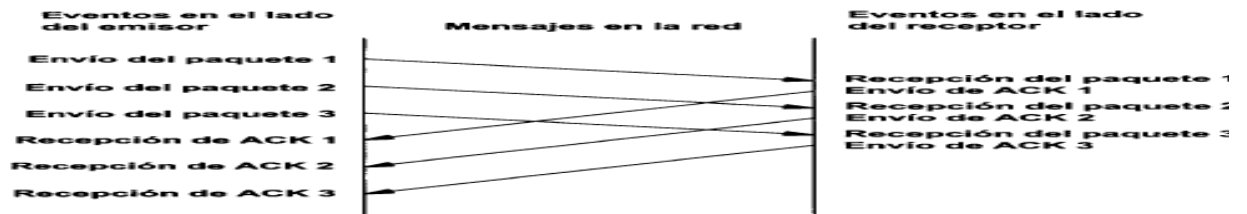


**Fuente:** [www.Saulo.net](http://www.Saulo.net), curso de TCP/IP.

En ese ejemplo el transmisor puede transmitir los paquetes del 1 al 8 sin espera por acuse alguno:



**Figura 14. Secuencia de envío y acuse.**

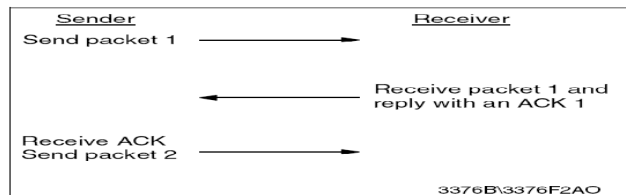


Fuente: [www.Saulo.net](http://www.Saulo.net), curso de TCP/IP.zip

Durante la transmisión de los primeros 8 paquetes se intercambian mensajes de acuse de recibo por cada paquete.

En el momento en el que el remitente recibe la acuse 1 (ACK1) el puede deslizar su ventana un paquete a la derecha como se muestra en la Fig.15.

**Figura 15. Deslizamiento de ventana al recibir un acuse.**



Fuente: *IP Network Design, Segunda edición. IBM.*

En este punto, el transmisor puede también transmitir el paquete 9

Imaginemos algunos casos especiales:

- El paquete 2 se pierde: el transmisor no recibirá el acuse 2 (ACK2), así que su ventana permanecerá en la posición 1 figura de arriba. De hecho, debido a que el receptor no recibió el paquete 2, este acusara a los paquetes 3,4 hasta el 8 con el acuse 1, ya que el paquete 1 fue

el último recibido en secuencia. Del lado del transmisor, eventualmente el tiempo de espera pasara por el paquete 2 y este será retransmitido. Nótese que a la hora que sea recibido, el receptor generara el acuse 8, debido a que ha recibido exitosamente todos los paquetes de 1 a 8, y la ventana del transmisor ahora se correrá la posiciones indicadas por el parámetro de tamaño de ventana en cuanto reciba este acuse 8.

- El paquete dos es recibido pero el acuse se pierde: el transmisor no recibe el acuse 2, pero recibirá el 3. El acuse 3 es la confirmación de que todos los paquetes hasta el 3 (incluyendo el paquete 2) ha llegado, con esto el transmisor corre su ventana al paquete 4.

El mecanismo de ventanas se asegura que:

- Existan una transmisión confiable.
- Un mejor uso del ancho de banda de la red (mejora el rendimiento).
- Exista un control de flujo: esto se logra a través del tamaño de ventana y de los acuses de recepción.

#### **2.3.4.2 El principio de ventanas aplicado a TCP**

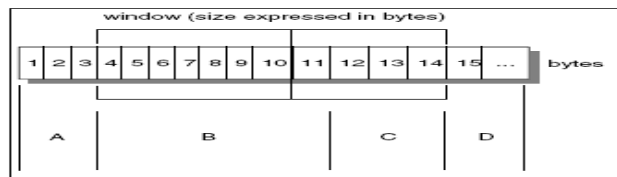
Debido a que TCP proporciona una conexión con un flujo de bytes continuo, números de secuencia son asignados a cada uno. TCP divide este flujo continuo de bytes en segmentos para transmitir los puntos el principio ventana es usado a nivel de bytes, esto es segmentos enviados y los acuses recibidos incluirán el número del secuencia de byte. El que mañana ventana es expresado como un número de bytes, más que un número de paquetes.

El que mañana ventana es determinado por el receptor cuando la conexión establecida y es variable durante la transferencia de datos. Cada

mensaje de acuse incluirá el tamaño de ventana que él receptor está listo para manejar en un tiempo particular.

El flujo de datos del transmisor puede ser visto como sigue:

**Figura 16. Estado de los mensajes de TCP durante la transferencia de datos.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Donde:

- A: son los bytes que han sido transmitidos y que han sido acusados de recibo.
- B: son los bytes que han sido transmitidos y que todavía no han sido acusado de recibo.
- C: son los bytes que pueden ser enviados sin esperar por acuse alguno.
- D: son los bytes que no pueden ser enviados todavía.

Recordemos que TCP agrupará los bloques de bytes en segmentos, y que el segmento sólo carga y una secuencia en el primer byte en el segmento.

La gestión de ventanas es una forma eficaz de control de flujo técnica ventanas permite que un cliente envíe sólo una cantidad precalculada bytes antes de esperar una respuesta, o acuse de recibo (ACK, aknowledge), del receptor. La gestión de ventanas, como todas las formas de control de flujo, impide que ningún dispositivo sobrecargue a otro mediante una comunicación en una red. TCP utiliza un tipo de gestión de ventanas basado en la acuse es

de recibo directos (FACK, *forward acknowledgements*), y sus límites se basan en bytes. Con un FACK, si se envían 50 bytes a un destinatario y éste recibe los 50, devolverá la acuse de 51. Este acuse de 51 bytes indica al emisor que los 50 bytes han sido recibidos y que se espera el byte 51. Ese byte 51 no se remitirá hasta que se reciba un acuse para los 50 anteriores. Si nunca se recibe el acuse para los primeros bytes, se volverán a retransmitir los 50 después de que expire un tiempo llamado tiempo de retransmisión. Si se recibe un acuse para algunos, pero no es para todos, se retransmitirán únicamente los no recibidos. Las ventanas deslizantes describen el modo en que TCP "mueve" su ventana flujo de datos como respuesta a los acuses. La técnica de ventanas es TCP y dinámica, en el sentido de que el tamaño de ventanas puede cambiar el curso de la sesión como respuesta a los errores o a la ausencia de los mismos. Durante el establecimiento inicial de la sesión se definirá el tamaño base de la ventana. También se enviará el número de secuencia inicial, que declara el inicio del número de byte. Por cada segmento enviado, el campo tamaño de ventana del encabezamiento TCP informará de que dimensión de ventana ha elegido el otro extremo de la comunicación. Si se produce un error y se pierden algunos datos haciendo que TCP los retransmita, el cliente puede reducir el tamaño de ventana, por otra parte si se han enviado enormes cantidades de datos sin errores, el cliente podría aumentar el tamaño de ventana.

Además de ser un proceso dinámico, la técnica de ventanas en TCP es full dúplex, lo que significa que existen la ventana de envío y una de recepción por cliente cada ventana funciona independientemente de la otra, y puede ampliarse o contraerse sin relación con su pareja. Otra importante propiedad de TCP es su capacidad de multiplexar sesiones lógicas entre clientes remotos. Esta característica está presente tanto en TCP como en UDP, y permite tener abiertas múltiples conexiones al mismo tiempo, ofreciendo al protocolo de transporte un método para diferenciar las conexiones.

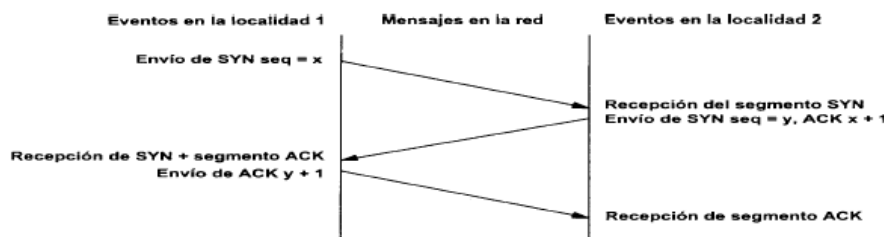
### 2.3.5 Establecimiento de la sesión en TCP

Por último, queda por explicar y el elemento que hace que funcionen todas las prestaciones de TCP: la sesión en sí. El establecimiento de una sesión en TCP tiene tres objetivos principales:

- Verificar la conectividad entre los dos clientes que participan en la sesión.
- Informar a ambos lados del número de secuencia de inicio que se utilizará.
- Informar a ambos lados del tamaño inicial de la ventana empleado.

El proceso de establecimiento de sesión también llamado establecimiento de conexión funciona el modo siguiente. El cliente inicia la sesión enviando un segmento con el bit de sincronización activado. Este segmento incluye el tamaño de ventana del cliente y su número de secuencia actual. El servidor responde con un acuse a la petición de sincronización del cliente, e incluye su propio bit de sincronía, su tamaño de ventana y su número de secuencia inicial. Finalmente el cliente responde con un acuse a la sincronía de servidor.

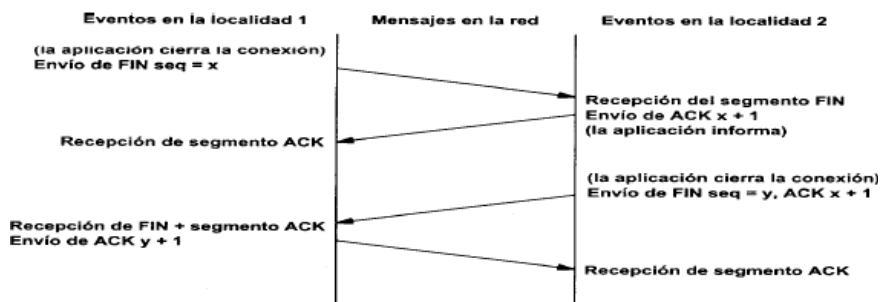
**Figura 17. Saludo de tres vías al iniciar una sesión de transferencia.**



Fuente: Saulo.net, curso de TCP/IP.zip.

El proceso de terminación de sesión es semejante al del establecimiento. Primero, el lado de la comunicación que quiere cerrar la sesión inicia la terminación enviando el bit FIN. El servidor responde con un acuse de recibo a este FIN del cliente y luego envía su propio segmento con el bit FIN activo.

**Figura 18. Secuencia de finalización de sesión de TCP.**



Fuente: [www.Saulo.net](http://www.Saulo.net), curso de TCP/IP.

### 2.3.6 Formato del segmento TCP

Segmento: unidad de transferencia TCP entre dos máquinas. Se intercambian para: establecer conexiones, enviar datos, enviar acuses de recibo, anunciar ventanas y cerrar conexiones.

**Figura 19. Formato de la trama TCP.**

|                       |          |                  |        |
|-----------------------|----------|------------------|--------|
| Source port           |          | Destination port |        |
| Sequence number       |          |                  |        |
| Acknowledgment number |          |                  |        |
| Data offset           | Reserved | Flags            | Window |
| Checksum              |          | Urgent pointer   |        |
| Options (+ padding)   |          |                  |        |
| Data (variable)       |          |                  |        |

Fuente: *IP Network Design, Segunda edición. IBM.*

El formato del segmento de TCP descrito por la figura anterior utiliza los campos incluidos anteriormente para lo siguiente:

- Puerto fuente y destino: identifica los puntos donde los procesos de capa superior de fuente y destino pueden acceder a los servicios de TCP.
- Número de secuencia: usualmente especifica el número asignado al primer byte de datos en el mensaje actual. En la fase de establecimiento de conexión, este campo puede ser utilizado para identificar un número de secuencia inicial que será usado durante la transmisión.
- Número de acuse de recibo: contienen el número de secuencia del siguiente byte de datos que receptor espera recibir.
- Data offset: longitud del encabezado en múltiplos de 32 bits.
- Reservado: este campo permanece reservado para futuros usos.
- Banderas: contienen una variedad información de control, incluyendo los bits de acuse y sincronía usados para establecer una conexión, y el bit de FIN usado para terminar una conexión.
- Ventana: especifica el tamaño de la ventana de recepción esto es el tamaño de buffer disponible para recepción de datos.
- Sumario: indica si el encabezado ha sido dañado durante el tránsito en la red.
- Puntero de urgencia: apunta o identifica el primer byte de urgencia del paquete.
- Opciones: especifica varias opciones de TCP.
- Data: contienen información de la capa superior.

### **2.3.7 IP (Internet Protocol)**

Se trata de un protocolo de nivel 3 no orientado a la conexión, permitiendo el intercambio de datos sin el establecimiento previo de la llamada.

Una característica fundamental es que soporta las operaciones de fragmentación y de reensamblado, por medio de las cuales un datagrama se subdivide y segmenta en paquetes más pequeños para ser introducidos a la red, y luego en destino se reconstruyen en su formato original para entregarlos al nivel superior. La otra operación que revista importancia es el enrutamiento, el cual implementa por medio de un esquema de direccionamiento que se trata a continuación. En la actualidad se emplea la versión 4 de este protocolo, pero está en estudio y muy próxima a implementarse la Versión 6 o Next Generation, pero para fines prácticos solo se explicará la versión 4.

#### **2.3.7.1 Asignación de direcciones y segmentación de redes**

Para proveer una comunicación efectiva entre los clientes y estaciones de una red, cada elemento debe mantener una identificación única. La distribución y administración de dichas direcciones es un factor muy importante para tomar en cuenta en el diseño de una red. Las direcciones para las redes deben ser bien planeadas, administradas y documentadas. Todo esto por que las direcciones para las redes y subredes no pueden ser asignadas dinámicamente, una red que no está bien planeada o documentada es una red en la cual hallar un error es imposible de escalar.

En oposición a la red misma los elementos que conforman la red si pueden ser programados para la asignación dinámica de direcciones. Esto permite una administración más fácil y robusta.

#### **2.3.7.2 Direcciones de IP**

La dirección IP es definida en la RFC 1166 como número constituido por 32 bit formado por dos partes:



Dirección IP = <numero de red> <numero de cliente>

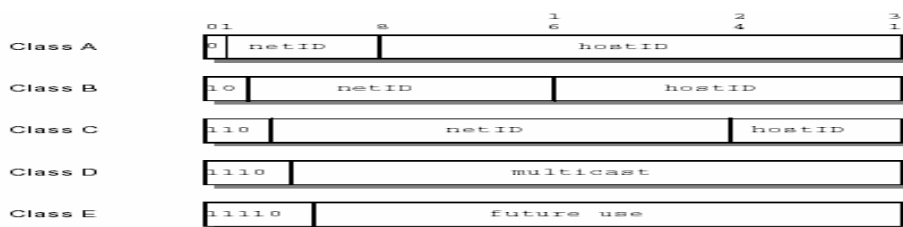
La primera parte de la dirección es asignada por una autoridad regional, y va a variar en su longitud dependiendo de la clase de direcciones a la que pertenezca. Esta parte de la dirección es utilizada por el protocolo de IP para enrutar los datagramas IP a través de la red TCP/IP. Estas redes por lo general están dentro de una empresa, lo cual permite cierta libertad por la asignación de esta parte de la dirección, sin tomar en cuenta a la autoridad regional de Internet, pero si este es el caso se recomienda el uso de ciertas direcciones preasignadas para las redes privadas por la IANA (Internet Assigned Number Authority). Sin embargo, su enrutamiento puede llevarlo a redes fuera de su control, usando, por ejemplo, los servicios a nivel mundial del Internet. En este caso es imperativo obtener una única dirección IP de la autoridad regional de Internet.

La segunda parte de la dirección es usada para identificar al cliente individual dentro de la red, esta porción de la dirección es asignada localmente dentro de la red por la autoridad que controla la red, el largo de esta parte es, como mencionamos anteriormente, es dependiente de la clase de la dirección IP que se está usando y también si se está haciendo el procedimiento de segmentación de red (SR).

Los 32 bits que constituyen la dirección IP son usualmente como valores decimales de 8 bits concatenados con puntos. Esta representación es comúnmente referida como notación decimal puntuada. Un ejemplo de esta notación es 192.18.4.19. En este ejemplo el 192.18 es la parte designada a la red y el 4.19 es la parte designada al cliente de la red. La

división entre la parte asignada a la red y la parte asignada al cliente es determinada por la clase de dirección IP. Existen cinco clases de direcciones IP como se muestra en la figura 20.

**Figura 20. Clases de direcciones IP.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Este diagrama muestra la división de la dirección IP en la parte de número de red y el la parte del número de cliente. Los primeros bits determinan la clase de la red y su estructura. Las clases A, B y C representan direcciones de uní\_ difusión y conforman la mayoría de las direcciones IP utilizadas por la INTERNIC. Una dirección de uní-difusión se refiere a una dirección que solo se dirige a un solo destino. Para dirigirse a múltiples direcciones o a todas se utilizan las direcciones de múltiple difusión y de difusión .

Las redes clase A tiene el primer bit puesto a cero. Los siguientes 7 bits sin usados para el número de la red. Esto da la posibilidad de 128 redes ( $2^7$ ) pero sin embargo debe hacerse notar que existen dos casos, todos los bits a 0 o todos los bits a 1, que tiene significados especiales en las redes clase A, B y C. Estos casos especiales de direcciones son reservas, lo que da como resultado solamente la posibilidad de 126 clases de redes A, los

24 bits restantes son utilizados para los números de los clientes. Aquí también se aplican los dos casos especiales de direcciones a la dirección del cliente. Cada red tipo A puede tener hasta 16, 777,214 clientes. Las redes clase A generalmente son asignadas a redes que tienen un número elevado de clientes. Las direcciones de clase B es más adecuada para las redes de tamaño mediano, los primeros dos bits de la direcciones están predefinidos a 10. los siguientes 14 bits son usados para asignar el número de red los restantes 16 son usados para el número de clientes esto da una posibilidad de 16,382 redes conteniendo 65,534 clientes.

Las direcciones clase C ofrecen un máximo de 254 clientes por red y es por eso más preasignados a 110, los siguiente 21 proveen un máximo de 2,097,150 de este tipo de redes.

Las clases restantes de estas direcciones que son las D y E, son clases reservadas y tienen un significado especial. Las clase E están reservadas para uso futuro mientras que las clase D son usadas para direccionar clientes en un área limitada. Esta última sería una red de múltí difusión

### **2.3.7.3 Subredes**

La idea de una subred es dividir en partes más pequeñas el numero de cliente de una dirección IP de manera de proporcionar niveles extra de direccionabilidad como hemos visto anteriormente la dirección IP se divide en:

Dirección IP = <numero de red> <numero de cliente>

El enrutamiento entre redes esta basado sobre la parte del número de red de la dirección IP. En una dirección de tipo A solamente una byte de la dirección IP es usado para la función de enrutamiento del paquete( por ejemplo la dirección 9), esto esta bien para redes remotas enrutando en la red local 9. ellas simplemente dirigen para la red a un enrutador especifico que acepta todo el trafico 9.0.0.0 Sin embargo el enrutador debe mover este trafico a cada una de la s16,777,214 direcciones que la red puede tener, esto resultaría en una tabla de enrutamiento inmensa, ya que este debe saber donde se encuentra el cliente o estación de trabajo dentro de la red. Para solucionar este problema, el numero que identifica al cliente dentro de la red puede ser subdividido dentro de un número de subred y numero de cliente para proveer una segunda red lógica dentro de la primera. Ahora la dirección dentro de la subred tendrá tres partes que son:

Dirección IP= <número de red>< numero de subred><numero de cliente>

El número de subred es transparente a las redes remotas. Los clientes remotos no se dan cuenta de la subdivisión de la red, solamente aquellos clientes que están dentro de la red que están configurados para usar estas subredes están concientes de que la segmentación de la red existe.

Exactamente como se divide la parte local de la dirección en número de subred y de cliente es determinado por su administrador local de red. La técnica de hacer subredes se puede utilizar con los tres tipos de direcciones A, B y C, pero hay que tomar ciertas precauciones de acuerdo con las diferentes direcciones, por ejemplo las direcciones clase C solamente tienen un byte de numero de cliente para dividir en subred y cliente, esto quiere decir que hay que tener cuidado al tomar el número de bits para hacer la subred

ya que si tomamos demasiados podemos hacer muy pequeña la cantidad de clientes que podemos soportar.

#### 2.3.7.4 Máscara de subred

Una subred es creada usando la máscara de subred. Esta máscara consiste en un número de 32bits igual que la dirección IP, cada una de las partes de la máscara puede ser relacionada con el número de red, el número de sub red y el cliente. Los bits en la máscara que identifican el número de la red son puestos a uno para conservar el enrutamiento original, el resto de los bits de la máscara local los bits puestos en uno identifican la subred los puestos a cero identifican en numero del cliente, se pueden usar cualquier numero de bits del numero de cliente para formar la máscara de subred. Sin embargo, estos bits deben permanecer continuos cuando se crea la máscara porque esto hace que la dirección sea más comprensible y fácil de administrar, también recomendamos que, cuando se pueda, se usen 8 o 4 bits para la máscara. De nuevo esto hace que mucho más fácil entender los valores de la máscara y la hace también más fácil de administrar. Ahora veamos la máscara 255.255.255.0. Esta tiene una representación binaria como sigue:

```
11111111 11111111 11111111 00000000
```

Para que un cliente o enrutador aplique la máscara, este le hace una AND lógica a la dirección IP que esta tratando de enrutan con la máscara por ejemplo 172.16.3.14

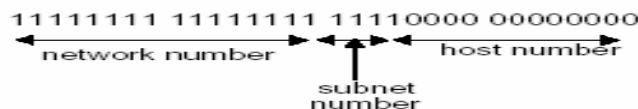
```
10000000 00001010 00000011 00001110
11111111 11111111 11111111 00000000    AND lógica
10000000 00001010 00000011 00000000
```

El resultado nos da el resultado de subred 172.16.3. Como se puede notar una subred es normalmente identificada como una concatenación del número de red y el número de sub red. El cero que los precede normalmente no es mostrado, el data grama original puede ser enrutado a su destino dentro de la red basado en el valor de sub red obtenida.

La máscara de sub red anterior utiliza los 8 bits para el numero de subred, esta es una practica que recomendamos fuertemente, sin embargo también puede utilizarse un número diferente de bits. Otra forma común de hacer este procedimiento es utilizar 4 bits para el número de subred y los bits restantes son utilizados para el numero de cliente esta puede ser una mejor opción cuando se este haciendo una subred en una red de direcciones tipo C. Tomando en cuenta de que solo se tiene solamente 1 byte de numero de cliente para usar. Usando el primer esquema es claro el numero de subredes que se pueden tener, la máscara de ocho bits nos provee de una cifra fácil de leer que en nuestro ejemplo es 3. Cuando se usan 4 bits las cosas nos son tan claras a primera vista.

Tomemos la misma red clase B antes usada y esta vez apliquemos la máscara de subred de 255.255.240.0 que solo tiene 4 bits significativos en el tercer byte para el número de subred los valores de los bits para esta máscara son:

**Figura 21.Representación binaria de las partes que componen la dirección IP.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Aplicando esta máscara , el tercer byte de la dirección es dividido en dos números de 4 bits cada uno: el primero representa el número de la subred, mientras que el segundo está concatenado con el último byte de la dirección para proveer una dirección de 12 bits para el cliente. La tabla I contiene el número de subred que son posibles de usar cuando se usan esta máscara de subred:

**Tabla I. Direcciones de subred**

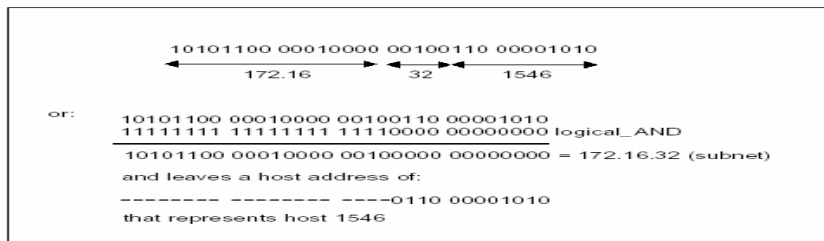
| Valor Hexadecimal | Número de Subred |
|-------------------|------------------|
| 0                 | 0                |
| 1                 | 16               |
| 10                | 32               |
| 11                | 48               |
| 100               | 64               |
| 101               | 80               |
| 110               | 96               |
| 111               | 112              |
| 1000              | 128              |
| 1001              | 144              |
| 1010              | 160              |
| 1011              | 176              |
| 1100              | 192              |
| 1101              | 208              |
| 1110              | 224              |
| 111               | 240              |

Para cada uno de estas direcciones de subred, solamente 14 direcciones (de 1 a 14) son válidas debido a las restricciones de las direcciones especiales. Esta división entonces daría 14 subredes cada una con 4094 clientes. Como se puede ver el valor aplicado al número de la subred como el valor del byte entero con los bits menos significativos puestos a cero. Por ejemplo, el valor hexadecimal 0001 en esta máscara de subred

asume un valor de 8 bits como sigue 00010000 y da un valor de subred de 16 y no de 1 como puede verse.

Aplicando esta máscara de subred a una dirección de clase B, por ejemplo, 172.16.38.10 dividiría la red como sigue:

**Figura 22. Asignación de dirección usando máscaras de subred.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

Como se puede ver en la figura 22 el número de cliente es número relativo de cliente esto es, es cliente 1546 en la red número 32 este número no se asemeja a la dirección IP actual que le ha sido asignada a este cliente y no tiene ningún significado en términos de enrutamiento.

### 2.3.7.5 Tipos de segmentación

En un principio presentamos la idea de que la razón con más peso para utilizar la segmentación de red era para solucionar el problema de enrutamiento, cuando la red es demasiado grande y tenía un número excesivo de clientes. Pero existen algunas otras razones por las cuales este procedimiento debe ser tomado en cuenta, por ejemplo la asignación de la



direcciones de clientes dentro de una red local sin las subredes puede llegar también a ser un problema serio.

Construir una red con diferentes tecnologías, por ejemplo red LAN basadas en anillos con control de transmisión (Token Ring), punto a punto sobre redes SNA, y así pueden imponer restricciones severas a la hora de asignar direcciones y puede que se necesario tratar a cada una de ellas como una red por separado. Si por otro lado el limite de la tecnología de la red es alcanzado en términos del número de clientes conectados a la red el hecho de añadir más clientes haría necesario una nueva red en términos físicos. Puede haber subconjunto de clientes que monopolizan el ancho de banda de la red y causan congestión de la red. Agrupando estos clientes en redes físicas basadas en sus altas necesidades de comunicación pueden aliviar el problema de congestión al resto de la red. En cada uno de los casos anteriores se necesitara asignar direcciones múltiples de IP para acomodar estas redes. Usando la segmentación estos problemas se ven resueltos y nos permite utilizar plenamente las direcciones IP que nos han sido asignadas.

#### **2.3.7.5.1 Segmentación estática**

En ejemplos anteriores, usamos la misma máscara de subred en cada uno de los clientes y enrutadores en la red 172.16. Esto puede llamarse Segmentación Estática este tipo de segmentación como ya puede ser obvio implica que solamente una máscara de subred va a ser utilizada dentro de toda la red. Una interrelación de redes puede darse entre redes de diferentes clases, pero cada una de estas redes solamente va a implementar una sub red dentro de ellas. Este es el tipo de segmentación más fácil de entender y mantener, esta implementada en casi la mayoría de clientes y enrutadores y es soportador en el RIP. Sin embargo, veamos la asignación de clientes dentro

de una subred. En nuestra red clase B (172.16.0.0) usa una máscara de subred de 255.255.255.0. Esto permite a cada una de las subredes hasta 254 clientes. Si una de las subredes es una red de trabajo, tal vez un enlace punto a punto con solamente dos direcciones de clientes, entonces hemos gastado 252 de las direcciones que pueden ser asignadas dentro de la red. Este es uno de los mayores inconvenientes del hecho de usar subredes estáticas.

#### **2.3.7.5.2 Segmentación con máscara de longitud variable**

Este desperdicio de direcciones puede solucionarse utilizando la segmentación de longitud variable, como su nombre indica la segmentación de longitud variable permite a varias subredes usar máscaras de subred de diferentes tamaños, de esta manera una subred puede usar una máscara de acuerdo a su tamaño evitando el desperdicio de direcciones, añadiendo o sustrayendo bits a la longitud de la máscara, la subred puede ser fácilmente reorganizada para acomodar cambios en la red el inconveniente con este tipo de segmentación es que no está implementado en la mayoría de clientes ni en los protocolos de enrutamiento.

#### **2.3.8 *Frame Relay***

*Frame Relay* es un protocolo de redes WAN de alto desempeño que opera en las capas, física y de enlace del modelo de referencia OSI. Originalmente fue diseñado para ser usado en las interfaces físicas de ISDN. Hoy es utilizado en una variedad de interfaces y redes.

Esta tecnología es un claro ejemplo de una red de conmutación de paquetes que permite a una Terminal compartir dinámicamente los medios y

el ancho de banda disponible de la red. Las siguientes técnicas son utilizadas en las tecnologías de conmutación de paquetes:

- Paquetes de longitud variable
- Multiplexado estadístico

La primera técnica es utilizada para una transferencia de datos más flexible y eficiente. Estos paquetes son conmutados entre varios de los segmentos de la red hasta que alcanza su destino.

La segunda técnica controla el acceso a la red en una red de conmutación de paquetes. La ventaja de esta técnica es que acomoda mapas de flexibilidad y un mejor uso del ancho de banda. La mayoría de las tecnologías LAN como *Ethernet* y *Token Ring*, son redes de conmutación de paquetes.

Frame Relay es a veces descrito como una versión más fluida de X.25, que ofrece menos de las robustas capacidades, tales como el ventaneo y la retransmisión de la última data que son obtenidas al usar X.25. Esto se debe a que por lo general Frame Relay trabaja en enlaces de WAN que por lo general ofrecen servicios de conexión mucho más confiables que los que se poseían en las décadas de los 70's y 80's época donde se implementó el X.25. Como se mencionó anteriormente Frame Relay es estrictamente un protocolo de capa 2 esto quiere decir que como X.25 también provee de servicios a la capa 3, esto permite a esta tecnología ofrecer servicios de transmisión con un mejor desempeño y eficiencia que los que ofrecía X.25, y la hace más adecuada a las necesidades y aplicaciones de las WAN como por ejemplo la interconexión de LAN.

### 2.3.8.1 Dispositivos de *Frame Relay* .

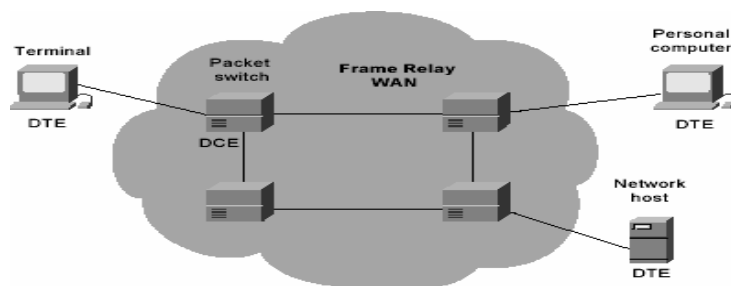
Los dispositivos conectados a una red de Frame Relay caen en dos categorías generales que son:

- Equipo terminal de datos (DTE)
- Equipo terminal de circuitos (DCE)

Los DTE generalmente son considerados como equipo terminal para una red específica y típicamente están instalados en el emplazamiento del cliente. De hecho este equipo puede pertenecerle al cliente. Ejemplos de equipos DTE serían: computadores personales, enrutadores, y puentes.

Los DCE por lo general son equipos que pertenecen al proveedor de servicios. El propósito de este equipo es de proporcionarle servicios de sincronía y de conmutación en una red, estos son los elementos que en verdad transmiten datos a través de la WAN, en la mayoría de los casos son conmutadores de paquetes en la figura se muestra la relación entre las dos categorías de elementos de una red *Frame Relay*.

**Figura 23. Elementos de una red *Frame Relay*.**



Fuente: [//www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm).

La conexión entre un elemento DTE y uno DCE consiste en un componente de dos capas tanto física como de enlace. El componente físico define las especificaciones mecánicas, eléctricas y funcionales para la conexión entre elementos una de las especificaciones mayormente usadas y recomendadas es el estándar RS-232. Los elementos de la capa de enlace definen el protocolo que establece la conexión entre los elementos DTE, tales como un enrutador, y los DCE, tales como un conmutador.

### **2.3.8.2 Circuitos virtuales**

El protocolo Frame Relay proporciona una comunicación a nivel de enlace orientada a conexión. Esto significa que una comunicación definida existen entre cada par de elementos y que esta comunicación esta asociada con un identificador de conexión, este servicio es implementado usando los circuitos virtuales de Frame Relay , los cuales son conexiones lógicas creada entre dos equipos DTE a través de la red de conmutación de paquete (PSN) de Frame Relay .

Los circuitos virtuales proveen canal de comunicación bidireccional de un elemento DTE a otro y son identificados de una manera única por medio del identificador de conexión de enlace (DLCI). Un número de circuitos virtuales pueden ser multiplexados en un único canal físico para su transmisión a través de la red esta capacidad a veces puede reducir la complejidad de la red y del equipo requerido para conectar múltiples equipos DTE.

Un circuito virtual puede pasar a través de cualquier numero de elementos intermedios DCE (conmutadores) localizados dentro de la red. Los circuitos de Frame Relay puede caer en dos categorías: circuitos virtuales conmutados (SVC) y circuitos virtuales permanentes (PVC).

### 2.3.8.2.1 Circuitos virtuales conmutados

Los SVC son conexiones temporales usadas en situaciones en las que se requiere solamente la transferencia de datos de forma esporádica entre elementos DTE a través de la red. Una sesión de comunicación a través de un SVC consiste en los cuatro estados operaciones siguientes:

- Establecimiento de llamada. El circuito virtual entre dos elementos DTE es establecida.
- Transferencia de datos. La data es transmitida entre los elementos DTE sobre el circuito virtual.
- Circuito Ocioso. La conexión entre los elementos DTE todavía esta activa, pero no existe transferencia de datos. Si un SVC permanece en un estado ocioso por un periodo de tiempo definido, la llamada puede ser terminada.
- Terminación de la llamada. El circuito virtual entre los elementos DTE es terminado.

Después de que un circuito virtual es terminado, el elemento DCE debe establecer un nuevo SVC si existe alguna data adicional que debe ser intercambiada. Se espera que los SVC serán establecidos, mantenidos, y terminados usando la misma señalización usados por los protocolos de ISDN.

Pocos fabricantes de equipos DCE de Frame Relay soportaban la conexión de circuitos conmutados. De allí que su implementación en las redes fuera mínima. Ahora la situación a cambiado ahora los SVC son soportados por norma, esto debido a al ahorro en el sentido económico que significa el hecho de que el canal no este establecido todo el tiempo.

### **2.3.8.2.2 Circuitos virtuales permanentes**

Este tipo de circuitos establecen conexiones permanentes que son usadas en transferencias frecuentes y consistentes de datos entre elementos DTE a través de la red Frame Relay. La comunicación a través de un circuitos no requieren los procedimientos de inicio y terminación de la llamada como en los SVC, los PVC siempre operan en uno de los siguientes estados:

- Transferencia de datos. La data es transmitida entre dos elementos DTE sobre el circuito virtual.
- Ocioso. La conexión entre los elementos permanece activa, pero no existe transferencia de datos. Al contrario de los SVC los PVC no terminara el circuito bajo ninguna circunstancia cuando esta en estad ocioso.

Los elementos DTE pueden iniciar la transferencia de datos en el momento que estén listos debido a que el canal esta permanentemente establecido.

### **2.3.8.3. Identificador de conexión de enlace**

Los circuitos virtuales de Frame Relay son identificados mediante el identificador de conexión de enlace (DLCI). Los valores de DLCI son asignados típicamente por el proveedor de servicios. Los DLCI tienen significado local, lo que quiere decir que sus valores son únicos en la LAN pero no necesariamente en la WAN.

#### 2.3.8.4 Mecanismos de control de congestión

Frame Relay reduce los encabezados mediante la implementación de mecanismos simples de notificación de congestión, por cada control de flujo de circuito virtual, las implementaciones de Frame Relay por lo general son hechas sobre un medio físico de transporte confiable, así la integridad de la data no es sacrificada, puesto que el control de flujo es responsabilidad de un protocolo de más alto nivel.

Frame Relay implementa dos mecanismos de notificación de congestión que son

- Notificación explícita hacia adelante o frontal (FECN)
- Notificación explícita hacia atrás o en reversa (BECN)

Ambas la FECN y al BECN son controladas por un sol bit contenido en la cabecera, esta última también contiene el bit de elegibilidad para ser descartado (DE), el cual es utilizado para identificar el tráfico de menos importancia el cual puede ser descartado en caso de congestión.

El bit de FECN es parte del campo de dirección en el encabezado de *Frame Relay*. EL mecanismo de FECN es iniciado cuando un elemento DTE envía una trama dentro de la red. Si la red esta congestionada , los elementos DCE cambian el estado del bit de FECN en el encabezado de trama, cuando las tramas alcanzan al elemento DTE destino, el campo de dirección con el bit de FECN en 1 indica que el paquete sufrió de congestión en el camino de fuente a destino. El elemento DTE puede confiar esta información a un protocolo de más alto nivel para su procesamiento. Dependiendo de la implementación, puede ser iniciado un proceso de control de flujo o la indicación puede ser ignorada.



#### **2.3.8.4.1 Elegibilidad para descarte**

El bit de elegibilidad para descarte de la trama DE indica que la trama en cuestión tiene una importancia menor a otras tramas. El bit DE es parte del campo de direcciones en el encabezado de *Frame Relay* (FR).

Un elemento DTE puede establecer el valor del bit de DE si este es puesto a 1 y indica que la trama tiene una importancia menor a las de otras tramas. Cuando la red se congestiona los elementos DCE descartan las tramas con el bit de DE puesto en uno antes de descartar las tramas que no están marcadas con este bit. Esto reduce la posibilidad de descartar tramas con información crítica durante la duración de la congestión.

#### **2.3.8.4.2 Chequeo de error**

*Frame Relay* utiliza un mecanismo de control de error conocido como CRC que es el Chequeo de Error Cíclico. El CRC compara dos valores calculados para determinar si algún error ocurrió durante la transmisión de la fuente al destino. FR reduce su tamaño de cabecera por medio de la implementación del chequeo de error en lugar de la corrección de errores. Típicamente una red de FR esta montada sobre un medio de transmisión confiable, así la integridad de la data no es sacrificada porque la corrección de errores se deja a un protocolo superior corriendo arriba de FR.

#### **2.3.8.5 Interfaz administrativa local (LMI)**

La interfaz administrativa local es un conjunto de mejoras a las especificaciones de FR básicas. Esta fue desarrollada en 1990 por Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation. Esta

ofrece un número de funciones (llamadas extensiones) par la administración de grandes redes. La funcione o funcionalidades claves incluidas en la extensiones de la LMI están las direccionamiento global, mensajes de estado de circuitos virtuales, y multidifusión.

El direccionamiento global de la LMI de al DLCI valores de tipo global en lugar de un valor de tipo local. Los valores de los DLCI se convierten en las direcciones de los DTE que son únicos en la WAN de FR. La extensión de direccionamiento global adhiere funcionalidad y manejabilidad a la interrelación de red de FR. La interfaces individuales de red y los nodos terminales adheridos a ellas , por ejemplo pueden se identificados por medio del uso de técnicas de resolución de direcciones y descubrimiento de elementos. Además la red entera de FR tiene la apariencia de una LAN para los enrutadores en su periferia.

Los mensajes virtuales de estado de circuito proveen de comunicación y sincronización ente los elementos DTE y DCE de la red de FR. Estos mensajes son utilizados para reportar periódicamente el estatus de los PVC, lo que evita que la data sea enviada a PVC que ya no existan. La extensión de multidifusión de la LMI permite crear grupos de multidifusión. La multidifusión ahorra ancho de banda porque permite enviar actualizaciones de rutas y resoluciones de direcciones solamente a grupos específicos de enrutadores.

#### **2.3.8.6 Formato de la trama de *Frame Relay***

Para entender muchas de las funcionalidades de FR, es de utilidad entender la estructura de la trama de FR. Unas banderas indican el principio y el final de una trama. Tres son los componentes principales que constituyen una trama de FR y son: la cabecera, un área de direcciones, la porción de datos

de usuario, y la secuencia de chequeo de trama (FCS). El área de direcciones, que es de dos bytes de largo, es comprendida de 10 bits que representan el verdadero identificador del circuito y 6 bits que tienen que ver con el manejo de la congestión de red, a este se le llama DLCI las diferentes tramas de FR que son la básica y la expandida (con LMI) son discutidas a continuación.

### 2.3.8.6.1 Trama de *Frame Relay Standard*

La trama estándar de FR consiste en los campos ilustrados en la figura24

**Figura 24. Trama estándar de *Frame Relay*.**



Fuente: [//www.cisco.com /univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm).

Descripción de los campos:

- **Banderas.** Delimitan el principio y el final de una trama, el valor en este campo es siempre el mismo y es representado por el número hexadecimal 7E o como el número binario 01111110.
- **Dirección.** Contiene la siguiente información.
  - **DLCI.** los 10 bits de DLCI son la esencia de la cabecera de FR, este valore representa la conexión virtual entre el elemento DTE y el conmutador. Cada conexión virtual que es multiplexada en el canal físico será representada por un único DLCI. Los valores de DLCI tiene significancia local solamente, lo que significa que son únicos solamente dentro del canal físico en los que residen. Por lo tanto, elementos ubicados en los extremos opuestos de la

conexión pueden usar diferentes valores de DLCI para referirse a la misma conexión virtual.

- **DIRECCION EXTENDIDA (EA).** la EA es usada para indicar si en el byte en el cual el valor de la EA es 1 es el último campo de direcciones. Si el valor es 1, entonces se determina que el byte actual es el último octeto del DLCI.
- **C/R.** El C/R es el bit que sigue al byte más significativo del DLCI en el campo de direcciones, este no está actualmente definido.
- **Control de congestión.** Este consiste en tres bits que controlan los mecanismos de notificación de congestión de FR, estos son los bits de FECN, BECN y DE, que son los últimos tres bits del campo de direcciones. El FECN es un campo de un solo bit que puede ser puesto a uno por un conmutador para indicar a un elemento DTE terminal, por ejemplo un enrutador, que se experimentó congestión en la dirección de transmisión de trama, de la fuente al destino. El beneficio primario de usar los campos de FECN y BECN es la capacidad de los protocolos de un nivel superior de reaccionar de forma inteligente ante la presencia de estos indicadores de congestión, actualmente solo los protocolos de DECnet y OSI son los únicos que soportan estas funcionalidades. El BECN es al igual que el FECN un campo de un solo bit, que cuando es puesto a un valor de 1 por un switch, indica que se experimentó congestión en dirección opuesta a la transmisión de la trama de la fuente al destino. Por último el DE es puesto por el elemento DTE, tal como un enrutador, para indicar que el paquete marcado con este bit es de menor importancia en relación con las otras tramas que está siendo transmitidas. Las tramas que son marcadas como desechables deberán ser eliminadas antes que otras tramas en

una red congestionada. Esto permite un mecanismo básico para priorizar las tramas en una red de FR congestionada.

- **Campo de datos.** Contiene encapsulada la data para los protocolos de más alto nivel. Cada trama incluye en este campo de largo variable incluye la data de usuario o campo de carga que variara en largo hasta 1600 octetos. Este campo sirve para transportar el paquete del protocolo de un nivel superior (PDU) a través de una red de FR:
- **Chequeo de secuencia de trama.** Asegura la integridad de la data transmitida. Este numero es calculado por el elemento fuente y verificado por el receptor para asegurar la integridad de la transmisión.

### 2.3.8.6.2 Formato de la LMI

Las tramas de FR que cumplen con las especificaciones de la LMI tienen la estructura mostrada en la figura 26.

**Figura 25. Formato de la LMI.**

| Field length, in bytes |          |                                  |                        |                |              |                      |     |      |  |
|------------------------|----------|----------------------------------|------------------------|----------------|--------------|----------------------|-----|------|--|
| 1                      | 2        | 1                                | 1                      | 1              | 1            | Variable             | 2   | 1    |  |
| Flag                   | LMI DLCI | Unnumbered information indicator | Protocol discriminator | Call reference | Message type | Information elements | FCS | Flag |  |

**Fuente:** [//www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm).

Descripción de los campos:

- **Banderas.** Delimitan el principio y el final de una trama.
- **LMI-DLCI.** Identifica la trama como una trama LMI en lugar de una trama básica de FR. El valor específico de LMI para un DLCI definido por el consorcio de la LMI es DLCI= 1023.

- **Indicador de información sin numerar.** Pone el bit de *poll/final* a cero.
- **Discriminador de protocolo.** Siempre contiene un valor indicando que la trama es una trama LMI.
- **Referencia de llamada.** Siempre contiene ceros, este campo actualmente no es usado para ningún propósito.
- **Tipo de mensaje.** Etiqueta la trama como alguno de los siguientes tipos de mensaje:
  - Identificador de IE. Identifica de manera única al IE.
  - Largo de IE. Indica el largo del IE.
  - Data. Consiste en 1 o más bytes que contienen encapsulada la data de capa superior.
- Chequeo de secuencia de trama (FCS). Asegura la integridad de la data transmitida.

## 2.4 Conceptos básicos de enrutamiento

Enrutamiento es el acto de mover a través de una interconexión de redes, de la fuente de la información hasta su destino, constantemente el enrutamiento es contrastado con el puenteo que para fines prácticos pareciera lograr lo mismo que el enrutamiento. la principal diferencia entre los dos es que el puenteo sucede en la capa 2 del modelo de referencia OSI, en cambio el enrutamiento ocurre en la capa 3 del modelo antes mencionado. Esta distinción entre ambos provee al enrutamiento y al puenteo diferente información para cumplir con su cometido de mover información de un lugar a otro, así las dos funciones cumplen con su cometido de diferente forma.

## **2.4.1 Componentes del enrutamiento**

El enrutamiento consiste básicamente en dos actividades : determinar las rutas optimas para el transporte de grupos de información típicamente llamados paquetes a través de una interconexión de redes y la segunda actividad es llamada conmutación de paquetes, aunque la conmutación de paquetes es un proceso relativamente más fácil que el proceso de hallar la ruta optima, este último puede ser un proceso desafiante como veremos más adelante.

### **2.4.1.1 Determinación de la trayectoria**

Los protocolos de enrutamiento utilizan métricas para evaluar que trayectoria es la mejor para que el paquete o los paquetes puedan viajar a través de la red. Una métrica es un estándar de medida, como el ancho de banda de la trayectoria , que es utilizada por los algoritmos de enrutamiento para encontrar la ruta óptima para transportar la información hacia su destino final. Para ayudarse en el proceso de enrutamiento los algoritmos de enrutamiento crean y mantienen tablas de trayectorias que contienen información de las trayectorias previamente utilizadas.

Los algoritmos de enrutamiento llenan estas tablas con información variada como por ejemplo: Destinos, nodos vecinos, esta información le dice al enrutador que un destino puede ser alcanzada de forma óptima enviándolo a un enrutador determinado que representa el “próximo salto” en el camino a su destino.Los enrutadores se comunican unos con otros y mantienen sus tablas de enrutamiento a través de la transmisión de una variedad de mensajes. El mensaje de actualización de trayectorias es un

mensaje que generalmente consiste en una porción de la tabla de trayectorias de un nodo vecino. Mediante el análisis de las tablas de trayectorias enviados por sus vecinos un enrutador puede construir una imagen detallada de la topología de la red. Otro mensaje común es el del estado de canal, este informa sobre el estado del canal del remitente del mensaje, con este mensaje también puede ser contraída una imagen de la topología de la red y también ayuda a los enrutadores a encontrar la ruta optima para poder enviar un paquete.

#### **2.4.1.2 Conmutación de paquetes**

El algoritmo de conmutación es relativamente sencillo; además es común para la mayoría de los protocolos de enrutamiento. En la mayoría de los casos, un ordenador determina que debe mandar un paquete a otro cliente, habiendo adquirido de alguna manera la dirección del enrutador el ordenador fuente envía un paquete con esta dirección específica, además envía dentro del protocolo la dirección lógica del ordenador destino. Mientras examina la dirección que esta incluida dentro del protocolo el enrutador determina si conoce o desconoce como enviar el paquete a través de la red al siguiente punto de repetición que en este caso sería otro enrutador, típicamente si desconoce como enviarlo este descarta el paquete pero si sabe como enviarlo, el cambia la dirección física que originalmente estaba incluida dentro del paquete por la del siguiente punto de repetición, por otro lado la dirección incluida dentro del protocolo de queda inalterada.

La Organización Internacional de Estándares (ISO por sus siglas en ingles) ha desarrollado una terminología jerárquica que es útil para describir el proceso de conmutación de un paquete entre una unidad fuente y una destino.



Usando esta terminología los dispositivos que no tienen capacidad de reenviar un paquete entre subredes son llamados Sistemas Terminales (ST), mientras que los que si poseen esta habilidad son llamados Sistemas Intermedios (SI),. Los SI son divididos en aquellos que pueden comunicarse en un dominio de enrutamiento y aquellos que pueden comunicarse de las dos formas dentro y fuera de un dominio de enrutamiento. Un dominio de enrutamiento es considerado como una porción de una red bajo una autoridad administrativa común que es regulada por un conjunto de reglas administrativa. Los dominios de son también llamados sistemas autónomos. Con cierto protocolo un dominio puede ser dividido en áreas de enrutamiento.

## **2.4.2 Algoritmos de enrutamiento**

Los algoritmos de enrutamiento se pueden diferenciar por ciertas características claves de funcionamiento. El primer factor seria la clase de objetivos del diseñador de algoritmos estos afectan la operación del protocolo de enrutamiento resultante. Segundo, Existen varios tipos de algoritmos de enrutamiento, y cada algoritmo tiene un impacto diferente en los recursos de la red y del enrutador y finalmente los algoritmos de enrutamiento utilizan una variedad de métricas que afectan el calculo de al ruta optima .

### **2.4.2.1 Objetivos de diseño**

En el diseño de los algoritmos de enrutamiento generalmente se persiguen los objetivos que describen a continuación:

- Optimización
- Simplicidad y un encabezamiento pequeño
- Robustez y confiabilidad

- Convergencia acelerada
- Flexibilidad

Con optimización de recursos nos referimos a la capacidad del algoritmo de seleccionar la mejor ruta, lo cual depende en las métricas y la ponderación utilizada para realizar el cálculo de la ruta.

Los algoritmos deben ser diseñados para ser lo más simples posible. En otras palabras, el algoritmo de enrutamiento debe ofrecer funcionalidad y eficiencia, con el mínimo de software y encabezamiento de paquetes posible. La eficiencia es uno de los factores de más peso por que el algoritmo debe corren en una computadora con recursos limitados.

Los algoritmos debes ser robustos esto quiere decir que deben tener un desempeño correcto aún durante circunstancias inusuales, como fallas de hardware , condiciones de sobre carga e implementaciones incorrectas.

Además de lo mencionado anteriormente los algoritmos deben tener una convergencia rápida. Convergencia es el proceso en el cual todos lo enrutadores involucrados en la red se ponen de acuerdo en cuales son las rutas óptimas para enviar el trafico. Cuando un evento en la red provoca que un enrutador caigo u otro este disponible los demás distribuyen mensajes de rutas actualizados que les permiten recalcular las rutas optimas y eventualmente todos los enrutadores convergen al admitir que estas son las rutas optimas.

Por último los algoritmos deben ser flexibles, lo que significa que deben ser rápidos y certeros al adaptase a una variedad de circunstancias de la red, asumamos que un segmento de la red se perdió. Mientras muchos algoritmos se dan cuenta da la situación, ellos rápidamente seleccionarán el siguiente mejor camino para las rutas que estaban usando ese segmento de

red. Los algoritmos deben tener las opciones para poder programarlos de manera que puedan adaptarse a eventos tales como cambio de ancho de banda, retraso de la red entre otras variables.

### **2.4.3 Tipos de algoritmos**

#### **2.4.3.1 Estático y dinámico**

A los algoritmos estáticos difícilmente se les puede llamar algoritmos, estos no son nada más que tablas de mapeo establecidas por el administrador de red antes de empezar con el enrutamiento. Este mapeo no cambia si no es porque el mismo administrador los altera. Los algoritmos que utilizan rutas estáticas son simples de diseñar y trabajan bien en ambientes donde el tráfico es predecible la mayoría del tiempo y donde el diseño de red es relativamente sencillo.

Debido a que un algoritmo estático no puede reaccionar a los cambios de la red, son generalmente considerados no adecuados para las redes grandes que están en constante cambio. La mayoría de los algoritmos dominantes de hoy en día son del tipo dinámicos que se ajustan a las condiciones de la red mediante mensajes de actualización de rutas. Si el mensaje indica que la red ha sufrido un cambio, el software de enrutamiento recalcula las rutas y envía un mensaje de actualización de las mismas, este mensajes se distribuye en toda la red forzando a los demás a recalcular sus propias rutas y a cambiar sus tablas de acuerdo a la necesidad que se tenga. Estos algoritmos pueden ser complementados con tablas de enrutamiento estático donde sea conveniente. Un enrutador de último recurso o se un enrutador a donde todos los paquetes que no pueden ser enrutados son enviados, por ejemplo, puede ser designado como un deposito para todos

estos paquetes, asegurándose de que todos los mensajes son manejados de alguna manera.

#### **2.4.3.2 Algoritmo de una sola ruta o de múltiples rutas**

Algunos algoritmos sofisticados soportan varios caminos al mismo destino. No así los algoritmos más simples que solo soportan un camino hacia un destino, los algoritmos mencionados primero permiten la multiplexación del tráfico a través de varias líneas. La ventaja de este tipo de algoritmo es que nos permite tener un mejor throughput y confiabilidad. Esto es llamado generalmente compartir la carga.

#### **2.4.3.3 Plano versus Jerárquico**

Algunos algoritmos operan en espacios planos, mientras que otros utilizan jerarquías de enrutamiento. En un sistema de enrutamiento plano, los enrutadores son iguales a los demás, en un sistema de enrutamiento jerárquico algunos enrutadores forman la red primaria de enrutadores. Los demás forman la red secundaria. Los paquetes que provienen de la red secundaria viajan por la red primaria hasta un área destino, en este punto ellos viajan del último enrutador primario y es transportado hacia su destino final por medio de uno o varios enrutadores secundarios.

Los sistemas de enrutamiento muchas veces designan grupos lógicos de nodos, llamados dominios, sistemas autónomos, o áreas. En los sistemas jerárquicos, algunos enrutadores en un dominio pueden comunicarse con otro en otro dominio, mientras que otros solamente lo pueden hacer con otros dentro de su propio dominio. En las redes grandes jerarquías adicionales pueden existir, con los enrutadores más importantes formando el

grupo primario y los demás formando grupos de jerarquías inferiores hasta llegar al destino o ordenador final.

La ventaja principal del enrutamiento jerárquico es que mimetiza la organización de la mayoría de las compañías por lo tanto soporta los patrones de tráfico de una manera más eficiente. La mayoría de las comunicaciones de la red ocurren dentro de pequeños grupos (dominios). Los enrutadores de intra dominio solo necesitan saber de enrutadores dentro su mismo dominio, sus algoritmos de enrutamiento pueden ser simplificados, y, dependiendo del algoritmo que se use, el tráfico generado para refrescar las rutas puede ser disminuido.

#### **2.4.3.4 Cliente inteligente versus enrutador inteligente.**

Algunos algoritmos asumen que el nodo fuente va a determinar la ruta completa, esto es usualmente llamado enrutamiento de fuente. En este caso los enrutadores solo sirven como elementos de almacenamiento y envió, enviando los paquetes al siguiente elemento en la cadena.

Otros algoritmos asumen que el ordenador nos sabe nada acerca de las rutas. En estos algoritmos los enrutadores determinan el camino a través de las conexiones de la red basados en sus propios cálculos, en el primer caso el ordenador es el que posee la inteligencia sobre las rutas mientras que en el último el enrutador es el que toma las disposiciones acerca del camino a tomar.

#### **2.4.3.5 Estado de conexión versus vector distancia**

El algoritmo de estado de conexión (también conocido como el algoritmo del camino más corto primero) inunda de información a todos los nodos de la interred. Sin embargo, cada enrutador, envía solamente una porción de la tabla de enrutamiento que describe el estado de su propia conexión. En este algoritmo cada uno de los enrutadores forma una imagen de toda la red en su tabla de enrutamiento. Por otro lado los algoritmos de vector de distancia (también conocidos como Bellman-Ford) llama a todos los enrutadores para que envíen toda o una parte de su tabla, pero solamente a sus vecinos. En esencia los algoritmos de estado de conexión envían mensajes pequeños de refresco a toda la red, mientras el algoritmo de vector de distancia envía mensajes grandes pero solo a sus vecinos por lo tanto este último solo posee información sobre sus vecinos.

Debido a que convergen más rápido, los algoritmos de estado de conexión son menos propensos a los lazos de enrutamiento que los de vector de distancia. Por otro lado el primer algoritmo consume más recursos de procesamiento que los últimos, por lo tanto los algoritmos de estado de conexión son mucho más caros de implementar y mantener que los de vector de distancia. Los protocolos de estado de conexión son mucho más escalables que los protocolos de vector de distancia.

#### **2.4.4 Métricas de enrutamiento**

Las tablas de enrutamiento contienen información utilizada por el software de conmutación para elegir la mejor ruta. ¿Pero como específicamente son construidas estas tablas? ¿Cual es la naturaleza

especifica de la información que en ellas está contenida? y por último ¿Cómo determina los algoritmos de enrutamiento que una ruta es preferible a otra?

Los algoritmos de enrutamiento han utilizado muchas y diferentes métricas para determinar la mejor ruta. Algoritmos sofisticados pueden basar la selección de la ruta en múltiples métricas, combinándolas en una sola métrica.

Todas las siguientes métricas han sido utilizadas:

- Longitud de tramo
  - Confiabilidad
  - Retardo
  - Ancho de banda
  - Carga y
  - Costo de comunicación
- 
- La longitud del tramo que tiene que recorrer el paquete es la métrica más común. Algunos protocolos permiten a los administradores de la red asignar arbitrariamente costos a cada uno de los enlaces de la red. En este caso, el largo es la sumatoria de todos los costos asociadas con la cantidad de enlaces que tiene que atravesar hasta su destino final. Otros protocolos de enrutamiento definen el conteo de saltos, una métrica que especifica el número de elementos de red que tiene que atravesar, por ejemplo enrutadores, de su fuente a su destino.
  - Confiabilidad, en el contexto de algoritmos de enrutamiento, se refiere a la dependencia (usualmente descrita la tasa de error de bit) que se puede tener de cada uno de los enlaces. Algunos enlaces de la red pueden caerse con más frecuencia que otros. Después de que una red falla algunos enlaces pueden ser reparados más rápido o más fácilmente que otros. Cualquier factor de confiabilidad puede ser tomado en cuenta en la asignación de las medidas de confiabilidad, los

cuales son valores numéricos arbitrarios usualmente asignados a los enlaces por los administradores de la red.

- Retardo de Enrutamiento se refiere al tiempo en total requerido para mover un paquete de su fuente a su destino a través de la Interred. El retardo depende de varios factores, incluyendo el ancho de banda de enlaces intermedios de la red, la colas que existan en cada uno de los enrutadores que exista en el camino, congestión de la red, y la distancia física que exista entre los dos punto.
- Ancho de banda esto se refiere a la capacidad disponible para trafico en un enlace. El ancho de banda es un valor del máximo obtenible del rendimiento de un enlace, las rutas a través de una enlace con una capacidad grande no necesariamente proporcionan una mejor ruta que un enlace más lento.
- Carga, con esto nos referimos en la medida con que un recurso de la red, como un enrutador, esta ocupado. La carga puede ser calculada en una variedad de formas, incluyendo la utilización del CPU y el número de paquetes procesados por segundo.
- Costo de comunicación es otra métrica importante, especialmente porque algunas compañías no toman tan en cuenta el desempeño como toman en cuenta los costos de operación.



## 3 TECNOLOGÍAS DE TRANSPORTE DIGITAL

### 3.1 Introducción

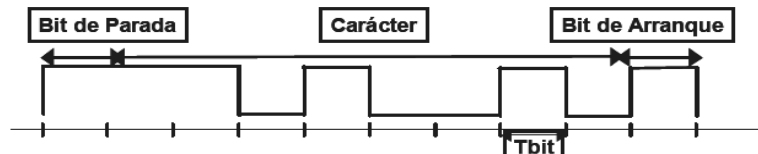
El concepto de transmisión digital es completamente diferente de su contraparte la transmisión análoga. Con la transmisión análoga existía la continuidad, en el caso de la señal digital contrasta con la señal análoga en el sentido de que esta sólo se interesa en estado discretos. La información contenida en una señal análoga es transportada por el valor o magnitud de algunas características de la señal tales como amplitud, frecuencia, o fase de un voltaje; la amplitud o duración de un pulso; la posición angular de una flecha; o la presión de un fluido. Para extraer la información de una señal de esta naturaleza es necesario comparar el valor o magnitud de la señal contra un estándar. La información contenida en una señal digital es concerniente a los estado discretos de la señal, tales como la presencia o ausencia de voltaje, un contacto en la posición de abierto o cerrado, un voltaje en un flanco positivo o negativo, o si una luz está encendida o apagada. La señal obtiene su significado al asignársele valores numéricos u otra información a las posibles combinaciones de los estados discretos de la señal. Los ejemplos de las señales digitales que acabamos de dar en su totalidad son binarios. Por supuesto, en una señal binaria, la señal sólo puede tomar uno de dos valores. Esto es muy útil por diferentes razones. La primera, por supuesto, con un sistema binario, podemos utilizar la numeración en base dos y aplicar la aritmética binaria. La otra buena razón es que podemos utilizar un circuito de decisión donde solamente existen dos posibles condiciones. Nosotros llamamos a estas condiciones uno y cero.

La clave en la principal ventaja de una transmisión digital es el empleo de los circuitos de decisión simple. Nosotros los llamaremos regeneradores. Una señal corrupta entra de un lado, y una señal, limpia y casi perfectamente cuadrada sale del otro lado. El acumulado en la señal corrompida se queda en el regenerador. Esta es la principal desventaja de la transmisión análoga: el ruido se acumula. No siendo así en la transmisión digital.

### **3.2 Sincronismo**

Cuando el modo de transmisión entre dos equipos es asíncrono éstos no tienen un reloj común. Sin embargo es imprescindible que el receptor sepa en qué instante recibe un bit y cuál es la duración del mismo, ya que tiene que recogerlo del enlace para interpretar la información que le está llegando. Para conseguir esta imprescindible sincronización el emisor envía la información en bloques de palabras (o caracteres), cada vez que va a transmitir una palabra nueva envía un bit especial denominado bit de comienzo o arranque, que indicará al receptor que a partir de ese momento va a comenzar a recibir una palabra. Terminada la transmisión de la palabra el emisor envía uno (o varios bits) denominados de final o parada, que indican al receptor que la palabra ha terminado. Como la longitud de la palabra es fija (normalmente 8 bits) el receptor puede leer e interpretar esta información sin problemas y sin la necesidad de compartir un reloj con el emisor. La figura 26 muestra el caso de una transmisión asíncrona. El mayor problema de este mecanismo es la necesidad de insertar bits adicionales de parada y espera que disminuyen el rendimiento de las líneas de transmisión.

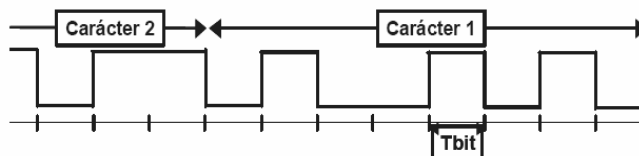
**Figura 26. Método de transmisión asíncrono.**



Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

Cuando el modo de transmisión es síncrono los datos se transmiten con un ritmo fijo, marcado por un reloj o base de tiempo común a los equipos transmisor y receptor. Se denomina sincronismo al establecimiento de este reloj con la finalidad de interpretar adecuadamente las señales recibidas. Cuando existe este sincronismo los equipos involucrados en una transmisión conocen el instante exacto en que debe aparecer determinada información, de este modo las tareas de inserción, recuperación o conmutación de los datos del canal resultan mucho más sencillas. Además no es necesario transmitir bits de arranque y parada para indicar el comienzo y el final de la transmisión, como ocurría con las transmisiones asíncronas. Esto conlleva un mejor aprovechamiento de la capacidad del enlace, ya que toda la información transmitida es útil. La figura 27 muestra el caso de una transmisión síncrona. Como se puede apreciar el receptor conoce dónde comienza y termina cada bit sin necesidad de que el emisor añada ninguna información adicional.

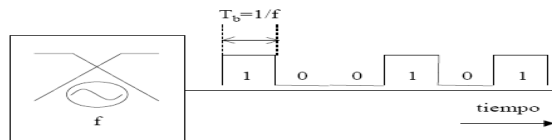
**Figura 27. Transmisión síncrona.**



Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

Todos los componentes de un sistema de transmisión digital necesitan una señal de reloj para su funcionamiento. Utilizando ésta señal se generarán las secuencias de unos y ceros, es decir la información digital, con un régimen binario determinado. La figura 28 muestra como la frecuencia de reloj determinará el tiempo de bit de la señal digital generada por el dispositivo. El comienzo de cada bit vendrá marcado por la fase del reloj. Dentro de un dispositivo, donde las distancias son pequeñas, existe un reloj que proporciona el sincronismo para todos los elementos que lo componen. Así en un computador, o en una central de conmutación, todos los componentes funcionan exactamente a la misma frecuencia. Si las distancias entre los componentes del sistema aumentan, como ocurre en un sistema de transmisión, conseguir un reloj común resulta más complejo y puede requerir de toda una red adicional de sincronización.

**Figura 28. Tiempo de bit determinada por el reloj.**



Fuente:<http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

Para que la transmisión fuera perfectamente síncrona el reloj utilizado para generar la señal transmitida al enlace debería ser exactamente igual, en frecuencia y fase, que el utilizado para leer los datos recibidos. Así el receptor leería los datos con el mismo régimen binario que fueron generados y recogería los datos del enlace justo en el momento apropiado.

### 3.2.1 Relojes imperfectos

Hay que comenzar distinguiendo dos conceptos fundamentales, la frecuencia nominal y la frecuencia instantánea. Los relojes de dos equipos que deben estar sincronizados se ajustan a la misma frecuencia, ésta es la denominada frecuencia nominal. Sin embargo en un instante determinado la frecuencia real que genera el reloj de un dispositivo, la denominada frecuencia instantánea, es muy difícil que sea exactamente igual a la nominal, con lo que dos relojes ajustados a la misma frecuencia nominal es difícil que trabajen a la misma frecuencia instantánea exactamente. Este fenómeno se suele denominar fluctuación o deriva de frecuencia y es debido a las imperfecciones propias de los relojes de manera que depende en gran manera de la calidad de los mismos. Se podría cuantificar como:

#### Ecuación 2.

$$\frac{|f_n - f_i|}{f_n}$$

La primera causa de deriva de frecuencia es la precisión con la que un reloj puede ser sintonizado. Si se puede sintonizar el reloj con una precisión de  $x$  Hz la frecuencia instantánea puede variar hasta  $x$  Hz por debajo o por encima de la nominal. De este modo la diferencia entre las frecuencias instantáneas de dos relojes ajustados a la misma frecuencia nominal puede llegar hasta los  $2x$  Hz desde el momento mismo de la sincronización. La segunda es la estabilidad del reloj, es decir el modo en que éste cambia su frecuencia en un periodo de tiempo como resultado del envejecimiento. Un reloj ajustado a una frecuencia nominal acaba desviándose de ésta y trabajando con una frecuencia instantánea distinta. De este modo la desintonización con cualquier otro reloj que fuera ajustado a la

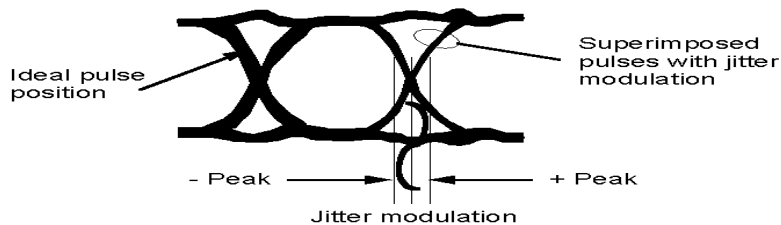
misma frecuencia nominal y que funcione de forma aislada a éste es cada vez mayor.

De esta forma un equipo puede estar generando información usando un reloj de frecuencia  $f_a$  y, en el otro extremo del enlace, se está interpretando la información como si llegara a una frecuencia  $f_a \pm \Delta f$ . Esto es lo mismo que decir que un equipo transmite con un régimen binario de  $R_b$  bps y en el otro extremo se lee a  $R_b \pm \Delta R_b$  bps.

### 3.2.2 Fluctuación de fase

Los términos de *Jitter* y *Wander* son definidos respectivamente como variaciones de de una duración corta y duración larga respectivamente, de la posición del valor significativo de una señal con respecto a su posición ideal en el tiempo. Una forma de ver esto es que una señal digital esta continuamente variado su posición en el tiempo adelantándose y atrasándose, con respecto a una señal ideal de reloj. En la figura 29 se muestra la señal obtenida de un osciloscopio el cual tiene como referencia de disparo la señal de un reloj estable, se puede ver la señal digital claramente afectada moviéndose en torno a la señal de reloj.

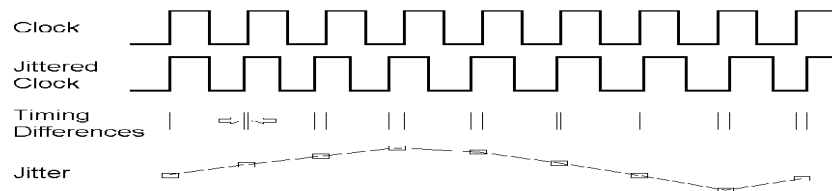
**Figura 29. Desviación en fase de una señal.**



Fuente: <http://www.article-175-highperformancesynchronizationdesignsintransmissionsystems-Asia>.

De hecho, las señales de *Jitter* y *Wander* en una señal de datos son equivalentes a una modulación en fase de la señal de reloj usado para generar la data. Naturalmente, en una situación practica, el efecto de *Jitter* estaría compuesto de un rango grande de frecuencias a diferentes amplitudes.

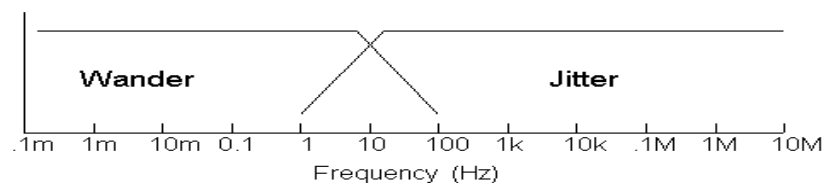
**Figura 30. Variación de fase entre dos señales.**



Fuente:<http://www.article-175-highperformance-synchronization-designs-in-transmission-systems-Asia>.

Ambas señales *Jitter* y *Wander* poseen una amplitud ( esto indica cuanto es que la señal esta cambiando en fase) y frecuencia ( esto indica con que velocidad lo esta haciendo). El efecto del *Jitter* esta definido en estándar de ITU ITU-TG810 como una variación de fase con componentes mayores o iguales a 10HZ, mientras que el *Wander* esta definido como un variación de fase con una rata de frecuencia inferior a 10HZ.

**Figura 31. Rangos de frecuencia de *Jitter* y *Wander*.**

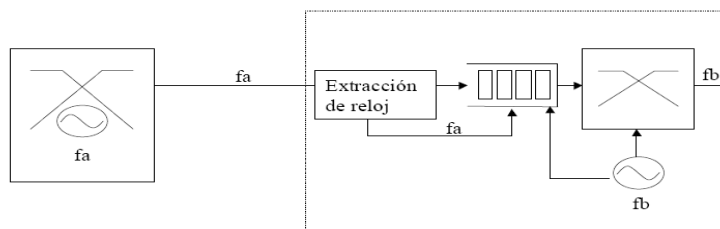


Fuente:<http://www.article-175-highperformance-synchronization-designs-in-transmission-systems-Asia>.

### 3.2.3 Deslizamiento de trama

Una de las primeras medidas para soportar pequeñas desviaciones en la frecuencia instantánea entre un emisor y un receptor separados por un enlace es que el receptor no lea los datos que llegan directamente del enlace si no de un buffer o memoria donde se van almacenando los bits que llegan desde el otro extremo. Así la escritura puede efectuarse a un ritmo, el que marca la frecuencia instantánea del emisor, y la lectura a otro ligeramente distinto, el que marca la frecuencia instantánea del receptor, sin peligro de perder datos. Evidentemente cuanto mayor sea el tamaño de esta memoria mayor será la desviación de frecuencias que se podrá soportar. Normalmente esta variación entre las frecuencias instantáneas que el sistema es capaz de soportar se expresa en partes por millón. Si, por ejemplo, en una línea de 2,048 Mbps se permiten variaciones de 50ppm las variaciones de hasta 200 bps, son soportadas sin que se pierdan ni dupliquen datos. La figura 32 muestra como un nodo que recibe datos con frecuencia  $f_a$  puede enviarlos a un enlace de salida con otra frecuencia  $f_b$ , utilizando también un buffer a la entrada.

**Figura 32. Lectura de datos desde memoria de entrada con reloj propio.**



Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

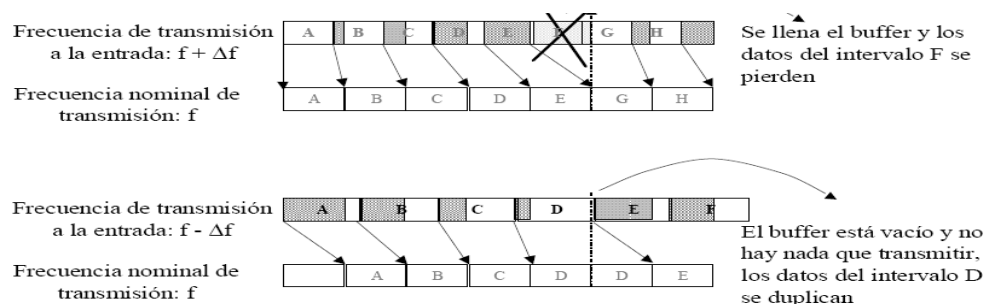
El fenómeno de "Slip" o deslizamiento de trama ocurre cada cierto tiempo en el sistema si existe una diferencia continuada, y en la misma dirección,



entre las frecuencias de entrada y salida de la línea, es decir entre la frecuencia con que se escribe en el buffer y la frecuencia con que se lee de él.

Cada uno de estos deslizamientos implica un error dado que se pierde o inserta información de forma inapropiada. La figura 33 representa lo que ocurre en un equipo de conmutación cuando el régimen binario de entrada al mismo es distinto al régimen binario con el que se leen los datos y se transmiten al siguiente enlace. Se considera la existencia de un buffer a la entrada del conmutador para soportar pequeñas fluctuaciones de frecuencia, sin embargo si la diferencia de frecuencias se mantiene cierto tiempo esta memoria no es capaz de soportar esa variación.

**Figura 33. Variación de frecuencias continuada.**



**Fuente:** [http://www.teleco .upct.es /docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf](http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf).

El primer problema sería que el régimen binario a la entrada de la línea fuera mayor que el de lectura. En esta ocasión el buffer se empieza a llenar con datos que esperan a que les toque su turno para ser recogidos y transmitidos al siguiente enlace. Mientras el buffer no se ha llenado del todo no hay problema, cuando hay que leer algo se recoge de esta memoria. Pero si el buffer se llena los datos que lleguen a continuación se perderán, ya que no tienen donde guardarse hasta que les llegue su turno.

El otro problema sería tener un régimen binario en la línea de entrada menor que el que se utiliza para la lectura de los datos. El contenido del buffer irá disminuyendo de forma gradual, ya que se sacarán los datos más rápidamente de lo que se introducen, cuando se vacíe no habrá nada que transmitir al siguiente enlace. En este caso lo que suele hacer el equipo es volver a enviar la información anterior. Hay que considerar que mientras que las variaciones de velocidad no sean continuadas o no sean siempre iguales, es decir, que unas veces la lectura sea más rápida que la escritura y otras al contrario, el buffer soporta estas variaciones y no ocurriría este fenómeno de deslizamiento de trama.

Además de la utilización de memorias de tamaño adecuado para controlar los deslizamientos existen otras técnicas como las de justificación.

### **3.2.3.1 Justificación positiva**

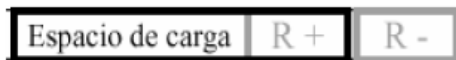
A cada flujo de bits que entra a un nodo se le asigna a la salida del mismo una capacidad algo mayor de la que necesita, los denominados bits de justificación. Si en un momento dado el buffer se vacía se envía relleno en este bit, esto se denomina realizar justificación positiva. Evidentemente será necesario también añadir bits que indiquen al otro extremo si en el bit de justificación va información o relleno para que actúe en consecuencia.

### **3.2.3.2 Justificación positiva/nula/negativa**

Se basa en el mismo principio anterior, pero en este caso hay dos zonas de justificación, positiva y negativa, como indica la figura 34. El flujo de bits tiene un espacio de carga asignado a la salida y dentro de este espacio

está la zona de justificación positiva. Además fuera del espacio de carga está la zona de justificación negativa. Cuando la tasa de entrada a un nodo es justo la nominal a la salida se ocupa justo el espacio de carga y en la zona de justificación negativa se envía relleno (no se realiza ningún tipo de justificación). Si la tasa es superior a la nominal se envía información en el espacio de carga completo y en la zona de justificación negativa (se realiza justificación negativa). Cuando la tasa de entrada es inferior a la nominal se envía relleno tanto en la zona de justificación positiva como en la negativa (se realiza justificación positiva).

**Figura 34. Justificación positiva/nula/negativa.**

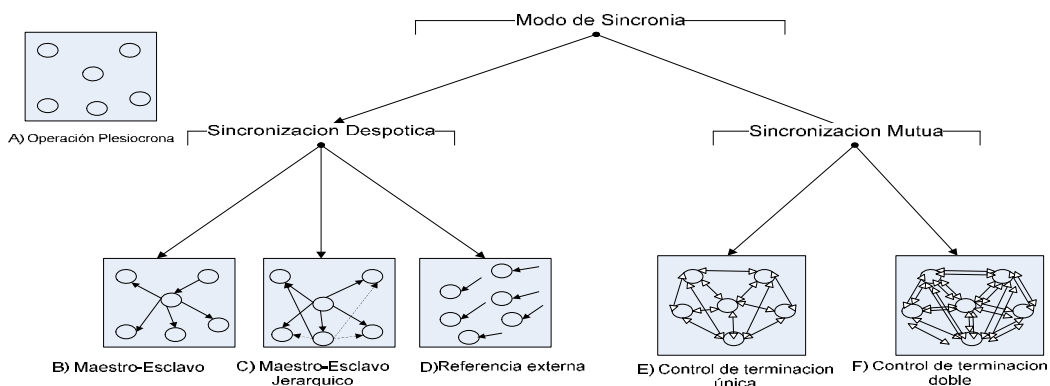


Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

### 3.2.4 Métodos de sincronización de red.

Existen un sinnúmero de métodos que pueden ser implementados para sincronizar una red digital. Seis de estos métodos son mostrados en la figura 35.

**Figura 35. Métodos de sincronización de una red digital.**



Metodos de sincronizacion en una red digital.

En la figura 35.A se ilustra una operación lesiocrona. En este caso cada reloj de cada conmutador está en modo libre. Cada conmutador nodal de la red tiene un reloj de gran estabilidad operando a la misma tasa nominal. Cuando decimos de gran estabilidad nos referimos a un rango de estabilidad de reloj de  $1 \cdot 10^{-11}$  a  $5 \cdot 10^{-15}$  por mes. Esta clase estabilidad sólo puede lograrse con relojes atómicos, de rubidio o de cesio. La precisión y la estabilidad de cada reloj es tal que existe una gran coincidencia de sincronía. Y la desviación de fase entre muchos relojes, es en teoría evitada esto quiere decir que la tasa de deslizamientos es acertadamente baja. Esto requiere que para todos los nodos de conmutación, sin importar que tan pequeños, tengan relojes de alta precisión. Para las telecomunicaciones comerciales esto es de alguna manera una carga de alto costo.

Otro sistema de sincronización es el e sincronización mutua, el cual es ilustrado en la figura e y f. En este caso todos los nodos en la red intercambian referencias de frecuencia, de esa forma se establece una frecuencia de reloj común en la red. Cada nodo hace un promedio de las referencias entrantes y usa el resultado para corregir su reloj local. Después del período de inicialización de la red, el reloj de la red converge a una frecuencia única y estable.

Es importante aquí entender cómo podemos intercambiar referencias de frecuencia. Un método sería tener un canal separado de sincronización conectado a cada uno los nodos en la red. Esto sería un desperdicio de recursos. También podremos hacerlo también podríamos sincronizar el conmutador utilizando los canales de entrada que contienen tráfico sin embargo estos canales entrantes deben derivar de una fuente, la cual tiene un reloj de igual o mayor nivel. Un método para asignar niveles de reloj basado en la estabilidad será descrito posteriormente. La información de sincronía es llevada

transiciones de bit del canal. Un PLL esclaviza el reloj local a estas transiciones. Recordemos que una transición es un cambio de estado en el flujo de bits, un cambio de un uno binario a un cero binario, y viceversa.

Todos los sistemas militares como un número creciente de sistemas civiles usan sincronización externa, como se ilustra en las figuras d. Los relojes de los conmutadores usan un oscilador esclavo de una señal de radio externa. Uno de los más populares hoy en día es el GPS, el cual disemina coordenadas de tiempo universal llamadas un UTC. Este sistema es un sistema de múltiples satélites y funcionan tal manera que existe en tres o cuatro satélites a la vista al mismo tiempo en cualquier punto en la superficie de la tierra. Sus capacidades de transferencia de tiempo están en el rango de 10-ns a 100-ns UTC.

### **3.3 Jerarquías de multiplexación PDH**

En la transmisión de señales digitales se recurre a la multiplexación con el fin de agrupar varios canales en un mismo vínculo. Si bien la velocidad básica usada en las redes digitales se encuentra estandarizada en 64 kbps, las velocidades de los órdenes de multiplexación en cambio forman varias jerarquías.

La jerarquía europea, usada también en Latinoamérica, agrupa 30+2 canales de 64 kbps para obtener 2.048 kbps. Luego, por multiplexado de 4 tributarios sucesivamente, obteniéndose para el segundo orden de multiplexación la velocidad de 8.448 kbps; 34.368 kbps para la tercera y 139.264 kbps para la cuarta.

La jerarquía norteamericana agrupa en cambio 24 canales a una velocidad de 1.544 kbps. Posteriormente genera 2 ordenes superiores el primer

es un múltiplo de 4 del nivel anterior dando como resultado 6.312 kbps y el segundo es un múltiplo de 7 del nivel anterior dando como resultado 44.736 kbps.

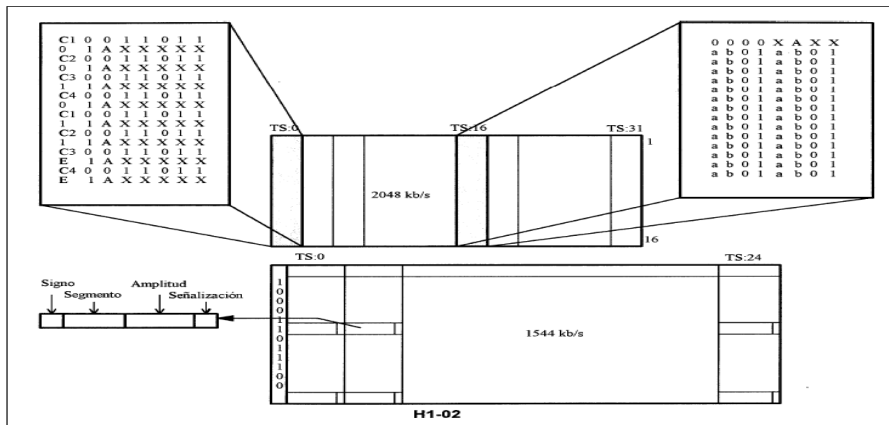
La jerarquía japonesa recupera el valor de 6.312 kbps pero obtiene los órdenes jerárquicos de (x5) 32.064 kbps y (x3) 97.728 kbps.

Las velocidades de cada orden es levemente superior al producto de la velocidad de tributario por el número de entradas, debido al agregado de información adicional. A las jerarquías mencionadas se las denomina Plesiócronicas PDH porque el reloj usado en cada nivel de multiplexación es independiente de los otros niveles. En oposición se encuentra la jerarquía Sincrónica SDH que adopta un solo reloj para toda la red.

### **3.3.1 Primer orden jerárquico trama digital de 2048 kbps.**

La disposición en el tiempo de los canales digitales se realiza mediante la Multitrama MFR (MultiFrame) consistente en 16 Tramas FR (Frame) numeradas desde fila 0 a 15. Cada trama tiene 32 columnas o Intervalos de Tiempo TS, numerados de 0 a 31. Cada intervalo de tiempo lleva un Octeto o Byte de un canal de 64 kbps. En lo que respecta a los tiempos la trama tiene una duración de 125  $\mu$ seg, correspondiente al período de muestreo de una señal telefónica (8 kHz). Cada uno de los 32 intervalos de tiempo dura entonces 3,9  $\mu$ seg y cada bit tiene una duración de 488 nseg. Una multitrama ocupa un tiempo de 2 mseg (Fig 36). El intervalo de tiempo TS:0 se utiliza para enviar el alineamiento de trama e información de supervisión del enlace. El intervalo de tiempo TS:16 se usa para Señalización Asociada al Canal. Los intervalos TS:1 a TS:15 y TS:17 a TS:31 llevan los canales de telefonía digital o datos a 64 kbps. El conjunto de 32 canales (intervalos de tiempo) de 64 kbps constituyen los 2048 kbps.

**Figura 36. Multitrama para la señal E1 a 2048 kb/s y T1 a 1544 kb/s.**



Fuente: <http://www.teleco.upct.es /docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

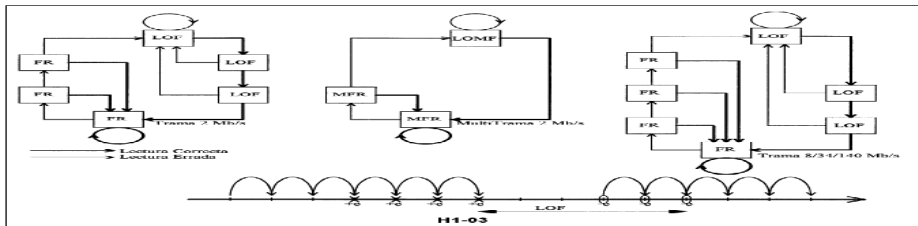
### 3.3.1.1 Lógica de alineamiento de trama

Se trata de la lógica (mediante un diagrama de estados finitos) usada para reconocer la palabra de alineamiento de trama **FR** (Fig 37). Supóngase partir del estado de no alineamiento LOF. Para llegar al estado de alineamiento de trama, el receptor debe reconocer consecutivamente las palabras FR-NFR-FR. Luego de ésta última palabra FR comienza el estado de alineamiento de trama. Para perder el alineamiento LOF, el receptor debe recibir con error la secuencia FR-FR-FR o la secuencia NFR-NFR-NFR en forma consecutiva. La palabra FR es [x001 1011] y la palabra NFR es [x1xx xxxx], ya que los restantes bits (x) tienen otras aplicaciones.

Durante el tiempo de alineamiento el receptor solo observa el estado de los bits cada 125 µseg, es decir cada 256 bits. En tanto se tenga pérdida de trama **LOF** se deben estudiar la totalidad de los bits recibidos para reconocer la palabra FR.

Además se reemplazan los intervalos de tiempo TS que llevan información de canal por una **Señal de Indicación de Alarma AIS**, consistente en una secuencia continua de bits 1. Por otro lado, el receptor induce al transmisor para colocar el bit A=1 en la palabra NFR de alineamiento. Este bit oficia de alarma remota de pérdida de trama del terminal correspondiente.

**Figura 37. Lógica utilizada para reconocer la palabra de alineamiento de trama.**



Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentación /PDH.pdf>.

El bit C se utiliza para enviar una trama de **Control de Redundancia Cíclica CRC-4**, que actúa como bits de paridad para el control de la tasa de error. La secuencia que se coloca en el bit C es:

C1 0 C2 0 C3 1 C4 0 C1 1 C2 1 C3 E C4 E

Donde la secuencia 001011 es la palabra de alineamiento para la trama CRC. Los bits C1..C4 se calculan mediante el criterio de redundancia cíclica como bits de paridad para la detección de errores. Los bits E actúan como alarma remota de recepción de errores. Como una multitrama tiene 2 secuencias CRC-4 se disponen de 2 bits E (uno para cada secuencia CRC).

El polinomio generador de los bits de paridad es  $X^4+X+1$ . Se efectúan 1000 comparaciones CRC-4 por segundo. Se puede emitir la alarma de tasa de



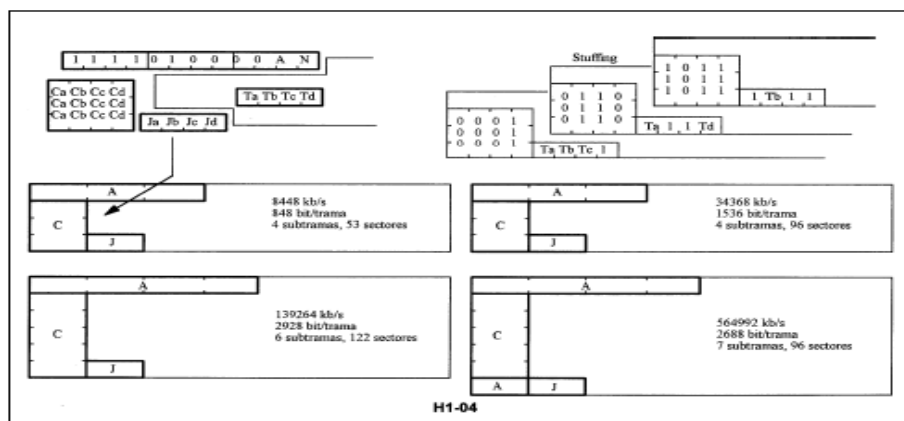
error o pérdida de trama LOF cuando se supera un umbral de comparaciones erróneas.

**Tabla II. Ordenes jerárquicos plesiócronicos**

| Jerarquía Europea        | Denominación | Velocidad   | Canales | Trama               |
|--------------------------|--------------|-------------|---------|---------------------|
| Primera                  | E1           | 2048 kbps   | 30      | 256 bit = 125 c     |
| Segunda                  | E2           | 8448 kbps   | 120     | 848 bit = 100,38µs  |
| Tercera                  | E3           | 34368 kbps  | 480     | 1536 bit = 44.70 µs |
| Cuarta                   | E4           | 139268 kbps | 1920    | 2904 bit = 20.85µs  |
| Quinta                   | E5           | 564992 kbps | 7680    | 2688 bit = 4.7µs    |
| Jerarquía Norteamericana |              |             |         |                     |
| Primera                  | DS1          |             | 24      |                     |
| Segunda                  | DS2          |             | 96      | 1176 bit            |
| Tercera                  | DS3          |             | 674     | 4760 bit            |

El primer orden jerárquico se multiplexa sucesivamente para obtener mayores velocidades y una multiplicación de la capacidad. La jerarquía plesiócrona correspondiente a 2048 kbps multiplexa en pasos de 4 entradas (tributarios de nivel inferior) para obtener la jerarquía superior.

**Figura 38. Trama y proceso de justificación en PDH.**



Fuente: <http://www.teleco.upct.es/docencia/material/t3/sistele/Tema3/Documentacion/PDH.pdf>.

### 3.3.2 Tramas de orden superior

En la figura 38 se observan las tramas digitales para los niveles jerárquicos a partir del segundo orden. Si bien el número de canales se multiplica por 4 a cada paso, la velocidad es levemente mayor a 4 debido al agregado de señales adicionales. Se describe en detalle el orden segundo ya que el resto son una extensión conceptual de aquel. Basta con observar la similitud de tramas.

#### 3.3.2.1 Trama digital de 8448 kbps

Al multiplexor de segundo orden ingresan 4 tributarios de 2048 kbps cada uno, cuya velocidad tiene una tolerancia de  $\pm 50$  ppm (equivalente a  $\pm 102,4$  b/s). La trama consiste en 848 bit/trama y se encuentra dividida en 4 subtramas de 212 bit; cada una se divide en 53 grupos de 4 bits. Al inicio de la trama se tiene un encabezado (*overhead*) con información de alineamiento de trama, alarma, bits de justificación positiva (*Stuffing*) y bits de control de justificación. La justificación positiva permite entrelazar 4 entradas denominadas tributarios de distinta velocidad dentro de la tolerancia de 50 ppm.

La palabra de alineamiento de trama consiste de 10 bits (1111 0100 00AN) y permite el sincronismo del receptor. La pérdida de alineamiento de trama LOF se produce cuando se detectan con error 4 palabras consecutivas. Para la recuperación del alineamiento se deben leer correctamente 3 palabras consecutivas. En la figura 37 se representa en forma gráfica el criterio de alineamiento de trama. En tanto dura la falta de alineamiento, la señal de los tributarios se reemplaza por una señal de indicación de alarma AIS consistente en una secuencia de bits 1.

El bit N de la palabra de alineamiento se encuentra reservado para uso nacional (si no se usa se coloca un bit 1); aplicado para alarma de BER remota. El bit A oficia de alarma distante al terminal remoto durante el tiempo de falta de alineamiento de la trama (A=1 para alarma y A=0 en estado normal). Los datos provenientes de los tributarios se entrelazan por bits en la zona denominada carga útil de la trama. Se observa que el proceso de multiplexación es transparente a la organización de la trama del orden jerárquico inferior. Es decir, la información del tributario de entrada solo debe cumplir con los requisitos de velocidad, nivel y código; sin importar la organización interna de los datos.

La velocidad de los tributarios de entrada es de 2048 kbps como valor nominal y con tolerancia de  $\pm 50$  ppm ( $\pm 102$  b/s). El entrelazado de 4 afluentes de entrada cuya velocidad puede no ser exactamente igual (funcionamiento plesiócrono) requiere entonces de la aplicación del proceso de Justificación Positiva. El mismo consiste en asignar a cada afluente una capacidad levemente superior a la real y rellenar el exceso con bits de justificación (*stuffing*) que se eliminan en el proceso de demultiplexación.

### **3.3.2.2 Ordenes jerárquicos superiores**

Por encima de los 8448 kbps se encuentran el tercer y cuarto orden jerárquico. El quinto orden se ha determinado para aplicaciones con interfaz para fibras ópticas. De acuerdo con la Fig. 38 la organización de las tramas es similar. Se disponen de palabras de alineamiento de trama al inicio de cada organización de iguales características. Siempre se dispone de una alarma para informar al terminal remoto de la falta de alineamiento local. El proceso de justificación positiva es conceptualmente idéntico. El número de bits de control de justificación es 3 o 5 para corregir 1 o 2 errores.

### 3.3.3 Proceso de justificación

La Justificación permite interrelacionar señales de datos generadas por relojes distintos (plesiócronicos). Un caso interesante de justificación de relojes es el día bisiesto (29 de febrero) del calendario.

Es usado en los órdenes jerárquicos plesiócronicos y sincrónicos. Se han identificado tres grupos de cuatro bits denominados Control de Justificación Cj y un grupo de cuatro bits denominado Oportunidad de justificación J. Cada bit de cada grupo pertenece a uno de los cuatro tributarios. Cada trama tiene 848 bits que distribuidos en 4 tributarios corresponde a 212 bit. La palabra de alineamiento ocupa 3 bit de cada tributario (12 en total) y el control de justificación otros 3 bits.

Lo cual determina que cada tributario disponga de 206 bit en cada trama. La velocidad de la jerarquía es de 8448 kbps y con los 848 bit/FR en la trama, se disponen de 9962 FR/s. Si ahora tenemos en cuenta que cada tributario de entrada tiene 206 bit/FR se llega a un valor de 2052 kbps.

La capacidad reservada en la trama para cada tributario es superior a la requerida. Por lo tanto, se rellenan periódicamente los espacios de justificación con bits 1 para equilibrar las velocidades. Si todos los espacios J son justificados (rellenados con bits 1) la velocidad resultante de cada tributario es de 205 bit/FR, es decir 2042 kbps; inferior a la velocidad requerida. Para acomodar 2048 kbps, aproximadamente 6 de cada 10 bits J llevan información del tributario y 4 son rellenos (justificados). Para que el receptor determine cuales de los bits J llevan un relleno se envían los bits de control Cj correspondientes al tributario en la condición 1; si en cambio, se transmite información los Cj corresponden a 0. Es decir:

- si  $C_j = 000$  en J se lleva un dato del tributario,
- si  $C_j = 111$  en J se coloca un relleno (bit 1).

Los bits  $C_j$  se repiten 3 veces con el propósito de corregir un error determinando la validez por mayoría de ceros o de unos. Si se comete un error en el receptor con respecto al valor de  $C_j$  se produce un deslizamiento en la señal del tributario. En otras palabras, si se transmite  $C_j=0$  y se recibe  $C_j=1$  el receptor interpreta al dato que se encuentra en J como un relleno y lo elimina de la trama de 2048 kbps. Si en cambio, se transmite  $C_j=1$  y se recibe  $C_j=0$  el receptor interpreta como dato un relleno y agrega un bit en la trama. En ambos casos, al eliminar o agregar un bit, la trama del afluente de 2048 kbps se desplaza y el nivel jerárquico correspondiente pierde el alineamiento de trama.

Un error de interpretación del bit  $C_j$  del nivel de 8448 kbps produce una pérdida de alineamiento de trama en 2048 kbps. Por ello el bit  $C_j$  está protegido, mediante la repetición, contra un error. Existen 4 controles  $C_j$  (se repiten 3 o 5 veces cada uno) asignados a cada uno de los 4 tributarios. El funcionamiento de los  $C_j$  y J es independiente para cada tributario. El estado de ellos en cada trama se determina mediante una memoria variable asignada a cada entrada de afluente.

### **3.4 Fundamentos de SDH**

Los sistemas de transmisión análogos ya establecidos de primera mano, han sido reemplazados gradualmente por redes de comunicación digital, en un principio en muchos países, la transmisión digital fueron desarrolladas basadas en estándares conocidos hoy como Jerarquía Digital Plesiócrona (PDH) descrita en párrafos anteriores .

Aun teniendo numerosas ventajas sobre las líneas análogas la tecnología PDH posee algunos inconvenientes: El hecho de aprovisionar un circuito representa un consumo de recursos de tiempo y trabajo exagerado, las capacidades de automatización y control centralizado de las redes es limitado y además la actualización a nuevas tecnologías es demasiado engorroso, la mayor desventaja de este tipo del es que los estándares existen para las interfaces eléctricas a las ratas de PDH pero para las interfaces ópticas no existe este tipo de estandarización, esto significa que cuando se usan equipos de diferentes vendedores es posible que esto no se puedan interconectar.

La reconfiguración de una red PDH es muy elaborada dando como resultado costos elevados y tiempos de indisponibilidad demasiado grandes cuando se quiere la introducción de nuevos servicios o un cambio de ancho de banda en un servicio y a existente la situación fue particularmente difícil en norte América , donde un sistema Plesiócrono (T) estaba instalado.

En 1985 se propuso una nueva jerarquía la cual tenía como mayor objetivo crear un sistema síncrono con una interfaz óptica compatible con múltiples fabricantes, dentro de la standardización también se incluía una estructura flexible de trama capaz de manejar tanto las señales existentes como nuevas señales, además numerosas funciones contenidas dentro de la cabecera de la señal, para administración, mantenimiento y aprovisionamiento este nuevo sistema fue llamado Red Óptica Síncrona (SONET). La Unión Internacional de Telecomunicaciones (ITU) estableció y estándar internacional basado en las especificaciones del SONET, conocido como Jerarquía Digital Síncrona (SDH).

Uno de los mayores beneficios del SDH es que permite a múltiples fabricantes de equipos de transmisión ópticos interconectar sus equipos

entre sí sin ningún problema de compatibilidad, esta tecnología permite el proceso de agregar y remover información en la trama de transmisión sea dinámico, en el caso de los operadores PDH de para realizar la operación antes mencionada tenían que demultiplexar y remultiplexar la señal a alta velocidad provocando retardos y requiriendo hardware adicional. Debido a que la cabecera es independiente de la carga, SDH integra nuevos servicios, tales como ATM (*Asynchronous Transfer Mode*) junto con los servicios de PDH existentes de 2, 34 y 140 Mbps en Europa y 1.5, 6.3 y 45 Mbps en Norte América.

### **3.4.1 Multiplexión de SDH**

La multiplexión en SDH combina señales de baja velocidad tales como 2.048 y 140 Mbps para formar una trama llamada Modulo de Transporte Síncrono a nivel 1 (STM-1) la trama de STM-1 esta conformada por 9 segmentos de 270 bytes cada una. Los primeros 9 bytes de cada segmento portan la información de cabecera, los restantes 261 bytes portan la información como tal. Cuando es visualizado como bloque la trama STM-1 aparece como 9 filas y 270 columnas de bytes. La transmisión de la trama STM-1 inicia con la fila 1, con los bits más significativos de cada byte transmitidos primero.

Esta formula calcula la rata de BIT de una señal digita tramada:

Rata de BIT = rata de trama \* capacidad de trama.

Con la finalidad de integrar fácilmente servicios digitales ya existentes en la nueva jerarquía, esta opera a una rata básica de 8Khz o 125 microsegundos por trama, así la rata de trama de es de 8,000 tramas por

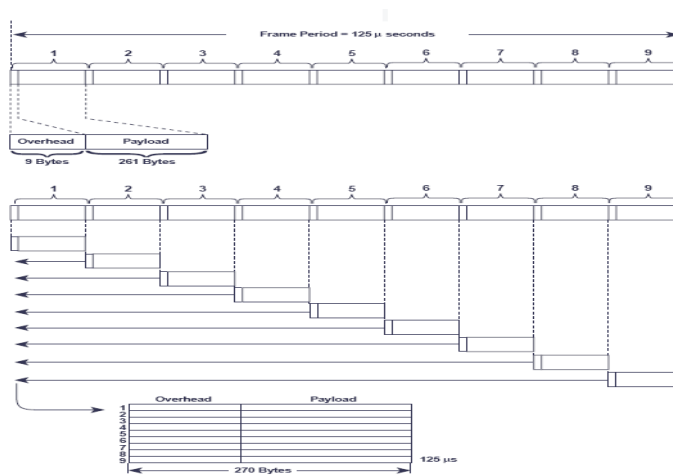
segundo. La capacidad de trama de una señal es el número de bits contenidos dentro de una trama:

Capacidad de trama = 270 bytes/fila \* 9 filas /trama= 19,440 bytes/trama

La rata de bits del STM-1 es calculado como sigue:

Rata de bit= 8,000 trama/segundo \* 19,440 bytes/trama  
 = 155.52 Mbytes/s

**Figura 39. Trama STM-1.**

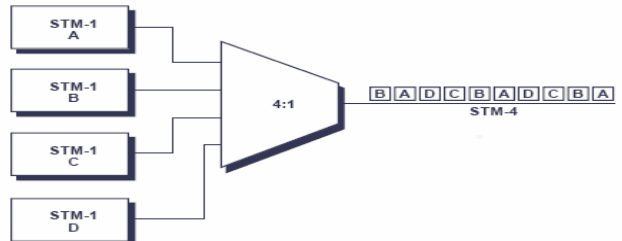


Fuente: [www.syrus.ru/files/docs/control/tech/SDH.pdf](http://www.syrus.ru/files/docs/control/tech/SDH.pdf).

Han sido definidos cuatro niveles de transmisión (STM-1, STM-4, STM-16 y STM-64) para la jerarquía SDH como lo muestra la figura 40, la ITU ha especificado que un STM-4 deberá ser creado a partir de 4 señales STM-1. La rata básica de trama permanece a 8,000 tramas por segundo, pero la capacidad se ha cuadruplicado, resultando en una rata de bit de 4\*155.52 Mbps, o 622.08 Mbps. La señal de STM-4 puede ser multiplexada con otras 3 STM-4 para formar una señal STM-16.



**Figura 40. Multiplexión de señales STM 1.**

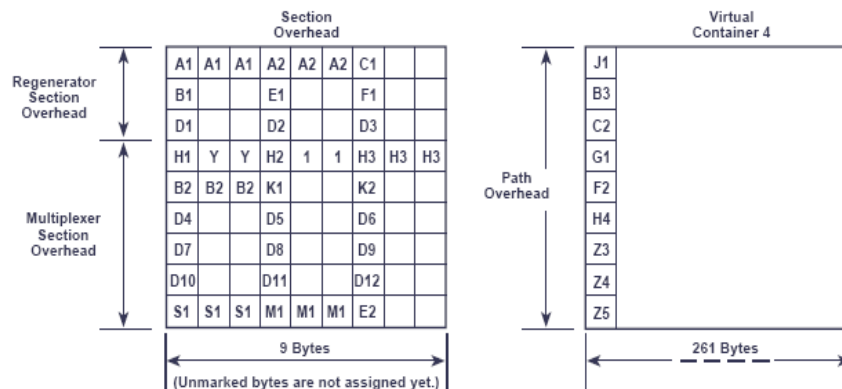


Fuente: Newall, Christopher, *Sistemas De Transmisión Sincrónica*.

### 3.4.2 La trama SDH

En la figura se muestra la trama SDH dividida en dos partes para separar físicamente donde cuadro representa un bite de 8 bits. Las primeras nueve columnas comprenden cabecera de sección (SOH), mientras el resto es llamado contenedor virtual nivel 4 (VC-4), la SOH dedica tres filas para la cabecera de sección de regeneración (RSOH) y seis filas mas para la cabecera de sección de multiplexión (MSOH). El VC-4 contiene una columna para su cabecera de ruta (VC-4POH), dejando las restantes 260 columnas para datos (149.76 Mbps).

**Figura 41. Encabezado básico de la trama STM-1.**



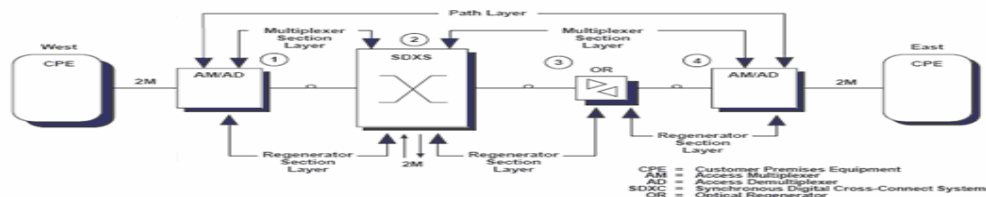
Fuente: Newall, Christopher, *Sistemas de Transmisión Sincrónica*.

### 3.4.3 Jerarquía de la señal SDH

La señal SDH esta constituida en capas para dividir responsabilidad por transportar la carga de datos a través de red. Cada elemento de red SDH (ER) es responsable de interpretar y generar su cabecera de capa, y de comunicar información de control y estatus a otros equipos en la misma capa, o terminar su cabecera de capa. Mientras viaja por la red, cada capa es terminada por un ER denominado equipo terminal de sección de regeneración (RSTE), equipo terminal de sección de multiplexión (MSTE), equipo terminal de ruta (PTE). La figura 42 muestra una red de ejemplo con las funciones de capa identificadas. La POH es generada en donde la señal de baja velocidad no SDH entra en la red SDH mediante un PTE, por ejemplo un multiplexor de acceso (AM).

La POH es removida cuando la carga de datos sale de la red SDH por medio de un PTE, como por ejemplo un demultiplexor de acceso (AD). La POH es de modalidad primero en entrar, ultimo en salir, de manera que la información de errores y alarmas contenida dentro de esta capa reprenda un estatus de punto a punto.

**Figura 42. Red de comunicación típica basada en capas.**



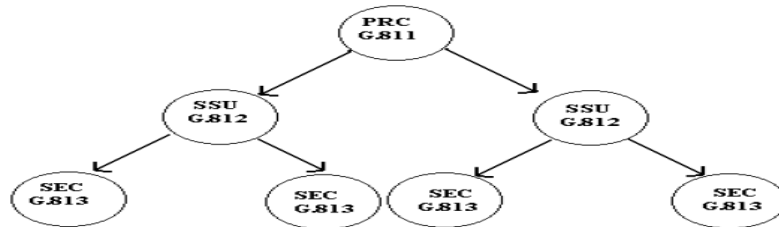
Fuente: [www.syrus.ru/files/docs/control/tech/SDH.pdf](http://www.syrus.ru/files/docs/control/tech/SDH.pdf)

La siguiente capa de terminación de cabecera es la MSOH y es realizado por medio del MSTE , por ejemplo un multiplexor síncrono (SM), un sistema de interconexión (SDXS), un AM , o un AD. La MSOH es donde la mayor parte de la comunicación y sincronización sucede entre los nodos principales además monitorea la información de errores entre los nodos principales de la red. Finalmente, RSOH es terminada por un RSTE, por ejemplo un regenerador óptico, y contiene información de errores cada nodo de la red SDH. Como la figura 42 muestra, las funciones de MSTE, PTE Y RSTE puede algunas veces estar combinada dentro de un mismo equipo. Debido a que cada capa es terminada y regenerada en los nodos apropiados, el monitoreo de desempeño en cada nodo de la red ayuda a sectorizar los problemas.

#### **3.4.4 Sincronización**

Como ya sabemos, SDH significa jerarquía digital síncrona y es muy importante que sea realmente síncrona. Si no se garantiza la sincronización puede producirse una degradación considerable en las funciones de la red e incluso el fallo total de la red. Para evitarlo todos los elementos de la red están sincronizados respecto a un reloj central, generado mediante un reloj de referencia primario (PRC) de alta precisión conforme a la Recomendación G.811 de la UITT, que especifica una precisión de  $1 \times 10^{-11}$ . Esta señal de reloj debe distribuirse por toda la red. Para ello se recurre a una estructura jerárquica, siendo las unidades de sincronización (SSU) y los relojes de equipos síncronos (SEC) quienes transfieren la señal. Las señales de sincronización circulan por los mismos circuitos que las comunicaciones SDH.

**Figura 43. Estructura jerárquica de la distribución de la señal de reloj.**



Fuente: Newall, Christopher, Sistemas de transmisión sincrónica.

La señal de reloj se regenera en las SSU y en los SEC con la ayuda de bucles enganchados en fase (PLL). Si falla la fuente de reloj, el elemento afectado conmuta a otra fuente de reloj de igual o menor calidad o, si esto no fuera posible, pasa al modo vestigial. En esta situación, la señal de reloj se mantiene relativamente precisa controlando el oscilador aplicando valores de corrección de frecuencia almacenados durante las últimas horas y teniendo en cuenta la temperatura del oscilador. Deben evitarse a toda costa las "islas de reloj" ya que, con el transcurso del tiempo, podrían llevar a la pérdida del sincronismo y al fallo total de la red.

Tales islas se evitan comunicando los elementos de la red con la ayuda de mensajes de estado de sincronización (SSM, parte del byte SI). El SSM informa al elemento vecino sobre el estado de la fuente de reloj utilizada para generar la señal por este recibido y es parte de la cabecera de sección de multiplexación.

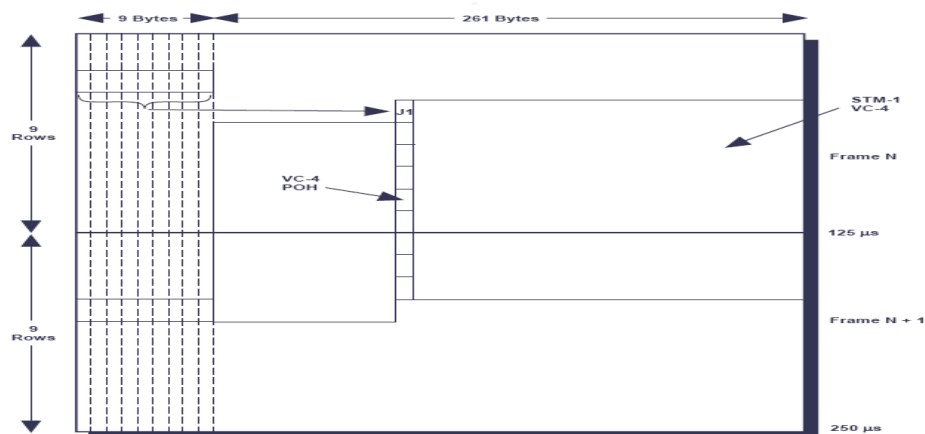
Las pasarelas entre redes con fuentes de reloj independientes plantean algunos problemas especiales. Los elementos de redes SDH pueden compensar desplazamientos de reloj hasta ciertos límites mediante operaciones con punteros. La actividad de los punteros es un buen indicador de los problemas con la fuente de reloj.

### 3.4.4.1 Compensación de sincronía en SDH

La señal de SDH fue diseñada para que pudiera tolerar variaciones de sincronía para contener las señales de PDH, señales que por lo general son mucho más lentas, y además poder soportar pequeñas variaciones de sincronía entre los NE de SDH. Existen dos mecanismos que permiten una compensación robusta de sincronía: Justificación variable de bit para señales de tasa más baja de datos, y una técnica llamada ajuste de apuntador entre elementos síncronos en la red de SDH.

El ajuste de apuntador le permite al VC-4 flotar con respecto a la trama de SDH. Esto significa que una simple trama de VC-4 típicamente cruza los bordes de la trama del STM-1 como lo muestra la figura 44.

**Figura 44. Bytes puntero marcando el inicio de la cabecera de POH del VC4.**



Fuente: Newall, Christopher, Sistemas De Transmisión Síncrona.

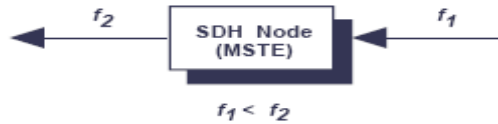
Este apuntador está contenido en los bytes de la MPOH, y no son más que un contador de la distancia que existe en bytes entre VC-4POHJ1

y el H3, sin incluir los bytes de cabecera de sección. Un puntero válido de VC-4 puede variar entre 0 a 782.

Cuando existe una diferencia de sincronía, bytes de relleno pueden ser insertados dentro de VC-4 sin afectar los datos. Debido que el puntero es ajustado para indicar donde la POH real comienza, el receptor puede recuperar efectivamente la carga de datos. Cuando se usan bytes de justificación se usan siempre en el mismo lugar sin importar donde comience la POH. Los bytes de H3 son llamados bits de justificación negativa y contienen datos reales por una trama durante un decremento de apuntador. Los tres bytes que siguen al último byte de la H3 en el VC-4 son llamados bytes de justificación positiva y contiene tres bytes de relleno por trama durante un incremento de apuntador.

Si no existiera diferencia de sincronismo entre dos nodos, la tasa de bit del STM-1 entrante es idéntica a la trama del nodo que la emitió de tal manera que no son necesarios los ajustes de apuntadores la figura 45 muestra un nodo SDH que tiene una frecuencia de entrada  $f_1$  y una de salida  $f_2$ . Si  $f_1$  es menor que  $f_2$ , existe un faltante en el área de datos en la trama STM-1 saliente. Para compensar, tres bytes tontos son puestos en los bytes de relleno positivo los datos son movidos a la derecha por tres bytes, así el contador del VC-4 es incrementado por uno, por otro lado si  $f_1$  es más grande que  $f_2$ , entonces tres bytes extras de VC-4 son guardados en los bytes negativos de relleno, H3, en la MSOH para una trama, mientras toda el área de datos es movida al a izquierda tres bytes y el puntero es decrementado en uno.

**Figura 45. Nodo SDH con frecuencias de entrada y salida diferente.**



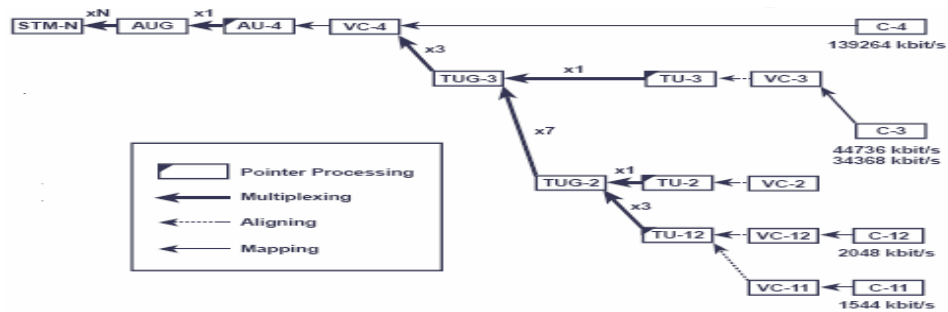
Fuente: [www.syrus.ru/files/docs/control/tech/SDH.pdf](http://www.syrus.ru/files/docs/control/tech/SDH.pdf).

El único equipo que puede realizar la tarea de ajustar el puntero de ruta es el MSTE, debido a que el valor del puntero está contenido dentro de la MSOH. Además, los ajustes de puntero de ruta no son realizados por el PTE, aunque puedan existir diferencias de sincronía en estos puntos de la red.

### 3.4.5 Mapeo de tributario asíncronos en la trama STM-1

Una señal STM-1 puede ser formada a partir de algunas de las jerarquías PDH solamente, se eligieron cuatro velocidades tratando así de que por lo menos alguna de las jerarquías que cada país tenía, tenga cabida dentro de la trama STM-1.

**Figura 46. Mapeo de tributarios en una trama STM-1.**



Fuente: Newall, Christopher, Sistemas De Transmisión Sincrónica.

En la figura 46 muestra el mapeo que se hace para llegar de una señal de jerarquía PDH a una señal básica de SDH, una trama STM-1.

Tomando como ejemplo la velocidad de 2Mb/s se ve que tomando 3 TU (Unidades Tributarias), se forma un TUG2 (Grupo de Unidades Tributarias de orden 2), agrupando 7 TUG, se forma una AU3 (Unidad Administrativa de orden 3), y por último agrupando 3 AU3, se forma una AUG (Grupo de Unidades Tributarias), a la cuál agregándole el SOH, forma la trama STM-1. A medida que se va armando la trama se van agregando a la carga útil, los diferentes identificadores y canales de cabecera. Se podría pensar la trama como si tuviera una estructura de cascarón, es decir que cada etapa va sumando una capa a este cascarón imaginativo.

A continuación se explica con más detalle cada una de estas etapas

**Contenedor C.** Toda información útil, ya sea plesiócrona o síncrona, se coloca en contenedores antes de ser transmitida en una STM-1. Por contenedor C se entiende una capacidad de transmisión definida y síncrona a la red. El tamaño de los contenedores se indica en Bytes, esta cantidad de bytes se pone a disposición como capacidad de transmisión en contenedores cada 125 us. Los tamaños de los contenedores establecidos corresponden a las señales plesiócronas actuales. En la siguiente tabla se distinguen los siguientes tamaños de contenedores.

**Tabla III. Contenedores de SDH**

| DENOMINACION | SEÑAL A TRANSMITIR |
|--------------|--------------------|
| C-11         | 1544Kb/s           |
| C-12         | 2048Kb/s           |
| C-2          | 6312Kb/s           |
| C-3          | 44736Kb/s          |
| C-3          | 34368Kb/s          |
| C-4          | 139364Kb/s         |



La información útil debe caber en estos contenedores, por lo tanto en las señales, esto se logra mediante un relleno de bits y bytes, para el cual se emplea tanto el procedimiento de relleno puramente positivo como el de relleno negativo-cero-positivo.

El contenedor contiene:

a) Información útil (por ej la señal PDH)

b) Bytes y bits de relleno fijos (*fixed stuffing*) para la adaptación basta del reloj. Estos rellenos, son siempre Bytes (bits) sin información para adaptar la velocidad PDH aproximadamente a la velocidad del Contenedor, que suele ser mayor. La adaptación más precisa se efectúa por medio de bits rellenables individuales.

c) Bits rellenables para la adaptación precisa del reloj. Según sea necesario, estos bits pueden usarse como bits de información útil o bien como bits de relleno.

d) Bits de relleno para comunicar al destinatario si el bit rellenable tiene información útil o es simplemente de relleno, permitiendo así al destinatario saber si debe tener en cuenta los bits de relleno o debe descartarlos.

**Contenedor Virtual.** A cada contenedor C se le agrega un Encabezado de camino (POH), luego el contenedor junto con el POH correspondiente forma lo que se denomina el Contenedor Virtual (VC), y se transporta como unidad inalterada a través de una ruta interconectada en la red.

El POH consiste en informaciones que sirven para transportar de manera confiable el contenedor desde el origen hasta el destino. El POH se agrega al formar el VC al principio de la ruta y se evalúa solo al final de ésta, en el

momento que se descompone el Contenedor, entonces el POH contiene información para supervisión y mantenimiento de una ruta interconectada en la red.

Un VC puede (según el tamaño) transmitirse en una trama STM-1 o bien, depositarse en un VC mayor, el cuál se transporta luego directamente en la STM-1. Se hace una distinción entre VC de orden superior (HO Higher Order), y VC de orden inferior (Lower Order ). Se conocen como LO aquellos que se transmiten en contenedores “más grandes”. Los VC11, VC12, VC 2, son del tipo LOVC. El VC 3 es un LOVC cuando es transmitido en un VC4. Los HO son aquellos que se transmiten directamente en la trama STM-1, por ej el VC4 e un HOVC, esto es valido también para el VC3 que se transmite directamente en la trama STM.

**Unidad Administrativa.** Los contenedores virtual VC4 y VC3, son transmitidos directamente en la trama STM-1, en este caso los apuntadores de bloque PTR AU incorporados en la trama STM-1 contiene la relación de fase entre la trama y el virtual contenedor respectivo. La parte de la trama dentro de la cuál puede deslizarse el VC se denomina “Unidad Administrativa”, también el puntero denominado PTR AU, forma parte de la AU. En los primero 9 bytes del cuarto renglón de la trama STM-1 están contenidos 3 punteros de 3 bytes cada uno.

Se debe hacer una distinción entre las AU4 y AU3. En la trama STM-1 pueden transmitirse, 1 x AU4, o bien 3 x AU3. Vale la pena aclarar que la transmisión del VC3 puede efectuarse directamente (AU3), en la STM-1 o indirectamente, en un AU4, por lo cual se depositan 3 VC Dentro de un VC4.

**Grupo de Unidades Administrativas.** Varias AU pueden agruparse, o sea multiplexarse, por bytes para formar el llamado grupo AU (AUG). El grupo AUG es una unidad con sincronía de trama que corresponde al STM-1 sin la SOH. Agregando la SOH –STM1 al AUG se obtiene un STM-1. Un grupo AUG puede constar entonces, de 1 x AU4 ó de 3 x AU3.

**Unidad Tributaria.** Todos los VC's, excepto el VC4, pueden transmitirse dentro de la STM-1, depositados dentro de un VC más grande. El VC "menor" puede, por regla general, tener deslizamientos de fase dentro del VC "mayor" (de orden superior), a tal efecto el VC de orden superior debe tener incorporado un puntero que reduzca la relación de fase entre ambos VC's. Por Unidad Tributaria TU, se entiende la parte del contenedor de orden superior dentro del cual puede deslizarse el LOVC incorporado, más el puntero correspondiente (PTR-TU). Se pueden distinguir las siguientes TU: TU11, TU12, TU2, y TU3.

**Grupo de Unidades Tributarias.** Antes de ser depositadas en un contenedor de orden superior, las TU se agrupan, es decir, se concatenan por bytes, y los grupos resultantes se denominan TUG (Grupo de Unidades Tributarias). Se han definido los siguientes TUG: TUG2 y TUG3.

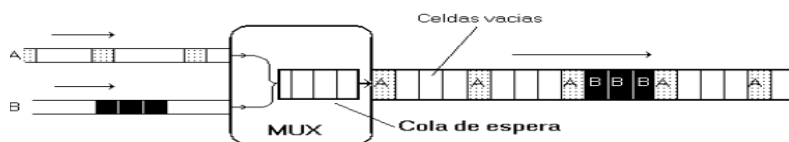
**Punteros.** Es oportuno hacer un comentario especial a cerca de los punteros. En las señales SDH es condición fundamental que antes de proceder a la multiplexación se efectúe la alineación de los punteros. Esto no significa que la señal sea retrasada ya que esto no es posible, hay que tener en cuenta que la información contenida en el área de carga útil es información que debe ser transmitida en tiempo real, lo que se hace entonces, es cambiar el contenido del puntero reacomodando la posición a la cual debe apuntar (posición donde empieza el área de carga útil). Es decir que el área de carga

útil tiene cierta libertad para deslizarse dentro del VC, siempre siendo apuntado por el puntero correspondiente.

### 3.5 Principios básicos de ATM

Es una técnica de conmutación, multiplexación así como una técnica de transmisión, diseñada para ser un modo de transferencia orientada a conexión, de propósito general, para un rango amplio de servicios. La técnica de multiplexación es por división asincrónica en el tiempo (ATD) (ver figura 47). ATM es una variación de las técnicas de conmutación de paquetes en la cual se emplean paquetes de tamaño fijo y reducido llamados celdas. En un nodo de conmutación ATM el procesamiento de las celdas se limita al análisis de una etiqueta con el número de canal lógico luego de lo cual la celda podrá ser enrutada apropiadamente. Otras funciones más complejas como chequeo y control de errores no son realizadas por la red ATM sino por los usuarios finales en los extremos de la red.

**Figura 47. Multiplexor de ATM.**



Fuente: [www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atm Apunte .pdf](http://www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atm%20Apunte.pdf).

Estas particulares características facilitan una solución razonable para los problemas propuestos por las restricciones simultaneas de tráfico diverso como voz, video y datos. Debido a su flexibilidad ATM podrá eventualmente integrar todos estos servicios en una única red de acceso común

donde la base física de transmisión este constituida principalmente por sistemas de alta velocidad SDH/SONET.

### **3.5.1 Características principales de ATM**

#### **3.5.1.1 Ausencia de control de flujo y chequeo de error nodo a nodo**

En una red ATM no existe control de flujo en nodos intermedios. La apropiada reserva inicial de recursos cuando se pretende establecer la conexión y el dimensionamiento de las colas de espera en los nodos, garantiza un número controlado de desbordes en dichas colas. De esta manera probabilidades de perdida de celdas por desborde del orden de  $10^{-8}$  a  $10^{-12}$  son perfectamente obtenibles.

Por otra parte debido a las altas velocidades de operación en ATM (>150 Mbps) un control de flujo sería impracticable pues para cuando llegue un pedido de retransmisión, un volumen importante de datos son ya fueron transmitidos.

Varios tipos de errores pueden ocurrir: errores en bits aislados y errores por pérdida o inserción de celdas.

Los errores en el medio de transmisión son en general errores en bits aislados y errores en ráfaga, causados por el ruido y por conmutación de protección (con pérdida de sincronización) respectivamente. Debido a la alta calidad de los enlaces a ser utilizados en ATM (BER pequeño) en una red ATM no se realiza ninguna acción en los nodos intermedios ante estos errores, quedando dichas acciones a cargo de protocolos extremo a extremo.

Análogamente ocurre con la pérdida e inserción de celdas. La pérdida de celdas puede ser debida a errores en la cabecera, lo que produce un enrutamiento incorrecto o bien por un problema de congestión en algún nodo, lo que produce el descarte de algunas celdas. Este fenómeno típico de las redes de conmutación de paquetes, es resuelto vía pedido de retransmisión (ARQ).

En cambio en ATM no hay acciones dinámicas definidas para estas situaciones. La única acción preventiva que se toma es la reserva previa de los recursos necesarios para la transmisión durante la configuración de la conexión. La pérdida de celdas debida al desborde de una cola de espera en nodo es un problema típico en ATM debido a la ausencia de control de flujo entre nodos intermedios y por lo tanto existe la posibilidad que una cola sea momentáneamente rebosada por la contribución de varias fuentes. Sin embargo esta pérdida de celdas momentánea está controlada y limitada a valores muy pequeños gracias al modo orientado a conexión y al dimensionamiento de los conmutadores (reserva previa de recursos, i.e. probabilidad muy baja de pérdida de celdas) en una red ATM. Por otra parte la pérdida de celdas por enrutamiento incorrecto es debido a errores en la cabecera y por esto la cabecera si tiene un control de error en los nodos.

### **3.5.1.2 Operación orientada a conexión**

Antes que la información sea transferida desde un terminal a la red, una fase de establecimiento de una conexión lógica/virtual debe ser realizada para permitir a la red la realización de la reserva de los recursos necesarios. En caso que dichos recursos no estuvieran disponibles el pedido de conexión es rechazado al terminal llamante.

Cuando la fase de transferencia de información finaliza, los recursos son liberados. Este modo orientado a conexión permite a la red garantizar para todos los casos una mínima pérdida de celdas y así la máxima calidad. En realidad la red cuando recibe la llamada de establecimiento verifica si hay suficientes recursos estadísticamente hablando. Se garantiza que la probabilidad que haya desborde de colas sea menor que cierto valor. Valores típicos en sistemas ATM son de  $10^{-8}$  a  $10^{-12}$  para la probabilidad de perder un paquete por desborde en una cola.

### **3.5.1.3 Funciones de la cabecera**

Para garantizar un rápido procesamiento en los nodos de la red la cabecera en ATM tiene funciones muy limitadas. La cabecera (de 5 bytes de longitud) contiene la identificación de la conexión virtual, la cual es empleada para enrutar apropiadamente la celda. Como errores en un bit de la cabecera producen errores en el enrutamiento y por lo tanto pérdida de celdas esta contiene un campo de detección/corrección de errores (de la cabecera solamente). Este campo para detección de errores es empleado también para la delimitación de celdas, puesto que en la cabecera no existe un campo especialmente asignado para delimitación como en otros protocolos a nivel de enlace.

Algunas otras funciones limitadas son realizadas por la cabecera, como aquellas relacionadas con operación y mantenimiento. Gracias a la limitada funcionalidad de la cabecera el procesamiento de las mismas es simple y por lo tanto puede ser realizado a muy altas velocidades (150 Mbps a Gbps). Esto resulta en muy pequeños retardos de procesamiento y encolamiento.

#### 3.5.1.4 Campo de información relativamente pequeño

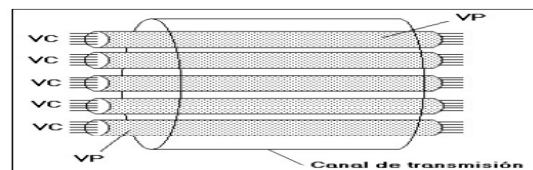
Para reducir los *buffers* internos en los nodos de conmutación y para limitar los retardos de encolamiento en dichos *buffers* el campo de información es relativamente pequeño (48 bytes). Al tener *buffers* pequeños se garantiza un retardo y *Jitter* de retardo reducidos así como es requerido en los servicios de tiempo real.

#### 3.5.2 Conexiones virtuales - Canales virtuales – Caminos virtuales

Como ya fue mencionado, una de las características de ATM es la limitada funcionalidad de la cabecera. Esta limitada funcionalidad es ampliamente soportada por el modo orientado a conexión de la red ATM. Efectivamente, funciones como dirección origen y dirección destino y número de secuencia, los cuales son necesarios en una red sin conexión, no son requeridas en una red ATM. Cada conexión virtual será identificada por un número (identificador), el cual solo tendrá significación local en cada tramo del enlace de dicha conexión virtual.

La identificación de la conexión virtual se hace mediante dos campos de la cabecera de las celdas:

**Figura 48. VCI y VPI de ATM.**



Fuente: [www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atm Apunte.pdf](http://www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atm%20Apunte.pdf).

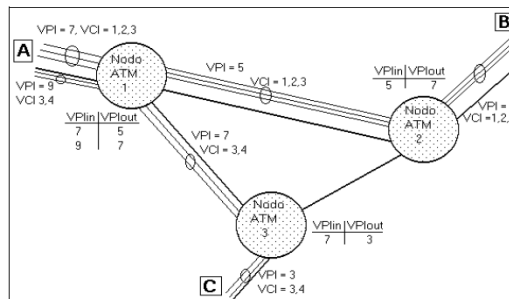


VCI (identificador de canal virtual): Identifica conexiones asignables dinámicamente.

VPI (identificador de camino virtual): Identifica conexiones asignables estáticamente.

Esta función es realizada por el campo de la cabecera llamado VCI. En la futura red de banda ancha las redes de transporte estarán fundamentalmente compuestas por fibras ópticas, permitiendo enlaces de cientos de Mbps a Gbps. Los canales virtuales estarán compuestos por señales de tasas del orden de los Kbps. Así un número grande de canales tendrá que ser soportado en un mismo enlace. Típicamente un número de canales del orden de las decenas de miles, esto requiere un campo identificador de canal de 16 bits.

**Figura 49. Red ATM.**



**Fuente:** [www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atmApunte.pdf](http://www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atmApunte.pdf).

Como la red ATM es orientada a conexión, cada una de ellas es caracterizada mediante un VCI, el cual es asignado inicialmente cuando el usuario hace un pedido de conexión. Un VCI tiene solo significación local sobre los nodos ATM y será trasladado en dichos nodos. Cuando la

conexión es liberada, todos los VCIs en los enlaces implicados son liberados y podrán ser usados por otras conexiones.

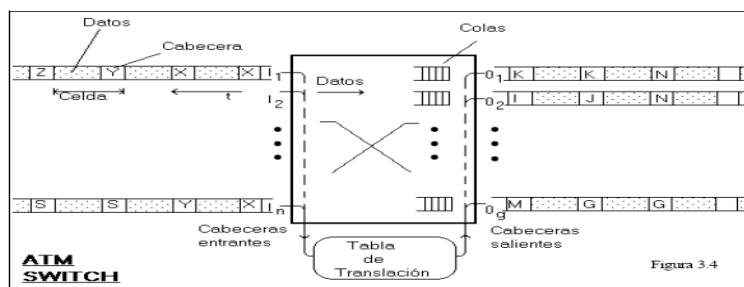
### 3.5.2.1 Caminos Virtuales

Adicionalmente está previsto que la futura red de banda ancha soporte conexiones semipermanentes entre puntos extremos. Estas conexiones semipermanentes transportan numerosas conexiones simultáneas. Este conjunto de conexiones que forman un camino virtual estarán caracterizadas por una misma QOS. Este concepto es conocido como conexión camino virtual (VPC). En este concepto los recursos de la red son reservados semipermanentemente para posibilitar una administración simple y eficiente.

### 3.5.3 Conmutación

El principio general de conmutación puede observarse en la figura 50 Un número de  $n$  puertos o enlaces de entrada transportando información ATM se conmutan en función del contenido de sus cabeceras hacia los  $q$  puertos de salida.

**Figura 50. Conmutador ATM.**



Fuente: [www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atmApunte.pdf](http://www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atmApunte.pdf).

Conjuntamente, el puerto de entrada y los valores VPI/VCI en la cabecera son el punto de entrada a una tabla de traducción, la cual contiene la información necesaria para el enrutamiento de las celdas. En esta tabla se decide sobre el puerto de salida por el que saldrá cada celda y si dicha celda conservará los valores VPI/VCI de la cabecera que identifican la conexión. En definitiva en el conmutador podrán ser trasladados el VPI, el VCI o ambos (además de la conmutación espacial sobre los puertos).

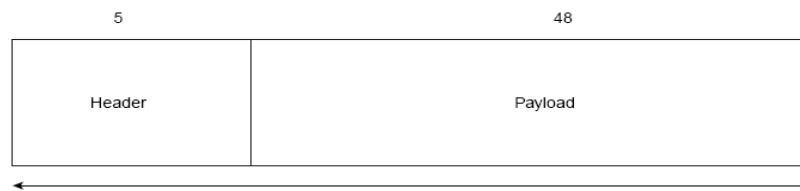
**Tabla IV. Tabla de conmutación ATM.**

| Enlace entrante | Ranura de tiempo | Enlace saliente | Ranura de tiempo |
|-----------------|------------------|-----------------|------------------|
| 11              | X<br>Y           | 01<br>02        | k<br>l           |
| ...             | ...              | ...             | ...              |
| in              | X<br>Y           | 01<br>02        | n<br>g           |

### 3.5.4 Formato básico de la celda

ATM transfiere información en unidades de tamaño fijo llamadas celdas. Cada celda consiste en 53 octetos, o bytes. Los cinco primeros bytes contienen la información de encabezado, los restantes 48 contiene en el área útil de información. Celdas pequeñas, y de un largo fijo son ideales para transferir tráfico de voz o video debido que este tipo de tráfico es intolerante a los retrasos resultantes por el hecho de tener que esperar a que un paquete grande sea transferido, entre otras cosas.

**Figura 51. Formato básico de la celda ATM.**



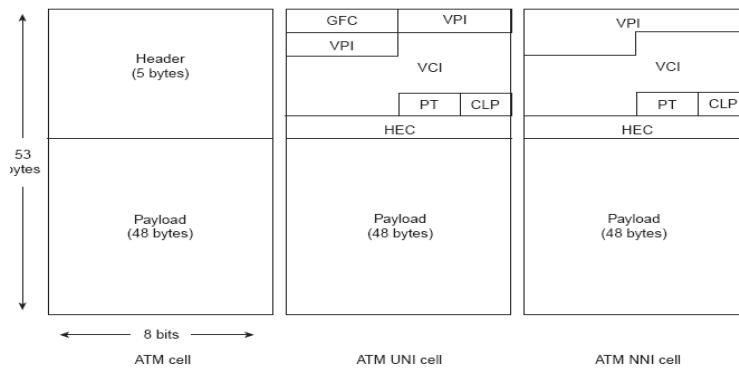
Fuente: [www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm).

En la figura 51 se muestran los campos de una celda ATM (el largo de los campos está en bytes).

### 3.5.4.1 Formato de cabecera de ATM

Una cabecera de ATM puede poseer uno de dos formatos: UNI o NNI. La cabecera UNI es usada para la comunicación entre puntos terminales y conmutador es en redes privadas de ATM. La cabecera NNI es usada para comunicación entre conmutadores en la figura se muestran ambos formatos básico de ATM, UNI y NNI.

**Figura 52. Formatos de celda de ATM.**



**Fuente:** [www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm).

Al contrario del formato UNI, el formato NNI no incluye el campo de control de flujo genérico (GFC). Adicionalmente la cabecera NNI tiene un identificador de camino virtual (VPI) que ocupa los primeros doce bits, permitiendo líneas troncales más largas entre conmutadores públicos de ATM.

### 3.5.4.2 Campos de las celdas de ATM

Adicionalmente a los campos de GFC y VPI, existen varios más que son utilizados en la cabecera de ATM. A continuación describiremos las funciones de los campos ilustrados en la figura:

- **Control de Flujo Genérico (GFC).** Proporciona funciones locales, como la identificación de múltiples estaciones que comparten una interfaz de ATM, este campo no es típicamente usado y casi siempre está puesto a su valor por defecto de 0 (0000 binario).
- **Identificador de Camino Virtual (VPI).** En conjunto con el VCI, identifica el siguiente destino de una celda a su paso por diversos conmutadores de ATM en camino a su destino final.
- **Tipo de Carga (PT).** Indican en primer bit si la celda contiene datos de usuario o datos de control. Si la celda contiene datos de usuario, el bit es puesto a cero, pero si contiene datos de control es puesto a 1. El segundo bit indica congestión (0 = no congestión 1=congestión), y el tercer bit indica si la celda es la última de una serie o si representa una celda simple AAL5 (1= representa la última celda de una trama).
- **Prioridad de Pérdida de Celda (CLP).** Indica si la celda debe ser descartada si se encuentra con una congestión extrema mientras se mueve dentro de la red. Si el bit de CLP es igual a 1, la celda debe ser descartada antes de las que tienen este bit a 0.
- **Control de Error de Cabecera (HEC).** Calcula el sumario solamente de los cuatro primeros bytes de la cabecera. HEC puede corregir un error a nivel de un solo bit en estos bytes, preservando así la celda en lugar de descartarla.

### 3.5.5 Modelo de referencia ATM.

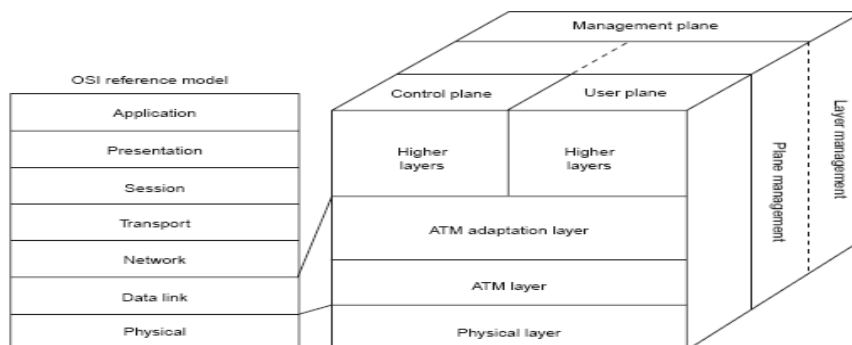
La arquitectura ATM usa un modelo lógico para describir la funcionalidad que soporta. Esta corresponde a la capa física y parte de la capa de enlace del modelo de referencia OSI.

El modelo de referencia de ATM es compuesto por los siguientes planos que abarcan todas las capas:

- Control. Este plano es responsable de generar y manejar requerimientos de señalización.
- Usuario. Este plano es responsable de la transferencia de datos.
- Administración. Este plano contiene dos componentes:
  1. Administración de capa. Maneja funciones específicas de capa, tales como la detección de fallas y problemas de protocolo.
  2. La administración de plano maneja y coordina funciones relacionadas con el sistema completo.

El modelo de referencia ATM esta compuesto por las siguientes capas:

**Figura 53. Modelo de referencia ATM.**



Fuente: [www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm).

### 3.5.5.1 La capa física de ATM

La capa física de ATM tiene cuatro funciones: convertir celdas en una cadena de bits, controlar la transmisión y recepción de bits en el medio físico, rastrear los límites de las celdas, y empaquetar las celdas de una forma adecuada para el medio físico. Por ejemplo las celdas son empaquetadas de forma diferente para los medios SDH que para los medios de un E3.

La capa física esta dividida en dos partes: la parte dependiente del medio físico (PMD) y la parte de convergencia de transmisión (TC). La subcapa de PMD provee dos funciones principales. La primera de ella es la sincronización de la transmisión y recepción esto mediante el envío y la recepción de un flujo continuo de bits con información de sincronía asociada a estos. La segunda especifica el medio físico utilizado, incluyendo el conector y el cable utilizado.

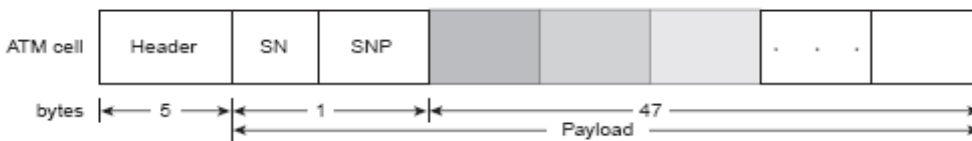
La capa TC tiene cuatro funciones: delineación de trama, control de error de cabecera (HEC), generación y verificación de secuencia, desacople de rata de celda y adaptación de trama para transmisión. La función de delineación de trama mantiene los límites de la celda de ATM, permitiendo a los elementos de red localizar una celda dentro de una cadena de bits. La generación de secuencia HEC, genera y verifica el código de control de errores en la cabecera para asegura que la información sea valida. La función de desacople de rata de celdas mantiene la sincronización, inserta o remueve celdas no asignadas para adaptar la rata de celdas validas a la capacidad de transporte del sistema de transmisión. La función de adaptación de transmisión de tramas empaqueta las celdas de ATM en tramas aceptables para la implementación física utilizada para la transmisión.

### 3.5.5.2 Capas de adaptación de ATM

**AAL1**, un servicio orientado a conexión, es apropiado para manejar fuentes con una tasa de bit constante (CBR), tales como voz y video conferencia. ATM transporta este tipo de tráfico usando servicios de emulación de circuitos, esta tecnología también soporta el uso de equipo que actualmente utiliza líneas dedicadas para conectarse a la red troncal de ATM. AAL1 requiere sincronización entre la fuente y el destino. Por esta razón AAL1 depende del medio, tales como SDH, que soporta un reloj.

La AAL1 prepara una celda para transmisión en tres pasos. Primero se insertan muestra síncronas en el área de carga útil. Segundo los campos de número de secuencia (SN) y protección de número de secuencia (SNP) sobre ellos para proporcionar información que el receptor AAL1 utiliza para verificar que ha recibido las celdas en orden correcto. Tercero el restante del área de carga es llenado con bytes suficientes para llegar a 48.

**Figura 54. AAL1 prepara la celda para transmisión (los cuadros sombreados representan bytes de relleno).**



Fuente: [www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm).

### 3.5.5.3 Capas ATM de adaptación ALL2

Existe otro tipo de tráfico que requiere temporización tal como el CBR pero tiene una naturaleza de ráfagas. Este es llamado tráfico de tasa de bit variable (VBR). Este incluye típicamente servicios como voz por paquetes o



vive o que no tiene una velocidad constante de transmisión pero sí tiene requerimientos similares a los servicios de velocidad de bit constante AAL2 es adecuado para este tipo de tráfico. El proceso AAL2 usa 44 bytes del área de carga de la celda para datos del usuario y reserva cuatro bytes para los procesos que intervienen en el AAL2. El tráfico antes descrito está caracterizado por ser de tiempo real (VBR-RT) o como servicios no en tiempo real (VBR-NRT). Esta capa soporta a ambos tipo de tráfico.

#### **3.5.5.4 Capa de adaptación AAL $\frac{3}{4}$**

Esta capa soporta datos orientado y no orientados a conexión. Esta fue diseñada para proveedores de servicios de red y esta estrechamente relacionada Servicios de Datos Conmutados de Multimegabit (SMDS).

Esta capa prepara una celda para la transmisión en cuatro pasos, Primero la subcapa de convergencia (CS) crea una unidad de protocolo (PDU), anexando un encabezado con etiquetas de principio, fin y largo. Segundo, la subcapa de segmentación y reensamblamiento (SAR), fragmenta la PDU y anexa un encabezado a este. Entonces la SAR anexa un CRC-10 y un encabezado a cada fragmento de la PDU para control de error. Finalmente, la PDU completa de la SAR se convierte en el campo o área de carga de la celda ATM a la cual la capa ATM le añade un encabezado estándar.

Un encabezado de PDU de AAL  $\frac{3}{4}$  consiste en los siguientes campos Tipo, Número de secuencia e identificador de multiplexión. El campo de Tipo identifica si la celda es un principio, continuación o el final d un mensaje. Le campo de número de secuencia identifica el orden en el que una celda debe ser reensamblada. El identificador de multiplexión determina que celdas de diferentes fuentes de trafico deben se entrelazadas en la misma conexión de

circuito virtual y así puedan ser reensambladas de forma correcta en su destino.

### **3.5.5.5 Capa de adaptación AAL5**

Esta capa es el AAL primaria para poder soportar ambos tipos de datos, orientados o no orientados a conexión, es utilizado para transferir la mayoría de tráfico no SMDS, tales como el clásico IP sobre ATM y Emulación de LAN (LANE). AAL5 es también llamada como la capa de adaptación simple y eficiente (SEAL). Debido a que la subcapa SAR simplemente acepta la CS-PDU y la segmenta en PDU-SAR de 48 bytes si reservar bytes en cada celda.

Esta capa prepara la celda en tres pasos. Primero, la subcapa CS anexa un relleno de largo variable y 8 bytes al final de la trama. El relleno asegura que la PDU se encuentre dentro de los límites de una celda de ATM de consiste en 48 bytes. Los bytes incluidos al final contienen la información de él largo de la trama y una secuencia de 32 bits de CRC calculado para toda la PDU. Esto permite a la parte de recepción de la capa AAL5 detectar pérdidas de celda o celdas que están fuera de secuencia. Segundo, la subcapa SAR fragmenta la PDU de la CS en bloques 48 bytes. En esta parte no se les añade un bytes de cabecera ni de final, en este caso los mensajes no puede ser entrelazados. Finalmente la capa de ATM coloca cada bloque en el área de carga de una celda. Para todas las celdas a excepción de la última, un bit en el campo de tipo es puesto a 0 a indicar que la celda no es la última celda en la serie que representa una trama. Por otro lado para la última celda, el bit en el campo de tipo expuesto uno.

### **3.5.6 Direccionamiento de ATM**

El estándar de la ITU-T está basado en el uso de direcciones E. 164 (similares a numeración telefónica) para redes ATM públicas. El foro de ATM extendió las direcciones para incluir redes privadas. Esto decidido en la subred o el modelo sobrepuesto de direccionamiento, en el cual la capa de ATM es responsable por mapear las direcciones de capa de red a direcciones de ATM. Este modelo de subred es una alternativa al uso de las direcciones de protocolos de capa de red y protocolos de enrutamiento existentes. El foro de ATM definió un formato de dirección basado en la estructura de las direcciones del servicio de punto de acceso de red NSAP del modelo OSI.

#### **3.5.6.1 Modelo de direccionamiento de subred**

El modelo de direccionamiento de subred separa la capa de ATM de cualquier protocolo de nivel superior, tales como IP o IPX. Debido a esto, este requiere un esquema de direccionamiento y enrutamiento completamente nuevo. A cada sistema de ATM se le debe asignar una dirección de ATM, adicionalmente a las direcciones de los protocolos de capa superior. Esto requiere un protocolo de resolución de direcciones para ATM (ATM ARP) para mapear las direcciones de protocolos superiores a sus correspondientes direcciones de ATM.

#### **3.5.6.2 Formato NSAP**

El formato de direcciones de 20 bytes NSAP de ATM está diseñado para su uso dentro de una red privada ATM, en tanto que en las redes públicas usan típicamente las direcciones E.164, las cuales son definidas por la ITU-T. El foro de ATM ha especificado una codificación NSAP para las

direcciones E.164, el cual es utilizado para codificar estas direcciones dentro de las redes privadas, a pesar de esto las direcciones E.164 también pueden ser utilizadas dentro de algunas redes privadas.

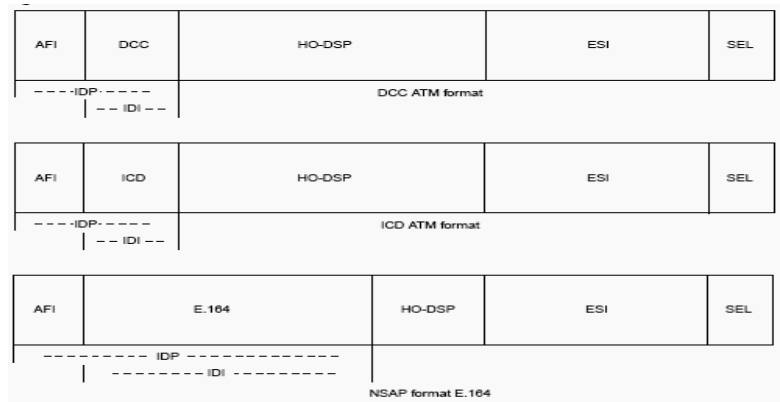
Estas redes privadas pueden basar su propio direccionamiento en las direcciones E.164 de la UNI a la cual están conectados y pueden tomar un prefijo de dirección de la numeración E.164, identificando los nodos locales mediante los bits de orden inferior.

Todas las direcciones con formato NSAP consisten de tres componentes: el identificador de formato y autoridad (AFI), el identificador inicial de dominio (IDI), y la parte específica de dominio (DSP). La AFI identifica el tipo y el formato de la IDI, quien, a su vez, identifica la adjudicación de dirección y la autoridad administrativa. El DSP contiene la información de enrutamiento.

Se distinguen tres formatos de direccionamiento en redes privadas de ATM, estos difieren en la naturaleza del AFI y la IDI. En el formato de NSAP codificada en E.164, la IDI es un número E.164. En el formato DCC, es un código de país (DCC), el cual identifica países en particular, como es especificado en el ISO 3166. Estas direcciones son administradas por el cuerpo nacional de miembros de la ISO en cada país. En el formato ICD, la IDI es un designador internacional de código (ICD), el cual está alojado en la autoridad de registro por la ISO 6523. El código ICD identifica organizaciones internacionales particulares. El foro de ATM recomienda que las organizaciones o los proveedores de servicios para redes privadas usen ya sea el formato DCC o el ICD para formar su propio plan de numeración.

En la figura 55 se muestran los tres formatos de direcciones de ATM que son usados por redes privadas.

**Figura 55. Formatos de dirección ATM.**



Fuente: [www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm).

### 3.5.6.3 Campos de la dirección ATM

La siguiente descripción resume los campos ilustrados en la figura:

- **AFI.** Identifica el tipo y formato de la dirección (E.164, ICD, o DCC).
- **CDD.** Identifica un país en particular.
- **Parte específica de dominio de orden superior.** Combina el dominio de enrutamiento (RD) y el identificador de area (AREA) del las direcciones de NSAP. El foro de ATM combino estos campos par a soportar una jerarquía de direccionamiento, flexible, multicapa para protocolos de enrutamiento basados en prefijos.
- **Identificador de sistema final.** Especifica la dirección MAC de 48 bits, es administrada por la IEEE.
- **Selector (SEL).** Es usado para multiplexión local entre estaciones finales y no tiene ningún significado para la red.
- **ICD.** Identifica organizaciones internacionales.
- **E.164.** Indica la dirección E.164.

### 3.5.7 Conexiones de ATM

El protocolo ATM soporta dos tipos de conexión: punto a punto y punto a multipunto. En la versión punto a punto se conectan dos sistemas terminales de ATM y puede ser unidireccional o bidireccional. En la versión de punto a multipunto este conecta un punto terminal a varios puntos terminales en una red ATM llamados comúnmente hojas. Este tipo de conexiones son unidireccionales únicamente. Los nodos raíz pueden transmitir a los nodos de hoja pero los nodos de hoja no pueden transmitir hacia el nodo raíz o a otro nodo de hoja. La replicación de celdas es llevada a cabo dentro de la red de ATM por conmutadores de ATM donde las conexiones pueden dividirse en dos o más ramas.

Es deseable que en las redes ATM existieran las conexiones multipunto a multipunto. Estas conexiones son análogas a la difusión o multidifusión de las Lan de medios compartidos, tales como Ethernet y Token Ring. Desafortunadamente, esta capacidad no puede ser implementado mediante el uso de la AAL5, que es la capa AAL más común utilizada para transmitir en la red de ATM. A diferencia de la capa AAL 3/4, y su campo identificador de mensaje (MID), AAL 5 no provee una manera dentro del formato de la celda para entrelazar celdas de diferentes paquetes de AAL5 dentro de una conexión. Esto significa que todos los paquetes de AAL5 enviados a un destino en particular a través de una conexión en particular deben ser recibidos en secuencia; de otra manera, el proceso de reensamblado del destino será incapaz de reconstruir el paquete.

Eso es el porque las conexiones de punto a multipunto de la capa AAL5 solo pueden ser unidireccionales. Si un nodo de hoja fuera a transmitir un paquete de AAL5 en la conexión, por ejemplo, este sería recibido por el nodo

raíz y todos los demás nodos de hoja. En estos nodos, el paquete enviado por el nodo de hoja puede ser entrelazado con paquetes enviados por el nodo raíz y posiblemente otros nodos de hoja, imposibilitando la reconstrucción de cualquier paquete entrelazado.

### **3.6 Evolución de la conmutación multicapa en la Internet**

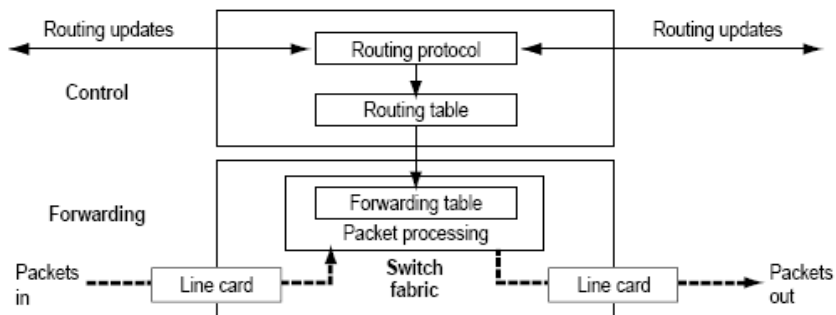
La conmutación multicapa describe la integración de la capa de conmutación y la de enrutamiento. En la actualidad las redes ISP son construidas utilizando un modelo sobrepuesto en el cual la una topología con lógica de enrutamiento IP corre de manera independiente de la topología de conmutación debajo de ella.

Los conmutadores proveen una conectividad de alta velocidad, mientras que los enrutadores de IP en los bordes de la red, interconectados por una malla de circuitos virtuales de capa dos, proveen a la red de la inteligencia necesaria para enviar paquetes. La dificultad de encarar el transporte de datos con esta aproximación recae en la complejidad del mapeo entre dos arquitecturas diferentes que requieren la definición y el mantenimiento de topologías separadas, espacios de direcciones, protocolos de enrutamiento, protocolos de señalización, y esquemas de asignación de recursos. La florecimiento de soluciones de conmutación multicapa y MPLS es parte de la evolución del Internet para aliviar la complejidad de combinar la conmutación de la capa dos y el enrutamiento de capa tres en una solución plenamente integrada.

### 3.6.1 Separación de los componentes de envío y control

Todas las soluciones de conmutación de multicapa, incluyendo MPLS. Esta compuestos de dos componentes funcionales, un componente de control y un componente de envío. La componente de control utiliza protocolos de enrutamiento estándar para intercambiar información con otros enrutadores para construir y mantener una tabla de envío. Cuando los paquetes llegan, el componente de envío busca la tabla de envío mantenido por la componente de control para hacer una decisión de enrutamiento para cada paquete, específicamente, la componente de envío examina la información contenida en el encabezado del paquete, busca la tabla de envío para comparar la información y por ultimo dirige el paquete de la interfaz de entrada a la interfaz de salida a través de la red.

**Figura 56. Descripción de las capas de control y envío.**



Fuente: [/www.rediris.es/rediris/boletín/53/enfoque1.html](http://www.rediris.es/rediris/boletín/53/enfoque1.html).

Con la separación de los componente de control y la componente de envío, cada componente puede ser independientemente actualizada y o modificada. El único requerimiento es que la componente de control se siga comunicando con la componente de envío por medio de la administración de la tabla de envío de paquetes. Veremos que mediante la implementación de



un algoritmo de envío incluso tan simple como el de intercambio de etiquetas, nos puede proveer de una capacidad de envío extendido ideal para cubrir las necesidades de los servicios de alta velocidad.

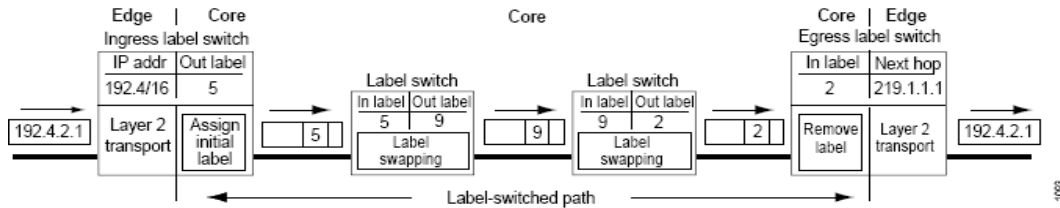
### **3.6.2 Algoritmo de intercambio de etiquetas.**

La componente de envío de virtualmente todas las soluciones de conmutación multicapa y MPLS están basadas en este algoritmo. Este es el mismo algoritmo utilizado para enviar datos a través de los conmutadores de ATM y Frame Relay. La señalización y la distribución son fundamentales en el funcionamiento de este algoritmo.

Una etiqueta es un valor de longitud fija que es transportado en el encabezado del paquete para identificar un Clase Equivalente de Envío (FEC). Una etiqueta es análoga a un identificador de conexión, tal y como en ATM lo son los VPI/VCI o en Frame Relay lo es el DLCI, debido a que también solamente poseen un significado local, no contiene información de la capa de red, y mapea el tráfico a un FEC específico. Un FEC es un conjunto de paquetes que son enviados sobre el mismo camino a través de una red, aun si sus destinos finales son diferentes.

Este protocolo requiere la clasificación de paquetes en lado de entrada de la red para asignar una etiqueta inicial a cada paquete. En la figura 57, el conmutador de nivel de ingreso recibe un paquete sin etiqueta con una dirección de destino de 192.4.2.1. El conmutador de entrada realiza una búsqueda en la tabla de enrutamiento y mapea el paquete a un FEC 192.4/16. Entonces el conmutador de ingreso asigna una etiqueta con valor de 5 al paquete y lo envía al siguiente conmutador, en el camino conmutado por etiquetas LSP

**Figura 57. Camino conmutado por etiquetas.**



Fuente: [www.rediris.es/rediris/boletín/53/en\\_foque1.html](http://www.rediris.es/rediris/boletín/53/en_foque1.html).

Un LSP funcionalmente es equivalente a un circuito virtual porque este define un camino de ingreso y egreso a través de la red que es seguido o tomado por todos los paquetes asignados a un FEC específico. El primer conmutador de etiquetas en un LSP es llamado conmutador de ingreso, o conmutador extremo cabeza del enlace. El último de los conmutadores es llamado conmutador de egreso o conmutador de cola del enlace.

En el núcleo de la red, los conmutadores ignoran los encabezados de capa tres y simplemente reenvían los paquetes usando el algoritmo de intercambio de etiquetas. Cuando un paquete etiquetado llega a un conmutador, la componente de envío usa el número del puerto de entrada y la etiqueta para realizar una búsqueda en la tabla de enrutamiento por una correspondencia exacta con los parámetros anteriormente descritos. Cuando estos parámetros son encontrados la componente de envío recupera la etiqueta de salida, la interfaz de salida, y la dirección del siguiente salto de la tabla de envío. La componente de envío entonces intercambia o reemplaza la etiqueta entrante con la etiqueta saliente y dirige el paquete a la interfaz de salida para su transmisión al siguiente salto en la red LSP:

Cuando el paquete llega al conmutador de etiquetas de salida la componente de envío busca en su tabla de envío, si el siguiente salto no es

un conmutador de etiquetas , el conmutador descarta la etiqueta y envía el paquete utilizando la tecnología IP convencional.

El intercambio de etiquetas provee un número significativo de beneficios operacionales cuando es comparado con el enrutamiento de salto por salto de la capa de red.

- El intercambio de etiquetas de a los proveedores de servicios una tremenda flexibilidad en al forma que asigna los paquetes a los FEC. Por ejemplo, para simular el envío IP convencional, el conmutador de ingreso puede ser configurado para asignar un FEC a un paquete basándose en la dirección de destino. Sin embargo los paquetes pueden se asignados a un FEC basándose en consideraciones de pólizas de un numero ilimitado, la dirección fuente, el tipo de aplicación, el punto de entrada a la red de intercambio de etiquetas, el punto de salida de la red, o cualquier combinación de pólizas.
- Los proveedores de servicios construyen LSP personalizados que soportan requerimientos de una aplicación específica. Estas pueden ser diseñadas para minimizar el numero de saltos, cumplir con cierto ancho de banda, para soportara requerimientos específicos de desempeño, evitar puntos de de congestión, dirigir el trafico lejos del camino escogido por el protocolo IGP, o simplemente forzar trafico a través de enlaces y nodos específicos de la red.
- El beneficio más significativo del algoritmo de intercambio de etiquetas es la habilidad de tomar cualquier tipo de trafico de usuario, asociarlo con un FEC, y mapear el FEC en un LSP que ha sido específicamente diseñado para satisfacer las necesidades del FEC. La implementación de tecnologías basadas en las técnicas de envío del algoritmo de intercambio de etiquetas ofrece a los ISPs un control

preciso sobre el flujo de tráfico sobre sus redes. Este nivel sin precedencia de control resulta en una red que opera más eficientemente y provee servicios más predecibles.

### **3.6.3 IP Sobre ATM**

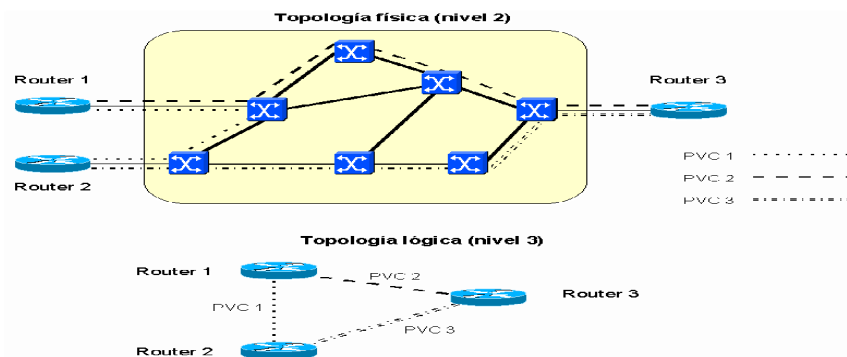
A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso. Por otro lado, hay que recordar que las redes de núcleo IP que los proveedores de servicio (ISP Proveedor de Servicios de Internet) habían empezado a desplegar en esos años, estaban construidos basados en enrutadores conectados por líneas dedicadas T1/E1 y T3/E. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los ISPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los ISPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los enrutadores tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los enrutadores IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los ISPs. Por un lado, proporcionaba mayores

velocidades (155 Mbps) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de ISPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de enrutadores IP sobre una topología real de conmutadores ATM. La red núcleo ATM se presenta como una nube central (el núcleo) rodeada por los enrutadores de la periferia. Cada enrutador comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los enrutadores de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los enrutadores ven los PVCs como enlaces punto a punto entre cada par. En la figura 58 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

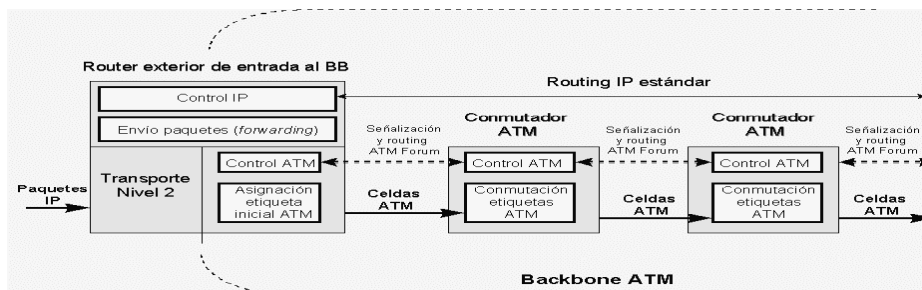
**Figura 58. Topología física ATM y topología lógica IP superpuesta.**



Fuente: [/www.rediris.es/rediris/boletín/53/enfoque1.html](http://www.rediris.es/rediris/boletín/53/enfoque1.html).

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y *enrutamiento*) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del *backbone*; el papel de los enrutadores IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 59 se representa el modelo IP/ATM con la separación de funciones entre los que es *enrutamiento* IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

**Figura 59. Modelo Funcional IP sobre ATM.**



Fuente: [www.rediris.es/rediris/boletín/53/enfoque1.html](http://www.rediris.es/rediris/boletín/53/enfoque1.html).

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores.

La ingeniería de tráfico se hace a base de proporcionar a los enrutadores los PVCs necesarios, con una topología lógica entre enrutadores totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los sub-interfaces en los enrutadores con los PVCs, a través de los cuales se intercambian los enrutadores la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de enrutadores, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un *overhead* aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial  $n \times (n-1)$  al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, p. ej., en una red con 5 enrutadores externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios  $5 \times 4 = 20$  PVCs (uno en cada sentido de transmisión). Si se añade un sexto enrutador se necesitan 10 PVCs más para mantener la misma estructura ( $6 \times 5 = 30$ ). Un problema adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. MPLS, logra esa integración de niveles sin discontinuidades.

#### **3.6.4 Alternativas de conmutación de multicapa para el modelo de IP sobre ATM**

Mientras los ISPs continuaron migrando al modelo de IP sobre ATM, un número de tendencias, técnicas, de mercadeo y financieras comenzaron a influenciar el desarrollo de nuevas tecnologías designadas para el núcleo del Internet. El público en general comenzó a entender el rol prominente de la Internet proveyendo las bases para una nueva base de la economía global. Quedó claro que el Mercado del Internet era lo suficientemente grande como para construir equipo específicamente diseñado para la red núcleo del Internet, IP se convirtió rápidamente en el único protocolo importante, ganando campo sobre IPX, AppleTalk, OSI y SNA.

Por el año 1996, varios vendedores estaban promoviendo soluciones propietarias de conmutación de multicapa que integraban la conmutación de ATM y el enrutamiento de IP estas incluían:

- Conmutación de IP diseñada por Ipsilon/Nokia
- Conmutación de etiquetas, desarrollado por Cisco Systems
- Agregado Basado en Enrutamiento Conmutación IP (ARIS), diseñado por IBM.
- Navegador IP diseñado por Cascade/Ascend/Lucent Technologies

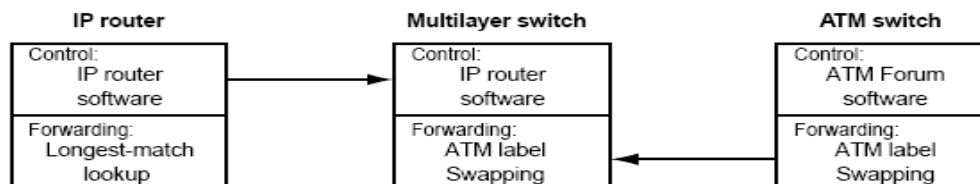


A pesar que estas soluciones tenían un número de características en común, no eran interoperables debido a que cada uno corría sobre diferentes tecnologías para combinar el enrutamiento IP y la conmutación de ATM en una solución integral. Sin embargo, al principio del 1997, muchos en la comunidad de Internet estaban impresionados con la simplicidad y elegancia de la solución, empezaron a ver a este tipo de tecnología como el siguiente paso lógico en la evolución para el diseño de las grandes red de ISP.

### 3.6.5 Similitudes entre las soluciones de conmutación multicapa.

Cada una de las soluciones de conmutación multicapa pretende combinar las mejores propiedades del enrutamiento de IP y a conmutación de ATM, mientras mantienen un enfoque de IP. El acercamiento fundamental adoptado por estas estrategias fue de tomar el software de control de un enrutador IP e integrarlo con el desempeño de envío de un conmutador de ATM y crear un enrutador IP extremadamente rápido y eficiente.

**Figura 60. Integración de un enrutador IP y un conmutador ATM en un conmutador multicapa.**



**Fuente:** /www.rediris.es/ rediris/boletín /53/enfoque1.html.

Para la componente de control, cada conmutador de multicapa corre un protocolo de enrutamiento IP standard (OSPF, IS-IS, y BGP4) y un mecanismo propietario para unir las etiquetas. El software de enrutamiento permitía a los conmutadores múlticapa intercambiar información de alcance de red de capa 3.

El mecanismo de unión de etiquetas mapeaba rutas de capa 3 para etiquetas y le distribuía sus vecinos para establecer LSPS a través de la red núcleo. El hecho de que los protocolos corran en la red núcleo del sistema en lugar que solamente en los sistemas exteriores proveía un número de beneficios que mejoraban la persona la red:

- Eliminaban el problema del modelo de IP sobre ATM de la escala elevada a la n de los PVC en dicha red.
- Reduce la carga del IGP mediante el decremento del número de puertos que cada enrutador debe tener y mantener.
- Permitía que la información sobre la topología real de la red núcleo estuviera disponible para los procedimientos de enrutamiento de capa 3.

Para la componente de envío, los conmutadores de multicapa usaban la conmutación convencional de ATM por hardware y el intercambio de etiquetas para enviar celdas a través de la red núcleo. Sin embargo, los procedimientos de control que asignaban las etiquetas a las rutas, distribuía en las etiquetas entre los conmutadores de multicapa, y creaban las tablas de envío eran administrados por protocolos basados en IP, y no en protocolos del foro ATM. Esto proporcionaba ciertos beneficios:

- El intercambio etiquetas optimiza el desempeño de la red utilizando los beneficios de un envío basado en hardware. Los fabricantes creían que esto promovería la creación de una nueva generación de productos que ofrecerían una relación de costo beneficio o en demanda.
- El intercambio de etiquetas hizo el enrutamiento explícito práctico. Una ruta explícita es una secuencia preconfigurada de saltos que describe el camino que el tráfico de tomar a través de la red del proveedor de servicios, permitiendo la construcción de un camino de envío que es

diferente al camino creado por el enrutamiento basado en el destino. Los caminos explícitos proveen a través un control preciso sobre flujo de tráfico, haciendo posible el soporte de la ingeniería de tráfico, calidad de servicio, y la prevención de bucles.

- El intercambio de etiquetas provee un instrumento para extender el control más allá de las limitantes impuestas por el enrutamiento basado en el destino. La habilidad de la conmutación multicapa para proveer un control mejorado de envío más allá de soportado por el mecanismo de enrutamiento convencional es una contribución duradera al diseño de red.

Al excluir los protocolos de señalización y enrutamiento del foro de ATM, la conmutación multicapa redujo la complejidad operacional eliminando la necesidad de coordinar y mapear entre dos arquitecturas de protocolo diferentes IP y ATM. A pesar de esto la conmutación multicapa todavía usa los VPI y los VCI de ATM como etiquetas, ellos serán asignados y distribuidos usando protocolos propietarios basados en IP en lugar de los protocolos establecidos del foro de ATM.

Esto es lo que la integración del enrutamiento IP y la conmutación de ATM fuera más estilizada eliminando la necesidad como anteriormente se mencionó de mapeo entre dos arquitecturas de protocolos diferentes. Sin embargo, una limitación crítica de la mayoría de la conmutación multicapa era que ellos están restringidos a correr sobre una infraestructura basada en las celdas de ATM mientras que la Internet se está transformando en una red orientada a paquetes.

### **3.6.6 Diferencias fundamentales entre las soluciones de conmutación multicapa**

Mientras para soluciones de conmutación multicapa tenían numerosas características en común, ellos dependían de dos diferentes formas para iniciar la asignación y distribución de las relaciones de etiquetas para establecer los LSP:

- El modelo manejado por datos y
- El modelo manejado por control

#### **3.6.6.1 Modelo manejado por datos**

En el modelo manejado por datos, las relaciones de las etiquetas son creadas cuando los datos de usuario llegan. Un flujo es una secuencia de paquetes que tienen la misma fuente y la misma edición IP, puerto TCP o UDP destino. Un conmutador multicapa puede crear la relación de etiquetas tan pronto como vea el primer paquete en un flujo de tráfico o esperar hasta que ha visto un número de paquetes en el flujo. El beneficio de esperar por un número de paquetes, asegura que el flujo es lo suficientemente largo para ameritar el encabezamiento para asignar y distribuir una etiqueta.

La ventaja del modelo manejado por datos es que una relación de etiquetas es creada solamente cuando hay un flujo de tráfico que usa la relación de etiqueta. Sin embargo, este modelo tiene un número de limitaciones para la implementación del núcleo eran de redes ISP, donde puede haber un número enorme de flujos de tráfico individuales:

- Cada conmutador de multicapa debe tener capacidades sofisticadas y de alto desempeño para clasificación de paquetes para identificar los flujos de tráfico.
- Típicamente, existe latencia entre el reconocimiento de un flujo y la asignación de una etiqueta al mismo. Esto significa que cada conmutador debe soportar el protocolo de envío convencional de IP durante la fase de arranque así los paquetes que no han sido asignados a un flujo puede ser enviados y no descartados.
- La cantidad de control de tráfico necesaria para distribuir las relaciones de etiquetas es directamente proporcional al número de flujos de tráfico.
- La presencia de un número significativo de flujos de corta vida puede imponer una carga pesada a las operaciones de la red.

El sentido común dicta que este tipo de modelo no posee las propiedades para formar parte de la red núcleo de Internet.

### **3.6.6.2 Modelo manejado por control**

En este modelo las relaciones de etiquetas son creadas cuando la información de control llega. Las etiquetas son asignadas en respuesta al procesamiento normal del tráfico del protocolo de enrutamiento, tráfico de control como el RSVP, o en respuesta a una concepción estática. Este posee las citas características:

- Las etiquetas son asignadas distribuidas antes de la llegada de los datos de usuario. Eso significa que si una ruta existe en la tabla de envío IP, una etiqueta ya ha sido asignada para la ruta, así el tráfico entrante al conmutador puede pasar por el procedimiento de intercambio etiquetas inmediatamente.

- La escalabilidad en este modelo es mucho mejor que en el anterior, porque el número de caminos conmutados por etiquetas es proporcional al número de entradas existentes en la tabla de envío IP, y no al número de flujos de tráfico individuales.
- Este modelo el encabezamiento es mucho menor que el anterior debido a que los caminos son establecidos después de que la información de control a llegado o existe un cambio en la antropología de red.

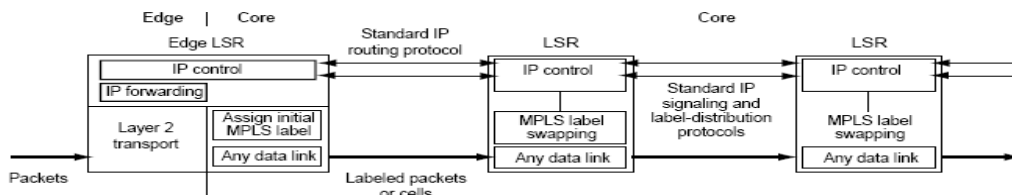
### **3.6.7 Conmutación de etiquetas múltiprotocolo MPLS**

MPLS es el último paso en la evolución de la conmutación multicapa. Es un estándar creado por la IETF. Utiliza el modelo manejado por control para iniciar la asignación y distribución de relaciones de etiqueta para el establecimiento de los caminos conmutados por etiquetas LSP. Los LSP sondeos de naturaleza simple (el tráfico fluyen en una dirección del conmutador de acceso al de egreso), el tráfico duplex requiere de dos LSP, cada uno para llevar formación en cada sentido. Un LSP es creado concatenando uno o más saltos conmutados por etiqueta, permitiendo a un paquete ser enviado de un enrutador conmutados por etiquetas (LSR) a otro a través del dominio de MPLS. Un LSR es un enrutador que soporta el envío de tráfico basado en MPLS.

La componente de control de MPLS se centra en la funcionalidad IP, lo cual es similar a las soluciones de conmutación multicapa descritas anteriormente. Sin embargo MPLS define un nuevo estándar basado en la señalización IP y en protocolos de distribución de etiquetas, como también extensiones a protocolos existentes, para soportar la interoperabilidad de

equipos. MPLS no implementa ninguno de los protocolos de enrutamiento o señalización del foro de ATM así la complejidad de manejar dos redes distintas es eliminada. De esta manera, MPLS proporciona beneficios significativos a la Internet orientada a paquetes.

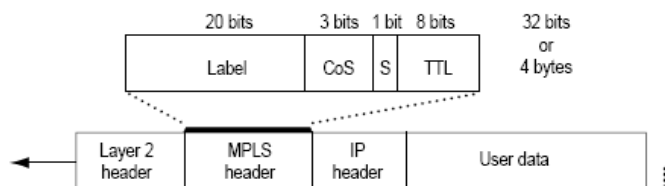
**Figura 61. Sistema funcional de MPLS.**



Fuente: [/www.rediris.es/rediris/boletín/53/elfoque1.html](http://www.rediris.es/rediris/boletín/53/elfoque1.html)

La componente de envío de MPLS está basada en el algoritmo de intercambio de etiquetas. Si la tecnología de capa dos soporta el campo de etiqueta, el campo nativo de etiqueta encapsula la etiqueta de MPLS. Sin embargo, si la tecnología de capa dos no soporta el campo de etiqueta, la etiqueta de MPLS es encapsulada en un encabezado estándar que es insertado entre los encabezados de capa dos y los encabezados IP. El encabezado en MPLS permite a cualquier tecnología de capa dos transportar una etiqueta de MPLS así éste se puede beneficiar de intercambio etiquetas a través de un LSP.

**Figura 62. Encabezado de etiqueta.**



Fuente: [://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/mpls\\_tsw.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/mpls_tsw.htm)

El encabezado de MPLS de 32 bits contienen los siguientes campos:

- El campo de etiqueta (20 bits) tras está el valor de la etiqueta de MPLS.
- El campo de CoS (3 bits) puede afectar los algoritmo de encolamiento y descarte aplicados a los paquetes conforme son trasmitidos a través de la red.
- El campo de apilamiento (S) dar soporte a un apilamiento jerárquico de etiquetas.
- El campo TTL (tiempo de vida) de ocho bits provee la funcionalidad del campo convencional TTL de IP.

### **3.6.7.1 Funcionamiento de MPLS**

La mejor forma de describir el funcionamiento de MPLS es usando la analogía de una empresa grande con sucursales ubicadas a lo largo de todo el país, cada sucursal posee un centro de procesamiento de correo a través del cual todo el correo es enviado a todas partes del mundo, como también a otras sucursales. Desde el principio, el centro de procesamiento de correo ha sido instruido para que el correo entre las sucursales sea enviado por correo de primera clase, el costo de esto es calculado dentro del presupuesto de Compañía.

Sin embargo desde hace meses, algunos departamentos se han estado quejando de que ellos requieren de entregas urgentes y del seguimiento de paquetes. Como administrador usted implementa un sistema para enviar tres tipos de correo entre sucursales primera clase, de alta prioridad y expreso. Los correo de alta prioridad y el expreso son procesados colocando el paquete dentro de un sobre especial con una etiqueta distintiva. Estos paquetes especiales con etiquetas especiales aseguran la prioridad del paquete. En orden de evitar tardanzas y cuellos de

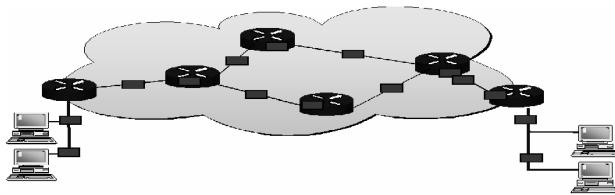


botellas, las instalaciones de correo crean un sistema que utiliza tablas de orden o bases de datos de orden para hacer expedito el trámite de estos paquetes especiales.

### 3.6.7.2 Construcción de un una red MPLS

En una a red IP, se puede pensar de los enrutadores como las oficinas postales o las estaciones de clasificación del correo. Sin los medio para marcar, clasificar y monitorear el correo, no habría forma de procesar las diferentes clases de correo. En una red IP, se encuentra una situación similar. La figura 63 muestra una red típica de IP con un tráfico sin ninguna ruta específica.

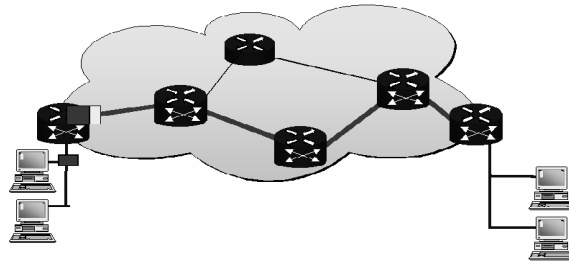
**Figura 63. Red IP clásica.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

En orden de designar diferentes clases de servicios o prioridades de servicios, el tráfico debe ser marcado con etiquetas especiales mientras se introduce a la red. Enrutadores especiales llamados LER (enrutadores de etiqueta de borde) proveen esta función de etiquetamiento. El LER convierte los paquetes IP en paquetes MPLS y viceversa. En lado de ingreso el LER examina el paquete entrante para determinar si el paquete debe ser etiquetado. Una base de datos especial en el LER encuentra una dirección destino de la etiqueta. Un encabezado de calce de MPLS es adherido al paquete y éste es enviado a su destino.

**Figura 64. Asignación de etiquetas por un LER.**



Fuente: [www.convergedigest.com / tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

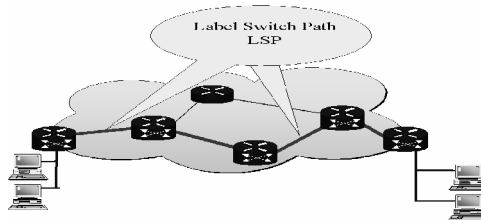
Para una explicación del encabezado de calce de MPLS, veamos el modelo en la figura 62.

En orden de enfrentar tráfico a través de la red una vez que las etiquetas han sido añadidas, los enrutadores del núcleo de la red LSR son usados. No pese que estos elementos siguen siendo enrutadores. El análisis de los paquetes determina si estos sirven como un conmutador de MPLS o como enrutador IP convencional. La función de uno de estos enrutadores es examinar los paquetes entrantes, si se encuentra una etiqueta, éste examinará y seguirá la instrucciones de la misma, y entonces enviará el paquete de acuerdo a las instrucciones, en general, el LSR realiza funciones de intercambio de etiqueta.

Como se mencionó anteriormente los caminos conmutados por etiquetas LSP entre los LER y los LSR son diseñados con características personalizadas de acuerdo al tipo de tráfico, como tal, son muy similares a los caminos de ATM.

En la figura 65 se muestran los LSP establecidos entre los elementos MPLS. Debido a que MPLS trabaja como un protocolo sobrepuesto a IP, los protocolos pueden coexistir en la misma nube sin ninguna interferencia.

**Figura 65. Flujo de datos en una red MPLS.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

La forma más simple de flujo de datos ocurre cuando un paquete es presentado al enrutador de ingreso LER. Muy parecido al centro de correo que clasifica el correo en una sucursal, el enrutador de borde clasifica el tráfico. En MPLS, el proceso de clasificación es llamado clase equivalente de envío, o FEC.

Los LER son puntos de decisión. Los LER son responsables de clasificar el tráfico IP entrante y relacionarlo con la etiqueta apropiada. El LER utiliza varios modos diferentes para etiquetar el tráfico. El ejemplo más simple, los paquetes IP son asignados a una etiqueta y a un FEC usando tablas preprogramadas como por ejemplo la tabla mostrada a continuación:

**Tabla V. Tablas de LER**

| Destino / IP | Número de puerto | FEC | Siguiente Salto | Etiqueta | Instrucción                |
|--------------|------------------|-----|-----------------|----------|----------------------------|
| 199.50.5.1   | 80               | B   | x.x.x.x.        | 80       | Empujar                    |
| 199.50.5.1   | 443              | A   | y.y.y.y         | 17       | Empuja                     |
| 199.50.5.1   | 25               | IP  | z.z.z.z         |          | (No hacer nada; IP Nativo) |

Cuando los paquetes de MPLS salen del LER, éste como destino un LSR donde son examinados por la presencia de etiquetas. El LSR busca en su tabla de envío (denominada base de información de etiquetas LIB o tabla de conectividad) por instrucciones. El LSR intercambiará etiquetas de acuerdo a las instrucciones en la LIB en la tabla VI se muestra un ejemplo de una LIB.

**Tabla VI. LIB**

| Etiqueta de entrada | Puerto de entrada | Etiqueta de salida | Puerto de salida | FEC | Instrucción salto siguiente |
|---------------------|-------------------|--------------------|------------------|-----|-----------------------------|
| 80                  | B                 | 40                 | B                | B   | Intercambiar                |
| 17                  | A                 | 18                 | C                | A   | Intercambiar                |

Al egreso de la red, el LER remueve el encabezado de MPLS y envían el paquete a una red IP. El intercambio de etiquetas simplifica grandemente el flujo de paquetes en una red MPLS.

El LER desempeña muchas funciones de análisis de paquete: mapeando la capa dos a MPLS, y mapeando MPLS a la capa 3, clasificando tráfico con una granularidad grande. Adicionalmente decide que tráfico se convierte en un paquete de MPLS. Un método de decisión es llamado modo de disparo. Utilizando este método cuando un número determinado de paquetes son asignados a un mismo destino dentro de una ventana de tiempo el enrutador determina que un flujo de tráfico, y reenrutara este flujo para ser procesado como MPLS.

### **3.6.8 Distribución de etiquetas en MPLS**

Los conmutadores deben ser entrenados, ellos deben aprender todas las reglas y cuando aplicarlas. Existen dos métodos para hacer estos

conmutadores. Uno de los métodos utiliza una programación rígida, es similar a cuando un enrutador es programado para hacer enrutamiento estático.

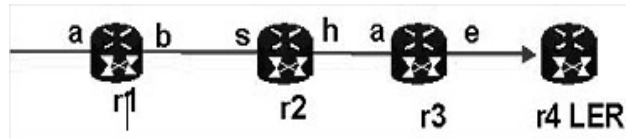
La programación estática elimina la habilidad de re-enrutar dinámicamente o administrar el tráfico.

Las redes modernas cambian de una forma dinámica. Para acomodar esta necesidad, muchos ingenieros de red han escogido usar el segundo método: señalización y distribución de etiquetas dinámica. Ese tipo de distribución puede utilizar uno de varios protocolos, con cada uno se pueden obtener ventajas o desventajas. Debido a que esta es una tecnología emergente, no hemos podido ver un panorama claro en el sentido de que protocolo es el dominante. Aún así independientemente de la selección del protocolo y sus funciones, el concepto básico de distribución de etiquetas y señalización permanecen consistentes en los protocolos.

Como mínimo los conmutadores de MPLS deben aprender cómo pasar paquetes entrantes con etiquetas. A veces esto es llamado una tabla de conexión cruzada. La mayor ventaja de usar tablas de conexión cruzada en lugar de enrutamiento es que estas pueden ser procesadas en la capa de enlace, donde procesamiento es considerablemente más rápido que el enrutamiento.

Empezaremos nuestra discusión usando la red simple de la figura 66 con cuatro enrutador es. Cada enrutador tiene puertos designados. Para una mejor ilustración a los puertos se les han dado y identificadores simples tales como a, b, s, h. Estos identificadores de puerto son específicos para cada enrutador. Los datos bien de la entrada a de r1 hacia la entrada de r4.

**Figura 66. Red ejemplo de MPLS.**

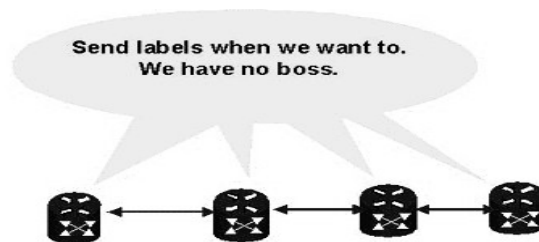


Fuente: [www.convergedigest.com/tutorials/mpls2/page1 .htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

### 3.6.8.1 Control de distribución de etiquetas

Existen dos formas o modos para llenar estas tablas. Cada enrutador puede escuchar a las tablas de enrutamiento, hacer su propia tabla de conexión cruzada, e informar a los otros de su información. Estos enrutador es que estarían operando independientemente. El control independiente ocurre cuando no existe un administrador designado de etiquetas, y cuando cada enrutador tiene la habilidad de escuchar a los protocolos de enrutamiento, generar tablas de conexión cruzada y distribuirlas.

**Figura 67. Control independiente.**

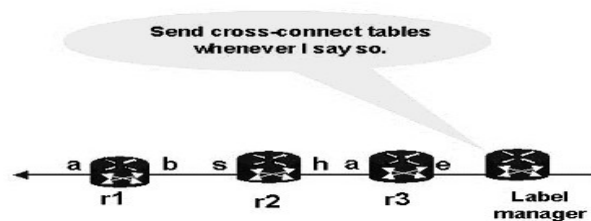


Fuente: [www.convergedigest.com/tutorials/mpls2/page1 .htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

El otro modelo es control ordenado como se muestra la figura en el modo de orden controlado, un enrutador, típicamente el conmutador de egreso es responsable de la distribución de etiquetas.

Cada uno de los protocolos tiene sus detalles. El protocolo de control independiente provee una convergencia de red más rápida. Cualquier enrutador que escuche de un cambio de enrutamiento puede pasar la información a todos los demás. La desventaja es que no hay ningún punto de control de tráfico, lo cual hace la ingeniería más difícil.

**Figura 68. Control ordenado.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

El control ordenado tiene la ventaja de una mejor ingeniería de tráfico y un mejor control de la red, sin embargo, sus desventajas son que el tiempo de convergencia es más lento y que el administrador de etiquetas es el punto único de falla.

Dentro del control ordenado, existen tres métodos para establecer la distribución de etiquetas. Estos son llamados corriente abajo no solicitado y bajo flujo en demanda.

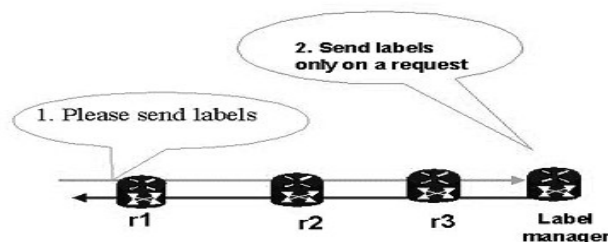
**DOU.** En figura 68, vimos que las etiquetas eran empujadas a los enrutadores corriente abajo. Esto basado en la decisión del enrutador administrador. Cuando las etiquetas son enviadas de forma no solicitada por el enrutador administrador, se conoce a este procedimiento como disparo de corriente abajo no solicitado (DOU).

Por ejemplo: el administrador de etiquetas puede usar un punto de disparo (tal como un intervalo de tiempo) para enviar las etiquetas o refrescar

los mensajes cada 45 segundos. O, puede usar un cambio de las tablas standard de enrutamiento como disparador, cuando un enrutador cambia, el administrador de etiquetas puede enviar actualizaciones de etiquetas a todos los enrutadores afectados.

**DOD.** Cuando las etiquetas son pedidas, estas son haladas en demanda, así este método ha sido llamado halado o corriente abajo en demanda (DOD). Nótese en la figura 69, que en el primer paso las etiquetas son pedidas y en el segundo paso las etiquetas son enviadas.

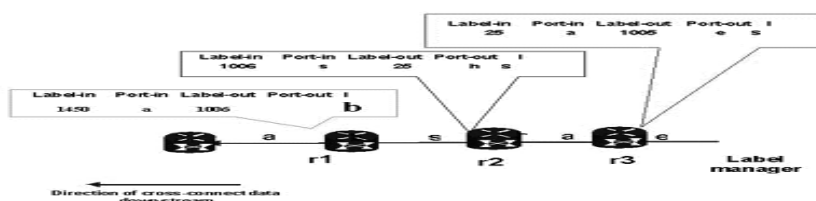
**Figura 69. DOD.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

No importando si las etiquetas llegan vía control independiente o controlado, o vía DOD o DOU, el conmutador de etiquetas (LSR) crea una tabla de conexión cruzadas similar a la mostrada en la figura 70.

**Figura 70. Tablas de conexión cruzada creadas por los enrutadores.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).



Las tablas de conexión son enviadas del enrutador r3 al r1. Los encabezados dicen: etiqueta de entrada, puerto de entrada, etiqueta de salida, puerto de salida e instrucción (I). En este caso, la instrucción es la intercambiar (S). Es importante notar que las etiquetas y las tablas de conexión cruzada son específicas del enrutador.

Después de que las tablas de conexión cruzada son cargadas, los datos pueden fluir del enrutador 1 al 4 con cada enrutador siguiendo sus instrucciones de intercambiar las etiquetas.

Hasta ahora hemos aprendido que los enrutadores necesitan de tabla de conexión cruzada en orden de hacer decisiones de conmutación. Los enrutadores pueden recibir estas tablas de sus vecinos vía control independiente o por control ordenado.

Con estos conceptos básicos entendidos, existen conceptos más avanzados que comprender pro ejemplo, ¿como son enviadas estas etiquetas a los enrutadores? ¿Qué vehiculo se utiliza para transportar esta etiqueta? ¿Cómo se envía la información de calidad de servicio a los enrutadores?

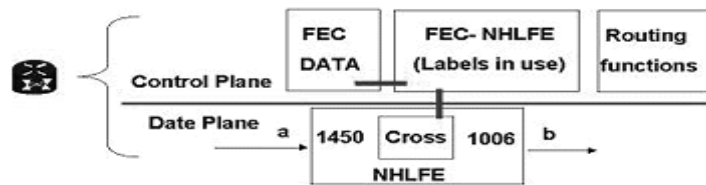
Recordando el paquete de MPLS lleva las etiquetas, sin embargo, los paquetes no tiene un campo que informe al enrutador como procesar el paquete para calidad de servicio.

Recordando que el trafico puede ser separado en grupos llamados clases equivalentes de envío (FEC) y que un FEC puede se asignado a un camino conmutado por etiquetas (LSP), podemos hacer la ingeniería de trafico forzando FECS de alta prioridad en LSP de gran calidad y los FEC de baja prioridad en LSP de menos calidad . El mapeo del tráfico utilizando

diferentes estándares de QoS causara que la distribución de etiquetas y el mapeo sea más complejo.

La figura 71 muestra un esquema de lo que pasa dentro de un LSR. Existen dos planos: el plano de datos y el plano de control. Los paquetes etiquetados entran con una etiqueta de 1450 en el puerto a y salen por el puerto b con etiquetas 1006. esta función toma lugar en la tabla de conexión cruzada, esta tabla puede también ser llamada tabla del siguiente salto (NHLFE).

**Figura 71. Tablas internas de LSR.**



Fuente: [www.convergedigest.com/tutorials/mpls2/page1.htm](http://www.convergedigest.com/tutorials/mpls2/page1.htm).

Esta base de datos no es una base del tipo auto soportada, esta se conecta con dos bases de datos adicionales en plano de control: la base de datos de la FEC y la base de datos de FEC a NHLFE. La base de datos de la FEC contiene, como mínimo, la dirección IP de destino, pero también puede contener características de tráfico y requerimientos de procesamiento de paquetes. Los datos de esta base deben estar relacionados con una etiqueta: el proceso de relacionar un FEC con una etiqueta se le conoce como relación.

He aquí un ejemplo de cómo son asignados los FEC y las etiquetas:

**Tabla VII. Base de datos FEC.**

| <b>FEC</b>   | <b>Protocolo</b> | <b>Puerto</b> |                                 |
|--------------|------------------|---------------|---------------------------------|
| 192.168.10.1 | 06               | 443           | Entrega de paquetes garantizada |
| 192.168.10.2 | 11               | 69            | Mejor esfuerzo                  |
| 192.168.10.3 | 06               | 80            | Carga controlada                |

**Tabla VIII. FEC a NHLFE.**

| <b>FEC</b>   | <b>Etiqueta de entrada</b> | <b>Etiqueta de salida</b> |
|--------------|----------------------------|---------------------------|
| 192.168.10.1 | 1400                       | 100                       |
| 192.168.10.2 | 500                        | 101                       |
| 192.168.10.3 | 107                        | 103                       |

**Tabla IX. NHLFE.**

| <b>Etiqueta de entrada</b> | <b>Etiqueta de salida</b> |
|----------------------------|---------------------------|
| 1400                       | 100                       |
| 500                        | 101                       |
| 107                        | 103                       |

Como podemos apreciar los paquetes pueden ser rápidamente procesados cuando entran al plano de datos, solo si las etiquetas están

relacionadas a un FEC. Sin embargo, muchos procesos de fondo deben ser aplicados al tráfico de datos fuera de línea antes de que la tabla de conexión cruzada pueda ser establecida.

### **3.7 Evolución de la transmisión en fibra óptica**

La tecnología de transmisión tuvo sus inicios de forma experimental en el siglo diecinueve, pero ha tenido un avance rápido a partir de la segunda mitad del siglo veinte con la invención del fibroscopio, que halló utilidad aplicación en la industria y en la medicina, tales como las cirugías laparoscópicas.

Después de que la viabilidad de transmitir luz a través de fibra fue establecida, el siguiente paso en el desarrollo de la fibra óptica fue encontrar una fuente de luz lo suficientemente fuerte y colimada. El diodo emisor de luz LED y el láser son los que más se acercaron a estos requerimientos. Los láser pasaron diferentes etapas que culminaron con los láser semiconductores utilizados actualmente.

Una de las ventajas de la fibra es enorme ancho de banda que posee. Ventajas adicionales de la fibra sobre el cobre son las habilidades de llevar información a distancias más grandes, tasas de errores bajas, inmunidad a la interferencia eléctrica y es menos pesada aunque su instalación requiere de procedimientos especiales.

A sabiendas de estas características, los investigadores a mediados de los sesentas propusieron a la fibra óptica como un medio de transmisión viable. Sin embargo existía un obstáculo, y era que la pérdida de potencia o atenuación, vista en el vidrio que ellos estaban usando. Finalmente Corning

produjo las primeras fibras apropiadas para la transmisión. Con una atenuación menor a 20 decibelios por kilómetro.

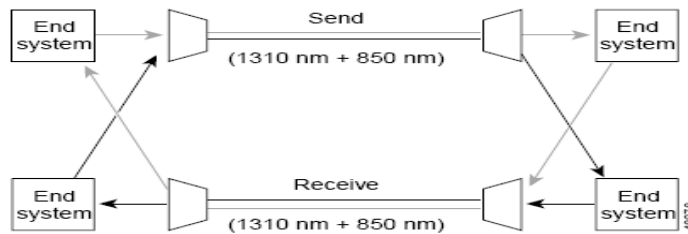
Las innovaciones en el área al principio fueron lentas mientras los gobiernos y las compañías que manejaban las empresas telefónicas eran cautos a la hora de migrar a la nueva tecnología, AT&T estandarizó a la velocidad denominada como DC3 (45MBPS) para fibra multimodo. Pronto después de esto las fibras monomodo mostraron capacidades de transmisión 10 veces mayores e intervalos más largos.

El desarrollo de la tecnología de fibra óptica está estrechamente ligado con el uso de regiones específicas del espectro visible de la luz donde la atenuación óptica es baja. Estas regiones, llamadas ventanas, yacen entre áreas de gran absorción. Los primeros sistemas fueron diseñados para trabajar alrededor de los 850nm, la primera ventana de las fibras hechas a base de sílices. Una segunda ventana (Banda S), a 1310 nm, pronto probó ser superior debido a su atenuación más baja, esta fue seguida por la tercera ventana (Banda C) a 1550nm la que tiene una pérdida óptica menor que la anterior. Hoy la cuarta ventana (banda L) cerca de los 1625 nm está bajo investigación y desarrollo.

### **3.7.1 Desarrollo de la tecnología de DWDM**

WDM empezó a desarrollarse a finales de los ochentas usando dos longitudes de onda ampliamente separadas en las regiones de 1310 y 1550, a veces es llamada WDM de banda ancha. En la figura 87 se muestra un ejemplo de esta implementación. Nótese que no de los pares de fibras es usado para transmitir y uno es usado para recibir. Este es el arreglo más eficiente y más encontrado en los sistemas de WDM.

**Figura 72. WDM de dos canales.**

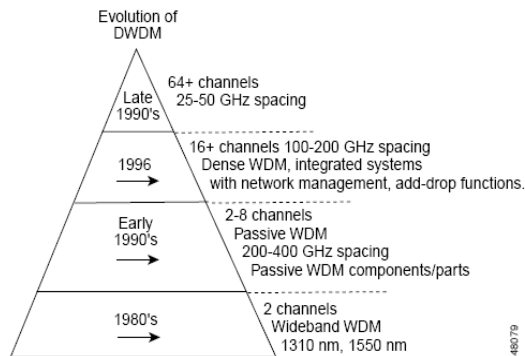


**Fuente:** [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

A principios de los noventa la segunda generación de WDM vio la luz, esta generación llamada WDM de banda angosta, en la cual se usan de dos a ocho canales los cuales están espaciados en intervalos aproximados de 400Ghz en la ventana de 1550. A mediados de los noventa sistemas de WDM densos estaban emergiendo con una cantidad de canales que variaba de 16 a 40 y el espaciamiento variaba de 100 a 200 Ghz.. Para finales de esa misma década los sistemas DWDM habían evolucionado de manera que ya eran capaces de transportar de 64 a 160 canales paralelos , densamente empaquetados en intervalos de 50 e incluso de 25 Ghz.

Como la figura 73 lo muestra la progresión de la tecnología se puede medir en el incremento de las longitudes de onda que se transmiten y en el decremento del tamaño del intervalo que separa estas longitudes de onda. Junto con el incremento en la densidad de longitudes de onda transmitidas el avance de un sistema se puede medir en la flexibilidad en la configuración , mediante las funciones de adición y substracción de señales y la capacidades de administración del sistema.

**Figura 73. Evolución de DWDM.**



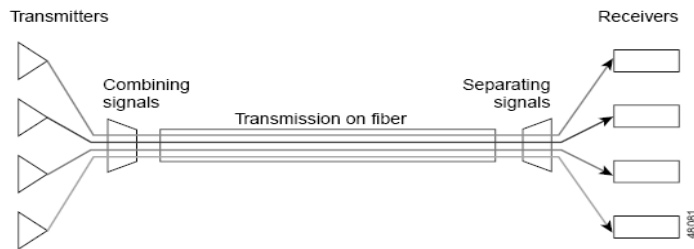
**Fuente:** [http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

El incremento de la densidad de canales resultado de la tecnología DWDM tienen un impacto dramático en la capacidad de transporte de la fibra. En 1995, cuando se hizo la demostración del primer sistema de 10Gbps la tasa de incremento de capacidad fue de una función lineal de aumento de cuatro veces por cada cuatro años a cuatro veces por cada año

### **3.7.2 Funciones de un sistema DWDM**

En su núcleo, DWDM realiza un número pequeño de funciones a nivel de capa física. Estas son esbozadas en la figura 61, que muestra el diagrama esquemático para un sistema de 4 canales. Cada canal óptico ocupa su propia longitud de onda.

**Figura 74. Plano esquemático funcional de DWDM.**



Fuente: [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

El sistema ejecuta las siguientes funciones:

- Generación de la señal. La fuente, un láser de estado sólido, debe proveer un haz estable dentro de un ancho de banda angosto donde se transportan los datos digitales, modulados como una señal análoga.
- Combinación de la señal. Los sistemas modernos de DWDM emplean multiplexores para combinar las señales. Existen algunas pérdidas asociadas con el proceso de multiplexión y demultiplexión de la señal. Esa pérdida es dependiente del número de señales pero puede ser mitigada con amplificadores ópticos, los cuales amplifican todas las longitudes de onda a la vez sin necesidad de convertirlas en señales eléctricas.
- Transmisión de la señal. Los efectos de la interferencia intercanales y la degradación de la señal óptica deben ser tomados en cuenta para la transmisión de datos en fibra óptica, estos efectos pueden ser minimizados controlando algunas variables tales como espaciado de canales, tolerancia de la longitud de onda, y los niveles de potencia de los láseres. Además debe considerarse que a través de un enlace determinado la señal es posible que requiera amplificación.



- Separación de las señales recibidas. En el punto de recibo, las señales multiplexadas deben ser separadas, Aunque la tarea pareciera ser simplemente el proceso opuesto a la combinación de las señales en realidad es un proceso técnicamente complicado.
- Recepción de las señales. Por ultimo la señal demultiplexada es recibida por una foto detectora.

Adicionalmente a estas funciones básicas descritas, un sistema DWDM debe ser equipado con interfaces para los clientes de manera que estos puedan acceder al sistema esto lo hace a través de los transpondedores.

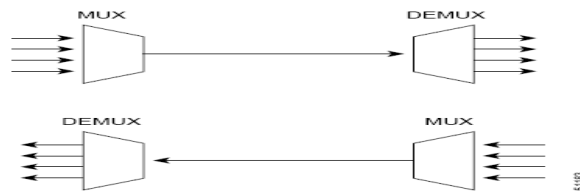
### **3.7.2.1 Multiplexores y demultiplexores**

Debido a que un sistema DWDM envía señales de diferentes fuentes sobre un solo hilo de fibra óptica, el sistema debe incluir algún medio para combinar las señales entrantes. Esto es realizado por un multiplexor, el cual toma las longitudes de onda ópticas de múltiples fibras y hace que converjan en un solo haz. En lado opuesto el sistema debe ser capaz de separar los componentes de luz así estos puedan ser detectados discretamente. Los demultiplexores ejecutan esta función separando el haz percibido en sus componentes de longitud de onda y acoplándolos a fibras individuales. La demultiplexación debe ser ejecutada antes de que la luz sea detectada, debido a que los fotodetectores son inherentemente elementos de banda ancha por lo tanto estos no pueden detectar selectivamente una longitud de onda .

En un sistema unidireccional como el que se muestra en la figura 62, hay un multiplexor en lado de emisión y un demultiplexor en lado de recepción. Se requerirían dos sistemas en cada lado para poder tener una

comunicación bidireccional, además se requerirían dos hilos de fibra individuales.

**Figura 75. Sistema de multiplexión y demultiplexión unidireccional.**



Fuente: [http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

En un sistema bidireccional, existe un elemento que realiza las dos funciones anteriormente descritas de multiplexión y demultiplexión esto en cada extremo con esto se logra la comunicación en un solo hilo de fibra.

**Figura 76. Sistema Full Duplex DWDM.**



Fuente: [http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

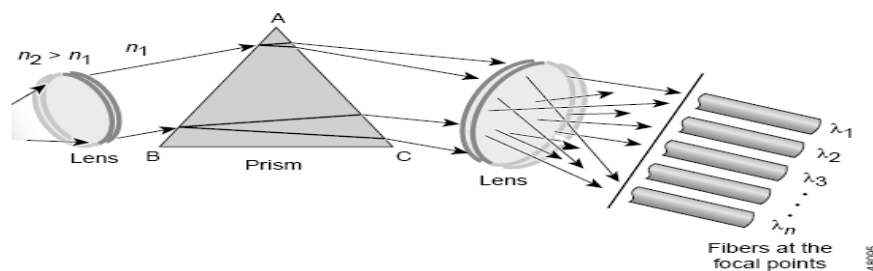
Tanto el multiplexor como el demultiplexor pueden ser activos o pasivos. Los diseños de los elementos pasivos se basan en prismas, rejillas de difracción, o filtros, mientras que los diseños activos combinan elementos pasivos con filtros graduables. El objetivo primordial en este tipo de elementos es el de minimizar la interferencia intercanal y maximizar la separación entre canales. La interferencia intercanales es una medida de que tan bien los

canales esta separados, mientras que la separación de canales se refiere a la habilidad de distinguir cada una de las longitudes de onda.

### 3.7.2.2 Técnicas de multiplexión y demultiplexión

Una forma de multiplexar y demultiplexar luz es a través de un prisma. La figura muestra el caso de demultiplexión. Un haz paralelo de luz policromática choca contra la superficie del prisma; como se puede apreciar cada una de las componentes del rayo es refractada de forma diferente debido a su longitud de onda. Este es el efecto de arcoiris, en el haz de salida cada una de las longitudes de onda está separada de la siguiente por un ángulo. Entonces un lente enfoca cada una de las longitudes de onda al punto de entrada de una fibra. Los mismos componentes pueden ser usados solamente que a la inversa para multiplexar diferentes longitudes de onda en una sola fibra.

**Figura 77. Multiplexor óptico por refracción.**

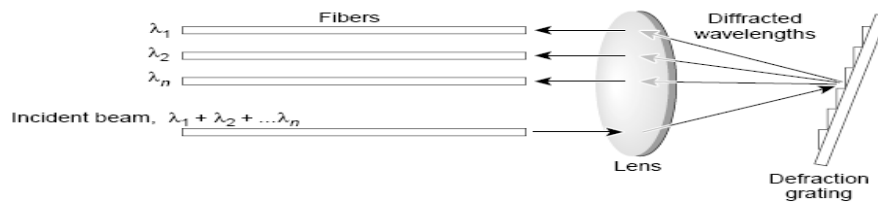


Fuente: [http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

Otro tipo de tecnología se basa en los principios de la difracción y de la interferencia óptica. Cuando un haz de luz policromática choca contra una rejilla difractora, cada longitud de onda es difractada a un ángulo diferente y

por consiguiente a un punto diferente en el espacio. Usando un lente, estas longitudes de onda pueden ser enfocadas a fibras individuales.

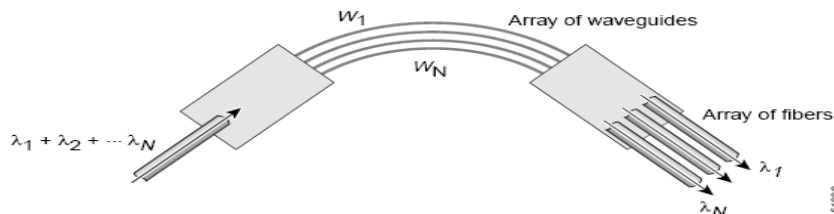
**Figura 78. Multiplexor por rejilla difractora.**



Fuente: [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

Arreglos de guía de onda con rejillas difractoras (AWG), también basan su funcionamiento en la difracción de la luz. Un AWG, a veces llamado un enrutador de longitudes de onda ópticos, constan en de un arreglo de guías de onda curvadas con una diferencia de longitud fija entre canales adyacentes. Las guías de onda esta conectadas a cavidades en la entrada y en la salida, con la luz entra en la primera cavidad, es difractada y entra en el arreglo de guías de onda. Allé la diferencia óptica de longitud de cada guía de onda introduce retardos de fase en la segunda cavidad, donde el arreglo de fibras es acoplado, resultado de este proceso diferentes longitudes de onda teniendo máxima interferencia en diferentes lugares, los cuales corresponden a los puertos de salida.

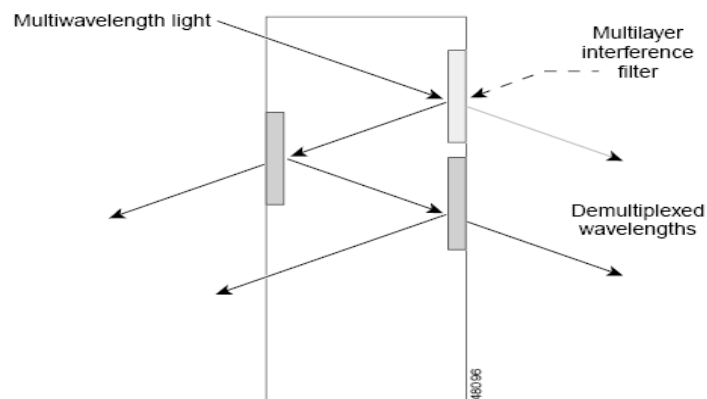
**Figura 79. Enrutador óptico.**



Fuente: [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

Una tecnología diferente usa filtros de interferencia en elementos denominados filtros de película delgada o filtros de interferencia multicapa. Mediante el correcto posicionamiento de los filtros, consistentes en una película delgada, en el camino óptico, las longitudes de onda pueden ser ordenadas. Cada uno de los filtros posee la propiedad de transmitir una única longitud de onda mientras rechaza las demás, colocando estos elementos en cascada, pueden ser demultiplexadas muchas longitudes de onda.

**Figura 80. Multiplexor de filtro de película delgada.**



**Fuentes:**[http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

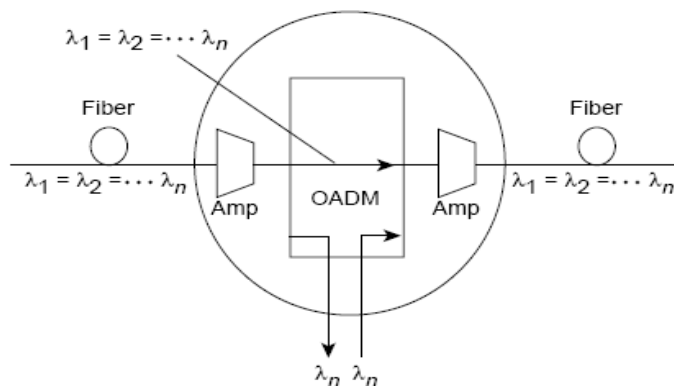
De estos diseños, los de tipo AWG y los filtros de película delgada tienen gran preferencia. Los filtros ofrecen buena estabilidad y aislamiento entre canales a un costo moderado, pero con una gran pérdida de inserción.

Los de tipo AWG son dependientes de la polarización de la luz, y exhiben una respuesta espectral plana y baja pérdida de inserción. Una posible limitación es la sensibilidad a la temperatura así el uso de estos pueda no resultar práctico bajo ciertas condiciones de ambiente. La gran ventaja es que pueden ser diseñados para que les sea posible multiplexar y demultiplexar de forma simultánea. Los de tipo AWG son mejores para cuando hay que manejar gran cantidad de canales, donde el uso de los filtros resulta impráctico.

### 3.7.2.3 Multiplexores de adición y sustracción.

Entre los puntos de multiplexión y demultiplexión de un sistema DWDM como se muestra en la figura 97, existe un área donde en la cual múltiples longitudes de onda existen. A menudo es deseable el hecho de retirar o insertar una o más longitudes de onda en algún punto a lo largo del tramo de fibra. Un multiplexor óptico de adición y sustracción (OADM) realiza esta operación. Más que combinar o separar todas las longitudes de onda, el OADM puede remover algunas mientras pasa otras inalteradas. Los OADM son la clave para conseguir el objetivo de toda red óptica. Los OADM son en varios aspectos muy similares a los ADM de SDH, excepto que solamente señales ópticas son añadidas o sustraídas, y no existe ninguna conversión de óptico a eléctrico. En la figura se muestra la representación esquemática del proceso de inserción y sustracción. Este ejemplo incluye el proceso de pre y post amplificación; estos componentes pueden o no estar presentes en un OADM, dependiendo de su diseño.

**Figura 81. Multiplexor de adición y sustracción.**



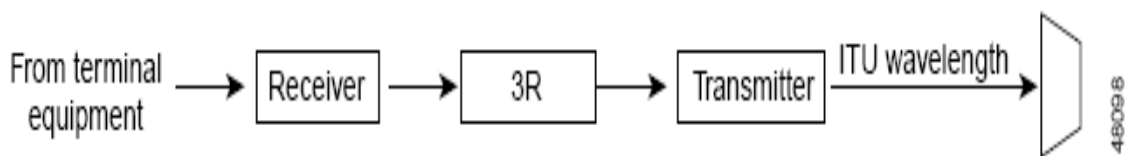
Fuente: [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

Existen dos tipos generales de OADM, los de primera generación que es un elemento físicamente fijo que está configurado para retirar predeterminadas longitudes de onda y añadir otras también predeterminadas. La segunda generación es reconfigurable y tiene la capacidad de seleccionar que longitudes de onda substraen y adiciona.

### 3.7.3 Interfaces de DWDM.

La mayoría de los sistemas DWDM soportan el estándar SDH en cuanto a las interfaces de corto alcance a la cual cualquier cliente que cumpla con la norma se puede conectar. En los sistemas actuales de gran capacidad, es más común una interfaz del tipo OC-48c/STM-16 operando en la ventana de 1310-nm. Adicionalmente otras importantes interfaces de redes metropolitanas son soportadas como la Ethernet (incluyendo la Fast Ethernet y la Gigabit Ethernet), ESCON. El nuevo estándar de Ethernet de 10Gigabit es soportado usando la interfaz de muy corto alcance (VSR) OC-192 entre el equipo de DWDM y el equipo de 10Gigabit Ethernet.

**Figura 82. Funciones del transpondedor.**



**Fuente:** [http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/.doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf).

En el lado del cliente pueden ser terminales SDH o ADM, conmutadores de ATM, o enrutadores. Por el hecho de convertir las señales ópticas que serán multiplexadas los transpondedores son los elementos claves en la gran apertura

de los sistemas DWDM. Dentro de un sistema DWDM un transpondedor convierte la señal que le entrega el cliente de óptica a eléctrica, ya convertida la señal en pulsos eléctricos es usada para estimular el láser del sistema DWDM. Cada transpondedor dentro del sistema convierte la señal de su cliente a una longitud de onda diferente. Después cada una de las señales de cada transpondedor es multiplexada óptimamente. En el punto de entrega del sistema este proceso tiene lugar de forma inversa. Longitudes de onda individuales son filtradas de la señal multiplexada, después de esto se alimenta con ellas a cada uno de los transpondedores , lo cuales convierten la señal óptica a eléctrica y así es entregada en una interfaz estándar al cliente.



## 4 DISEÑO DE LA RED

### 4.1 Introducción

Si no se toma el tiempo para planificar una red, la interconexión mediante el uso de TCP/IP o cualquier tipo de protocolo puede provocar complicaciones no previstas y por lo tanto posible fallas en un diseño. El propósito de la tesis en este punto es de señalar algunos problemas y resaltar los tipos de decisiones que se necesitan tomar para hacer la implementación de una red TCP/IP. En este momento el lector se preguntara que tiene que ver el diseño de una red TCP/IP con el diseño de una red TDM, la respuesta es simple, el objetivo de la red TDM es interconectar varios sitios distantes de una misma empresa transportando trafico TCP/IP encapsulado en Frame Relay, y para poder dimensionar el tamaño de los enlaces entre las diferentes sucursales debemos tener una idea clara de que es lo que se va a transportar en dichos enlaces.

Volviendo a la discusión, la falta de una efectiva planificación de la direcciones de red puede ser una seria limitante en el numero de clientes que seremos capaces de interconectar a través de la red. Por otro lado la falta de coordinación centralizada puede ser causa de una duplicación de nombres y direcciones de recursos de la red. Lo cual puede ser un gran problema a la hora de interconectar dos redes que hasta ese momento estaban separadas o aisladas. Errores en el sistema de direccionamiento pueden tener como consecuencia que no podamos conectarnos a la Internet, otros posibles problemas causados por los errores de direccionamiento es la imposibilidad de hacer la traducción de los nombres

de recursos a direcciones y viceversa debido a que las conexiones a los servidores de DNS no se han podido realizar.

Algunos problemas que proviene de diseñar una red de prisa tienen una solución trivial. Algunos, sin embargo, requieren de tiempo y esfuerzo significativo para corregirlos. Por ejemplo imagine configurar manualmente una red de 3000 usuarios solamente por que el esquema de direccionamiento que ya no soporta las necesidades de crecimiento de una compañía.

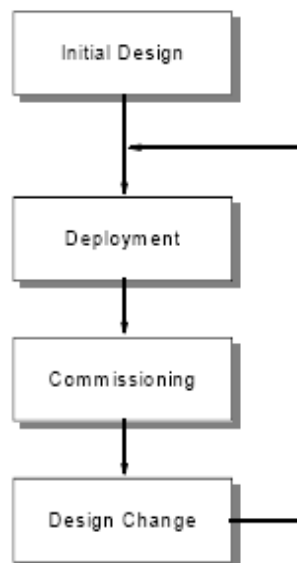
Cuando se encara la tarea de ya sea diseñar una red nueva TCP/IP o permitir que redes existentes interconectarse, como es nuestro caso, existen varios problemas de diseño que necesitan ser resueltos. Por ejemplo, como asignar direcciones a los recursos que serán compartidos en al red, como alterar las direcciones existentes, el uso de un enrutamiento estático o dinámico, como configurar los servidores de denominación y como proteger la red, son todas preguntas que necesita ser respondidas.

Al mismo tiempo el problema de disponibilidad, confiabilidad y respaldo deberán ser consideradas, de acuerdo a como se vaya a manejar y administrar la red.

Debido a la simplicidad y flexibilidad de IP una red puede ser montada de una forma desordenada. Esto es común para una red estar montada de esta manera, y esto puede que trabaje bien para una red pequeña, el problema surge cuando se requieren cambios y la documentación no es hallada. Lo peor de todo, es cuando los equipos de diseño/implementación dejan la organización, a los reemplazos les queda la bastante intimidante tarea de averiguara que es lo que hace la red, como es que embonan las piezas, y donde va que cosa.

Una red IP que no ha sido diseñada de una forma sistemática, invariablemente tendrá problemas desde el principio de la etapa de implementación. Cuando se esta actualizando una red existente, existen redes de legado que necesitaran ser conectadas. Al introducir una nueva tecnología sin considerar las limitaciones de red actual nos pueden guiar a problemas no previstos. Es posible que terminemos tratando de resolver un problema innecesario. El diseño de una red debe tomar lugar antes de la implementación el diseño de una red debe ser constantemente revisado conforme las necesidades de la red van cambiando con el tiempo, como es ilustrado en la figura 83.

**Figura 83. Diagrama de flujo para la implementación y actualización de una red.**

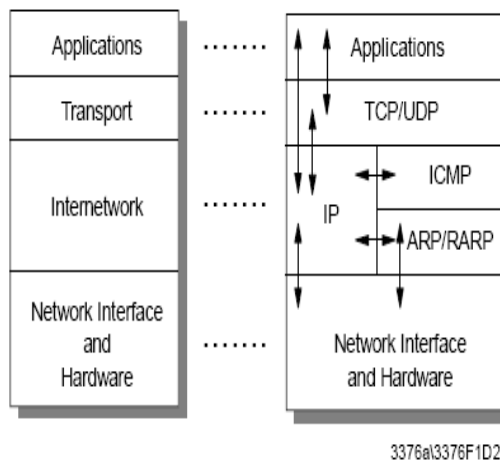


**Fuente:** *IP Network Design, Segunda edición. IBM.*

Un buen diseño también incluye documentación detallada de la red para futuras referencias. Una red bien diseñada debería ser en principio fácil de implementar sin muchas sorpresas.

La metodología de diseño para una red IP es enfoque de arriba hacia abajo. Esta técnica sigue aproximadamente la pila de TCP/IP como se puede observar en la figura 84.

**Figura 84. Modelo de referencia TCP/IP.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

En la parte superior de la pila se encuentra la capa de aplicación. Esta es la primera capa considerada en el diseño de una red. Las dos siguientes son la de transporte y la de red con la capa final que es la capa física.

El diseño de una aplicación es dictada por los requerimientos de la empresa. Las reglas de la empresa, los flujos de los procesos, los requerimientos de seguridad y los resultados esperados, todos estos factores se traducen como las especificaciones de la aplicación. Estos requerimientos no solo afectan el diseño de la aplicación sino que su influencia se filtra hacia todas las capas inferiores que soportan la capa de aplicación.

Una vez que los requerimientos de la capa de aplicación son identificados, se sigue con los requerimientos de las capas inferiores. Por ejemplo si la capa

de aplicación tiene un programa que necesita una respuesta garantizada en menos de dos segundos para cualquier transacción de red, el diseño de red deberá tener en consideración y tal vez implementar la optimización de desempeño como un factor de alta prioridad en el diseño de la red. La capa de enlace necesitara ser diseñada de tal manera que este requerimiento sea cumplido. Por ejemplo, usar el modelo de red plano para la capa de enlace con unos cuantos cientos de clientes basados en Windows puede que no sea el diseño más apto para cumplir con este tipo de requerimientos.

Una vez que el diseño de la red ha sido completado tomando en cuenta la capa de aplicación, se lleva a cabo la implementación de la red.

El diseño de la infraestructura de la red juega una parte importante, ya que esta afecta globalmente el diseño. Un buen ejemplo de esto es la modularidad y estabilidad global de la red IP. Las siguientes son algunas consideraciones en el diseño de una red IP.

#### **4.2 Consideraciones globales de diseño**

Aunque mucho puede ser dicho sobre el diseño de una red que excede los alcances de este trabajo, existen algunos puntos generales que deber ser tomados en cuenta en el diseño de una red que son los siguientes:

- **Escalabilidad.** Una red bien diseñada deberá ser escalable, para crecer junto con los nuevos requerimientos y necesidades de la empresa. La introducción de nuevos clientes, servidores, o redes a la red no debe requerir un rediseño completo de la topología de la red. La topología escogida debe poder acomodar la expansión debida a los requerimientos de la empresa.

- **Estándares abiertos.** El diseño completo y los componentes que integran la red deberán estar basados en estándares abiertos. Los estándares abiertos implican flexibilidad, esto se requiere debido a que puede existir la necesidad de la interconexión de elementos de diferentes fabricantes. Las características propietarias pueden ser apropiadas para llenar requerimientos a corto plazo pero a largo plazo, estas pueden limitar las posibilidades de adquirir nuevo equipo, debido a que estas limitan las opciones a tecnología compatible con ellas.
- **Disponibilidad/Confiabilidad.** Los requerimientos de la empresa seguramente demandaran un nivel de disponibilidad y confiabilidad de la red. Un sistema de transacciones basado en una red que garantiza un tiempo por transacción de dos segundos es inservible si la red esta caída tres de siete días de la semana. El tiempo promedio entre fallas (MBTF) de los componentes debe ser considerada cuando se esta diseñando una red, como también debe ser tomado en cuenta el tiempo promedio para reparar una falla en la red (MTTR). El diseño de una redundancia lógica en una red es tan importante como el diseño de una redundancia física.
- **Modularidad.** Un concepto importante a adoptar es la aproximación modular al construir una red. La modularidad divide un sistema en elementos más pequeños, manejables y hace que la implementación sea más fácil de manejar. La modularidad asegura que una falla en cierta parte de la red pueda ser aislada así esta no traerá abajo la red entera. El uso de la red es optimizado mediante la implementación de un diseño modular. Por ejemplo, añadir un nuevo segmento de red o una nueva aplicación a la red no requerirá un re-direccionamiento de todos los clientes de la red si la red fue implementada mediante el uso del diseño modular.

- **Seguridad.** La seguridad de la red de una organización es un aspecto importante en cualquier diseño, especialmente cuando la red va a tener una interfaz con la Internet. El hecho de considerar los riesgos de seguridad y tomarlos en cuenta durante la fase de diseño es esencial para tener una seguridad relativamente completa dentro de la red. La consideración de la seguridad hasta los últimos pasos de la implementación deja a la red abierta a ataques hasta que todos los hoyos de seguridad hayan sido cerrados, este sería un acercamiento reactivo más que proactivo al problema que termina siendo demasiado costoso. Aunque nuevos hoyos de seguridad pueden ser encontrados mientras los *hackers* se hacen más listos, la solución a los problemas básicos de seguridad pueden ser fácilmente incorporados en la etapa de diseño.
- **Administración de red.** La administración como un factor determinante en el funcionamiento de la red no debe ser tomada en cuenta hasta después de haber construido la red. La administración de la red es importante debido a que provee una manera de monitorear la salud de la red, para cerciorarse de las condiciones de operación, para aislar fallas y configurar elementos para efectuar cambios. La implementación de una estructura de administración debe ser integrada en el diseño de la red desde un principio. El diseñar e implementar una red IP y luego tratar de hacer casar una estructura de administración puede crear problemas innecesarios. Un poco de proactividad en la etapa de diseño puede dar como resultado una implementación efectiva y fácil de los recursos de administración.
- **Desempeño.** Existen dos tipos de medida para el desempeño que debes ser consideradas para la red. Una es el ancho de banda promedio (*throughput*) y la otra es el tiempo de respuesta. La primera es cuanta información puede ser enviada en el lapso de tiempo más

corto posible, mientras que el tiempo de respuesta es cuanto tiempo tiene que esperar el usuario antes de obtener una respuesta del sistema. Ambos factores deben ser considerados cuando se diseñan una red, nos es aceptable diseñar una red solamente para fallar a la hora de cumplir con los requerimientos de la organización. La escalabilidad de la red con respecto a los requerimientos de desempeño deberán ser considerados también, como fue mencionado anteriormente.

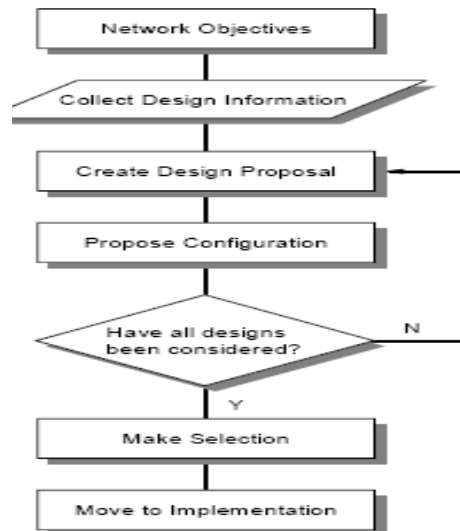
- **Economía.** Un diseño que cumple con el 100% de los requerimientos de la organización pero cuesta el 200% del presupuesto deberá ser revisada. El balanceo de los costos y encontrar la forma de cumplir con los requerimientos de la red es talvez uno de los aspectos más difíciles en un buen diseño de red. La esencia esta en la palabra compromiso. Uno talvez se necesite renunciar a algunas características elegantes de la implementación simplemente para poder cubrir las necesidades básicas de las aplicaciones.

#### **4.2.1 Pasos para el diseño de red.**

A continuación describimos una regla mas o menos general para el diseño de una red IP, este presenta un acercamiento estructurado para analizar y desarrollar un diseño de red para cumplir con las necesidades de una organización.



**Figura 85. Diagrama de flujo para el diseño de una red.**



**Fuente:** *IP Network Design, Segunda edición. IBM.*

#### 4.2.2 Objetivo de la red

¿Cuales son los objetivos de esta red IP? ¿Cuales son los requerimientos que necesitan ser satisfechos? Este paso del proceso de diseño necesita investigación y puede consumir gran cantidad de tiempo. Las siguientes, entre otras cosas, deberán ser consideradas:

- ¿Quienes son los usuarios de la red y cuales son sus requerimientos?
- ¿Que aplicaciones deben ser soportadas?
- ¿La red IP reemplaza un sistema de comunicación ya existente?
- ¿Que pasos deben ser considerador para la migración?
- ¿Cuales son los requerimientos del diseño global?
- ¿Quien es responsable por la administración de la red?

- ¿Debería la red estar dividida en más segmentos?
- ¿Cual es la expectativa de vida de la red?
- ¿Cuanto es el presupuesto?

La información que es requerida para la construcción de una red depende de cada implementación individual que se haga. Sin embargo, los tipos principales de información pueden ser deducidos de los párrafos anteriores donde se describieron las consideraciones globales de diseño de la red. Es importante recolectar información y pasar un tiempo analizándola para desarrollar un entendimiento profundo del ambiente y las limitaciones impuestas sobre el diseño de una nueva red IP.

Sobre el análisis de la información recolectada y los objetivos de la red, se puede idear una propuesta y después optimizarla. Las consideraciones de diseño pueden ser adaptadas para una necesidad omitiendo o haciendo de menos otras. Así la red puede ser:

- Optimizada para desempeño
- Optimizada para ser resistente
- Optimizadas para seguridad

Una vez las prioridades de diseño han sido identificadas el diseño puede ser creado y documentado.

### **4.3 Necesidades de la red.**

Descritos por lo menos los criterios básicos que deben ser tomados en cuenta a la hora de la implementación de una solución de diseño de red pasaremos a describir las aplicaciones y diversas necesidades de cada una de las oficinas que se desean interconectar.

A grandes rasgos el proyecto consisten en la interconexión de varias sucursales de la empresa que están diseminados en la región oriental de Guatemala, mediante enlaces propios, a manera de sustituir los enlaces que se tiene contratados a terceros, la ubicación geográfica es básicamente en los departamentos de El progreso, Zacapa, Chiquimula e Izabal. El proyecto de interconexión de las sucursales en su primera fase, contempla la interconexión de los siguientes sitios:

- Sanarate
- Pasabien
- Panaluya (nodo de concentración)
- Teculután
- Morales
- Chiquimula
- Shoropín

Cada una de las oficinas tiene un sistema de direccionamiento IP segmentado y cada segmento puede contener de acuerdo a la máscara de subred 128 clientes de red estos segmentos pertenecen a una red de clase A. Realmente cada una de las sucursales posee un máximo de 25 estaciones de trabajo y además también cuentan con un servidor local donde corre la parte Gráfica de las diversas aplicaciones que son necesarias para el funcionamiento interno de la oficina, esto con el objetivo de reducir y agilizar la transferencia de datos a través de los enlaces. La actualización de las bases de datos locales demanda una conexión a la base de datos central de todas las aplicaciones la cual se encuentra albergada en un servidor ubicado en las oficinas principales de la empresa, estas bases de datos corren en las plataformas de SQL, y Oracle, y la aplicaciones están desarrolladas en *Power Builder*, siendo esto la mayor parte del trafico que transita a través de los

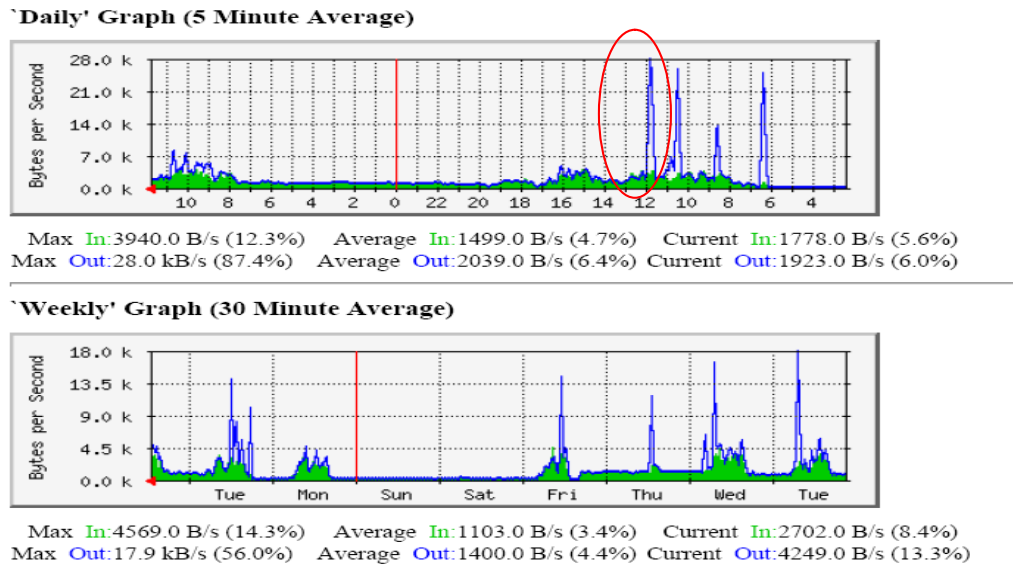
enlaces que proponemos instalar, el comportamiento de este tráfico es por ráfagas de datos esto basados en las Gráficas de tráfico que incluyo mas adelante en el estudio de ancho de banda, además de las necesidades de conexión a nivel de base de datos existen necesidades de comunicación vía telefonía sobre IP, las necesidades operacionales de ancho de banda para la comunicación por este medio se ve satisfecha si se tiene suficiente ancho de banda para alojar dos extensiones de telefonía con compresión G729 que utiliza un ancho de banda de 12 Kbps cada una. Una de estas extensiones tiene marcado directo al centro de atención al cliente y la otra esta programada para que se comunique con la operadora con el objetivo de comunicarse a diferentes puntos de la empresa, también se utiliza un programa de escritorio remoto el cual es utilizado por el encargado de soporte del área para solucionar contingencias de bajo nivel en los servidores y algunas terminales de las oficinas, por último existe el servicio de correo basado en Microsoft Exchange

#### **4.4 Estudio de tráfico**

Una vez identificadas las aplicaciones que se necesitan cada una de las oficinas para su funcionamiento se realizo un estudio del ancho de banda necesario para interconectar las oficinas entre si y también para conectarlas al servidor central de las aplicaciones, esto utilizando la herramienta de MRTG (*Multi Router Traffic Grapher*), continuación mostramos las Gráficas de utilización del ancho de banda disponible por cada una de las oficinas :

Sanarate:

**Figura 86. Gráfica de tráfico de Sanarate.**



. Fuente: Programa MRTG.

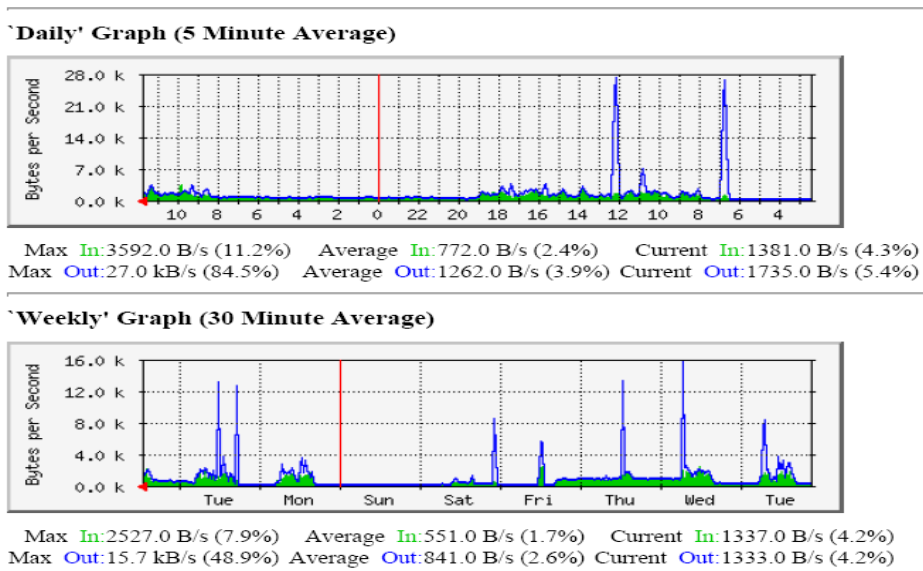
En la figura 86 se puede apreciar el tráfico que pasa a través de la interfaz de Sanarate siendo la marcada con *Out* el tráfico saliente del enrutador e *In* el entrante esto evidencia asimetría en cuanto al tráfico que se maneja en el enlace manteniendo esta tendencia en todos los enlaces.

En la Gráfica obtenida por el MRTG, que Gráfica en un periodo de diario que los picos de mayor tráfico se obtienen entre la once y doce de la mañana llegando a 28KBps, hora en la cual se presenta la mayor demanda en lo que respecta a las consultas de pagos y saldos en las oficinas, de este resultado se puede concluir que para esta oficina debemos aprovisionar un servicio de 256Kbps (de los primeros capítulos recordaremos que la B mayúscula representa Bytes y la b minúscula representa bits por eso los 256 Kbps serían igual a 32 KBps), como información adicional colocamos junto con la Gráfica de tráfico diario el tráfico semanal de la oficina, como es

de suponerse el ancho de banda necesario en esta Gráfica es inferior al descrito por la Gráfica diaria ya que la granularidad de las muestras es mas gruesa que en la Gráfica anterior, estos datos fueron obtenidos del enrutador que recibe el E1 en las oficinas centrales de la empresa, y que esta descrito en la topología de la red como enrutador 1.

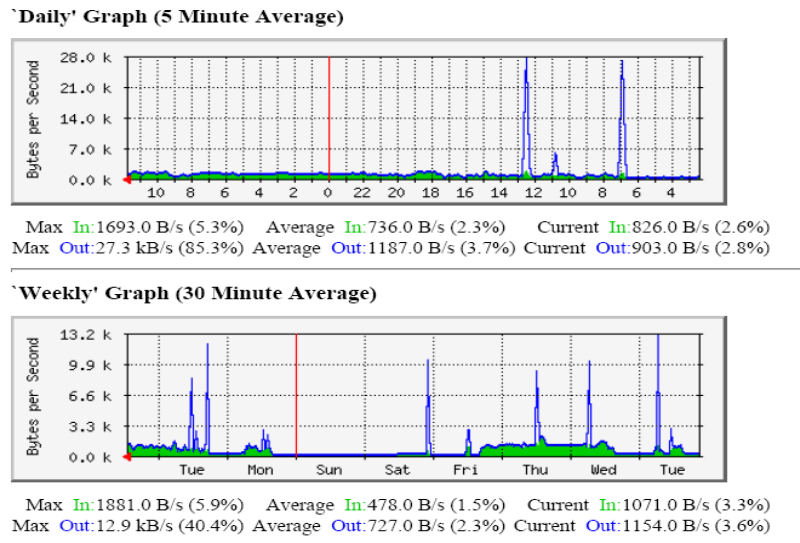
El análisis practicado para esta oficina es extensivo para las demás oficinas comerciales ya que como se puede observar en las demás Gráficas las horas pico y el ancho de banda necesario invariablemente arrojan el mismo resultado, a excepción de la de morales donde el pico máximo es de 21 KBps aún así por cuestiones de posible crecimiento en las necesidades de la oficina se le aprovisionara con un ancho de banda similar a las demás oficina, aprovechando la ventaja de poseer el control sobre la asignación del ancho de banda de cada enlace.

**Figura 87. Gráfica de tráfico de Teculután.**



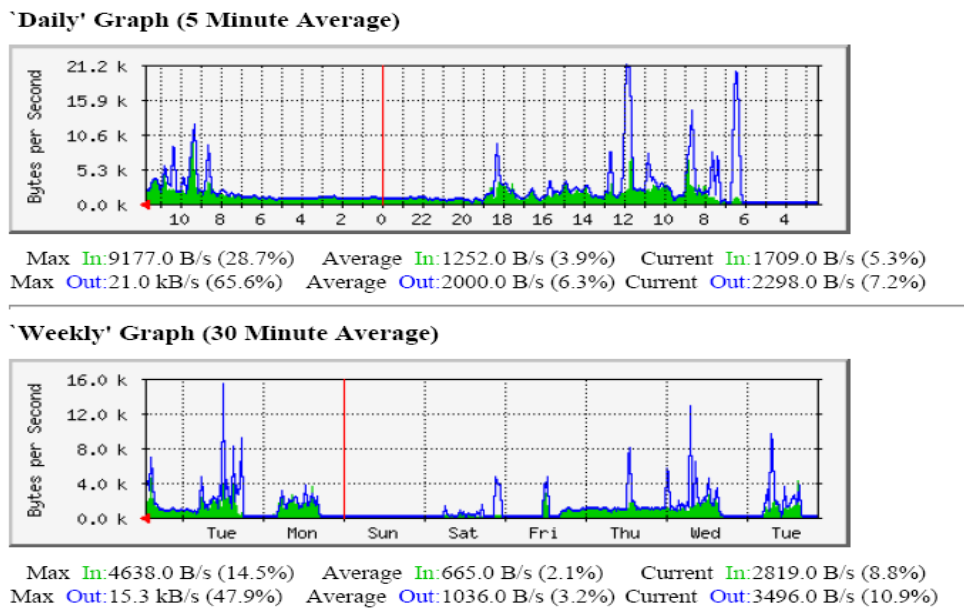
Fuente: Programa MRTG.

**Figura 88. Gráfica de tráfico de Pasabièn.**



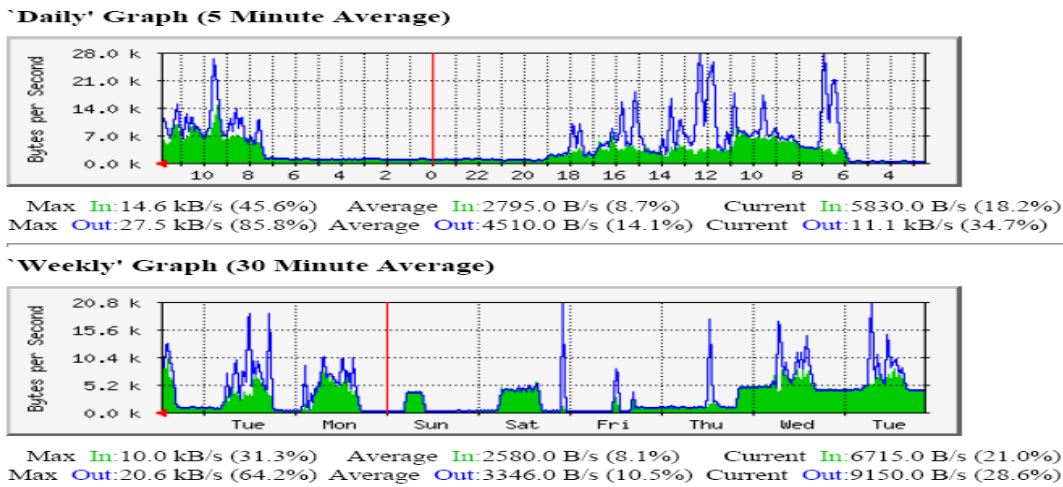
Fuente: Programa MRTG.

**Figura 89. Gráfica de tráfico de Morales.**



Fuente: Programa MRTG.

**Figura 90. Gráfica de tráfico de Chiquimula.**



**Fuente: Programa MRTG.**

#### **4.5 Descripción de la solución**

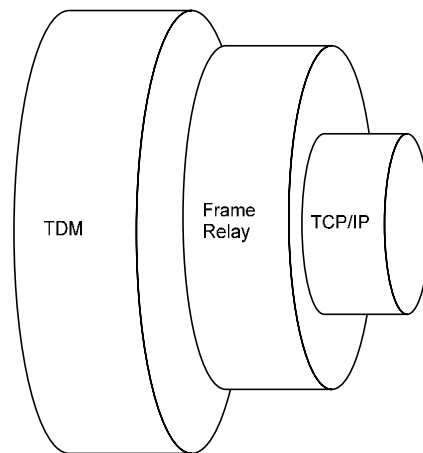
Como hemos explicado con anterioridad el objetivo de el proyecto de es el de sustituir hasta donde sea posible los enlaces existentes, contratados a terceros, uno de los factores determinante en el diseño y la implementación de cualquier tipo de red es la infraestructura que con que cuenta la empresa para poder proyectar una solución eficiente en todo sentido, tanto económico como técnico, en este caso la empresa posee un tendido de fibra que va desde el departamento de El Progreso en el municipio de San Antonio la Paz hasta el sitio de interconexión con el Arcos Uno en Puerto Barrios en el departamento de Izabal, este es un recurso de infraestructura determinante para tomar en cuenta en el diseño de la solución, ya que en el tendido se cuenta con fibras inactivas que pueden ser utilizadas y el único gasto que se tendría sería el de las derivaciones del tendido principal hasta donde están los puntos a interconectar.



Por cuestiones legales, la introducción de la fibra óptica dentro del perímetro del departamento de Guatemala resulta demasiado dificultoso por lo cual dentro de la solución debemos tomar en cuenta un punto de interconexión entre nuestros enlaces y un único enlace con un operador local de telecomunicaciones.

Después de realizar los estudios de las necesidades de ancho de banda de cada una de las oficinas y de la naturaleza del tráfico que deberá ser transportado en los enlaces que se pretenden instalar, se decidió utilizar una solución basada en Frame Relay sobre una red TDM, tal y como lo muestra la figura 91.

**Figura 91. Proceso de encapsulación de la información.**





En la figura 108 se muestra la topología de la red, la topología física de la red es de bus, se eligió esta topología física debido a que con esta distribución se utilizan solamente dos fibras del tendido principal para aprovechar al máximo el medio de transmisión que es de naturaleza escasa y cara, sin embargo la topología de lógica es en estrella debido a que todo el tráfico se dirige a la interfaz de salida ubicada en el nodo de Sanarate. En este nodo se concentra toda la información que será transmitida a las oficinas centrales de la empresa por medio de un enlace contratado a un operador local, este último enlace fue contratado debido a la falta de infraestructura hasta las oficinas centrales de la empresa.

En cada una de las sucursales se instalaran nodos de inserción a la red, en cada uno de los nodos configuraron 3 tipos de parámetros:

- Parámetros Administrativos.
- Parámetros de interfaces Tramadas.
- Parámetros de interfaces no tramadas.

#### **4.5.1 Parámetros Administrativos**

Los parámetros Administrativos configurados son el número de identificador del nodo; parámetros de sincronización (Lista de selección de reloj), Configuración de módulos de interfaz; verificación de estado de circuitos de memoria interna, Voltajes medidos en el bus de alimentación del nodo, y operación de indicadores LED. Adicionalmente se actualizó el programa de operación de los módulos LAN Bridge de los mininodos EH2541 v 1.0 a la versión 1.2, esta versión se requiere para poder configurar el temporizador del módulo LAN en pasos de 4min.

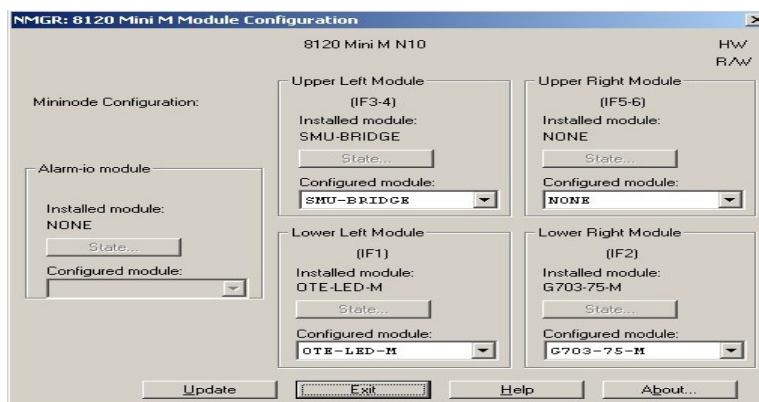
**Tabla X. Resume parámetros administrativos.**

| NODO       | Node ID | IF 1      | IF2                | IF3                  | IF4                       |
|------------|---------|-----------|--------------------|----------------------|---------------------------|
| Sanarte    | 10      | Ote-LP    | G.703-75-M<br>(E1) | SMU Bridge 10BaseT)  | Vacio                     |
| Teculután  | 20      | Ote-LP    | Ote-LED-M          | SMU Bridge (10BaseT) | Vacio                     |
| Pasabien   | 30      | Ote-LED-M | Ote-LED-M          | SMU Bridge (10BaseT  | Vacio                     |
| Panaluya   | 40      | Ote-LED-M | Ote-LP             | SMU Bridge (10BaseT  | Vacio                     |
| Chiquimula | 50      | Ote-LP    |                    | SMU Bridge (10BaseT  | SMU<br>Bridge<br>(10BaseT |

#### 4.5.2 Parámetros de interfaces Tramadas y no tramadas

Se Gráfica a continuación la pantalla del gestor de elementos utilizado para configurar el elemento de red:

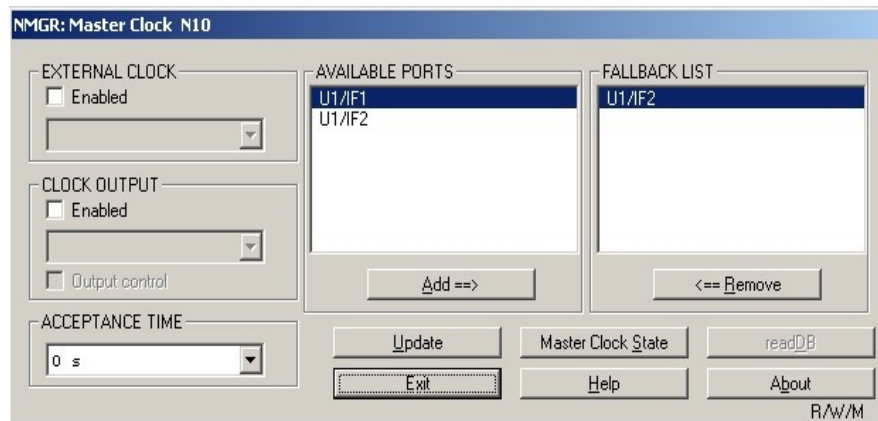
**Figura 93. Pantalla de asignación de interfaces.**



Fuente: Programa NMS de TELLABS.

En la figura 93 se aprecia la configuración de las interfaces del nodo de Sararate, el cual utilizaremos de ejemplo ya que posee una de cada una de las interfaces utilizadas en el proyecto.

**Figura 94. Pantalla de configuración de reloj.**

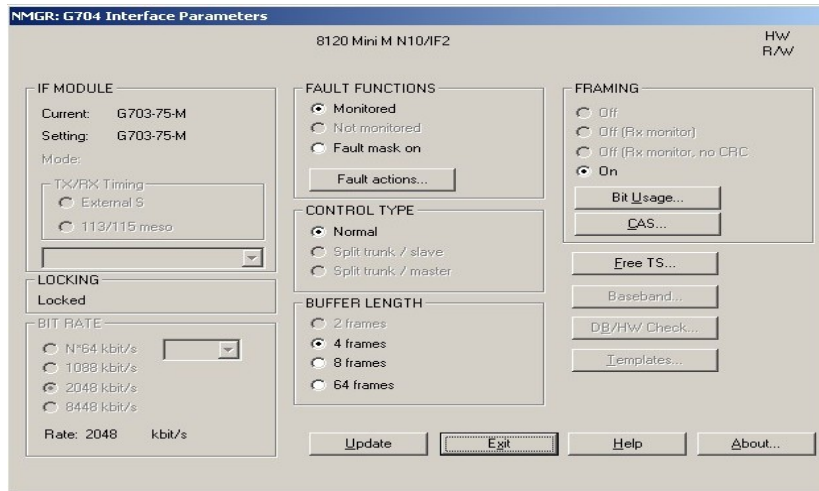


**Fuente: Programa NMS de TELLABS.**

El reloj de el nodo será tomado de la interfaz numero 1 como lo indica la Fig. 94 que en este caso de acuerdo con los parámetros administrativos el la G.703 (E1) de la cual se derivara también el reloj para los demás nodos.

La configuración de la interfaz E1 a 75 ohm en Sanarate se resume a continuación en la figura 95.

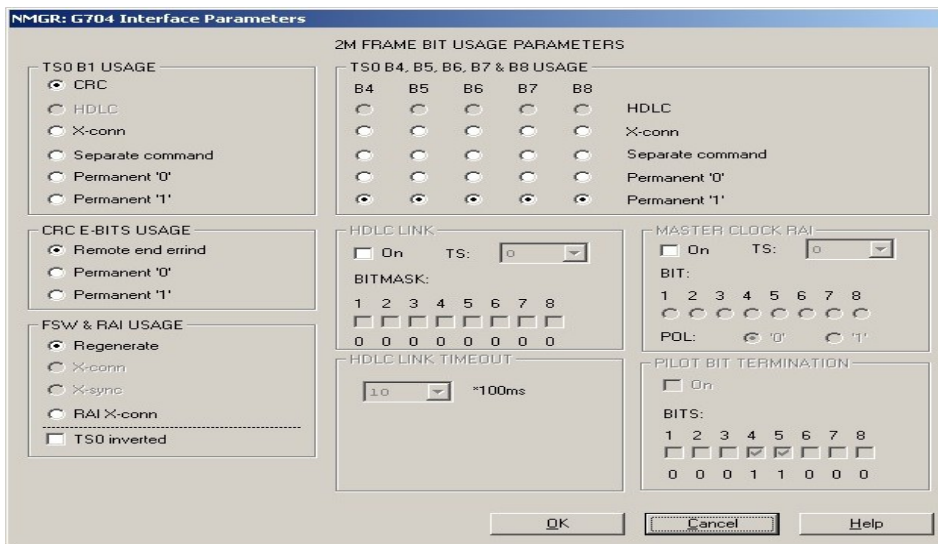
**Figura 95. Pantalla de configuración interfaz E1.**



**Fuente: Programa NMS de TELLABS.**

La configuración de la trama se realizó como indica la figura 112: (no usa CAS).

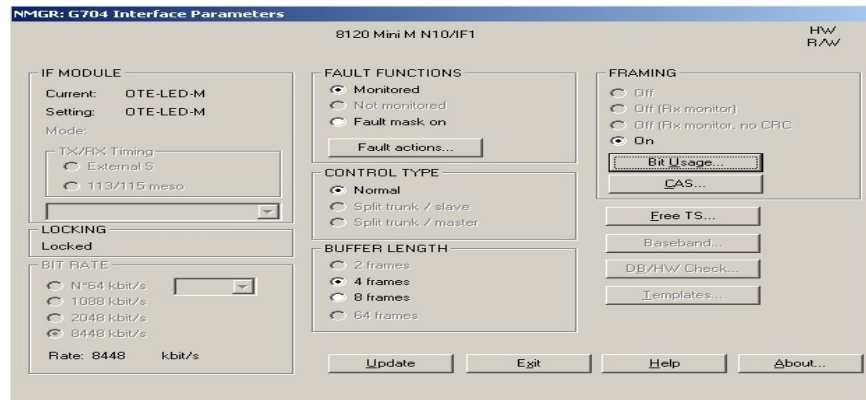
**Figura 96. Pantalla de configuración de bits de entramado interfaz E1.**



**Fuente: Programa NMS de TELLABS.**

La interfaz óptica (OTE-LP OTE-LED Interfaz óptica láser y LED correspondientemente), se configura como indica la figura 97.

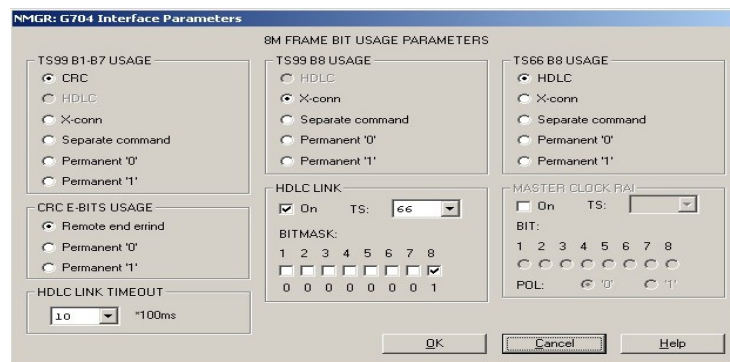
**Figura 97. Pantalla de configuración interfaz óptica.**



**Fuente: Programa NMS de TELLABS.**

La trama utilizada por la interfaz de 8Mbps (OTE –LED/LP) se configura como indica la figura 98.

**Figura 98. Pantalla de configuración de bits de entramado interfaz óptico.**

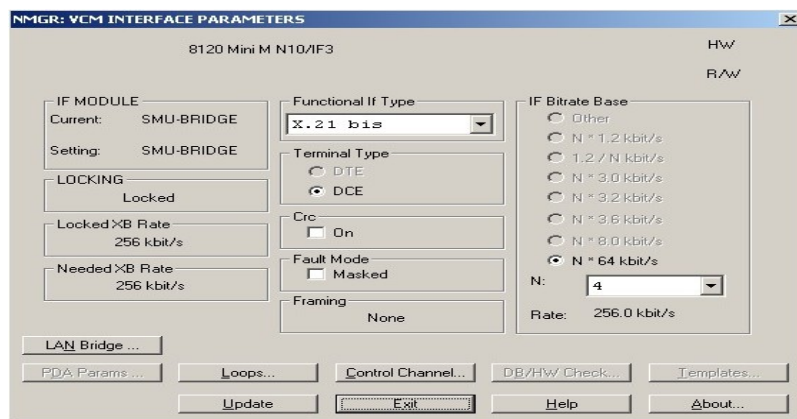


**Fuente: Programa NMS de TELLABS.**

### 4.5.3 Interfaces no tramadas

La configuración de la unidad VCM donde se insertan los módulos LAN Bridge y/o V.35 en el nodo 8120 se configura como se muestra a continuación en la Fig. 99.

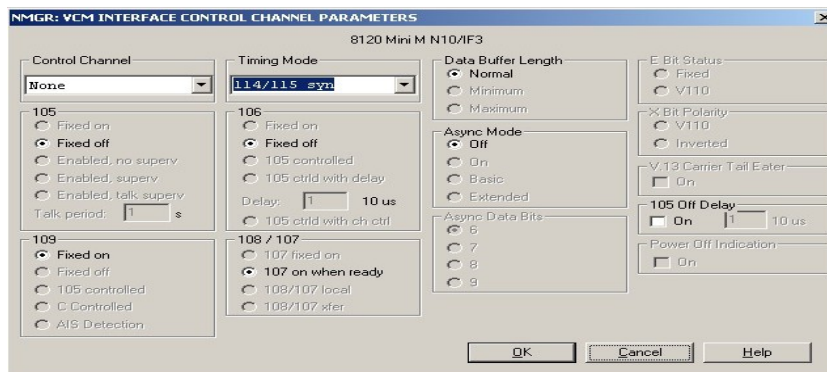
**Figura 99. Pantalla de configuración modulo base VCM.**



**Fuente: Programa NMS de TELLABS.**

Se configura a una tasa de bit de 256 kbps como se muestra en la figura 99 y las señales de control se configuran como indica la figura 100.

**Figura 100. Pantalla de configuración de señales de control modulo Puente.**

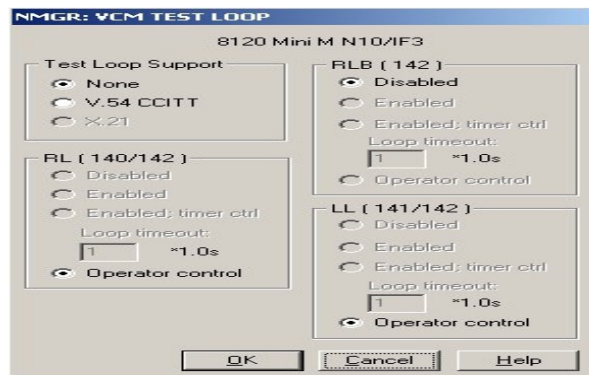


**Fuente: Programa NMS de TELLABS.**



La configuración de lazos posibles se realiza de la siguiente forma como indica la figura 101:

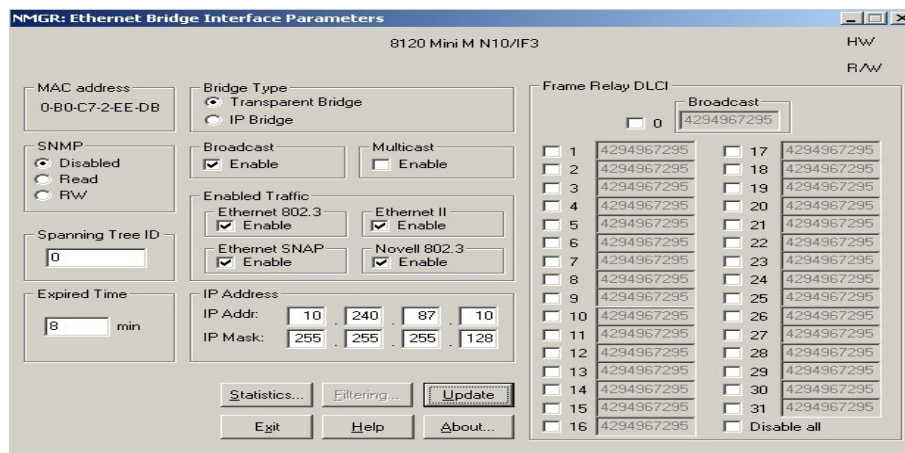
**Figura 101. Pantalla de configuración de los lazos de prueba internas.**



Fuente: Programa NMS de TELLABS.

La configuración del módulo LAN se realiza de acuerdo con las tablas de direccionamiento de las OC. Se muestra en la figura 102 la configuración del módulo LAN de Sanarate:

**Figura 102 Parámetros Frame Relay e IP de la interfaz puente.**

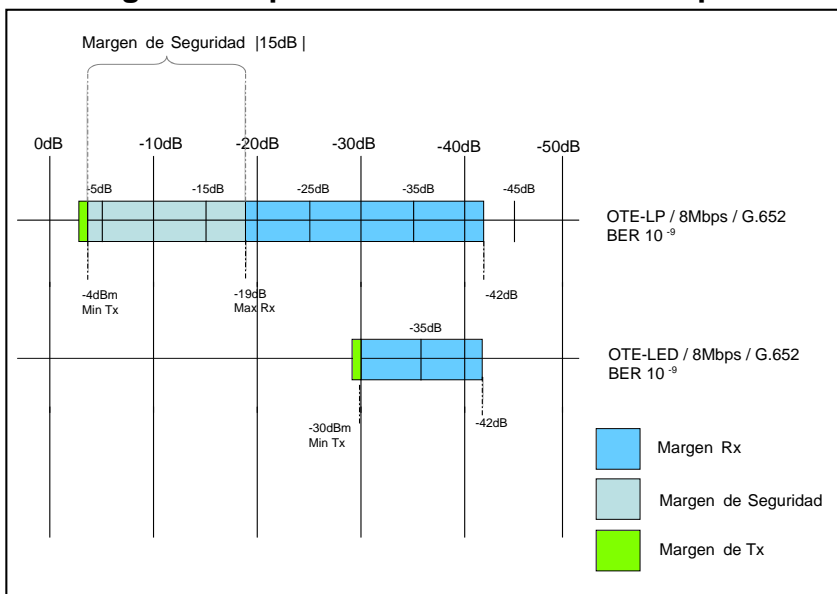


Fuente: Programa NMS de TELLABS.

Se deshabilitan todos los DLCI durante el comisionamiento, pero a la hora de poner en servicio se debe habilitar el primer DLCI con un número válido.

Como hemos detallado en los parámetros administrativos cada uno de los nodos de inserción poseen dos interfaces ópticas con las cuales se logra la comunicación con los nodos adyacentes, en el proyecto se utilizaron dos clases de interfaces ópticas, en las distancias más grandes a 30 kilómetros se utilizaron interfaces del tipo Láser en las distancia inferiores a los 30 kilómetros se utilizaron interfaces del tipo Led, cada una de las interfaces se utilizo basado en las características de potencia de la interfaz y de perdidas en la fibra las cuales fueron medidas directamente mediante instrumentos especializados tales como OTDRs y medidores de potencia, en la figura 103 se muestran las características de potencia de ambas interfaces ópticas.

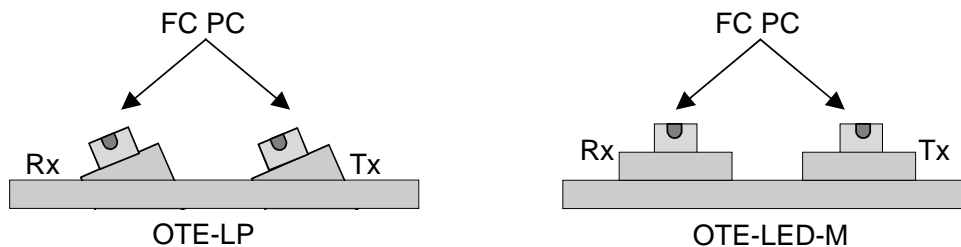
**Figura 103. Márgenes de potencia de las interfaces ópticas.**



Fuente: Manual de mininodo 8120.

Las interfaces se diferencian físicamente por la disposición de los conectores como se muestra en la figura 104.

**Figura 104. Disposición física de las interfaces ópticas.**



**Fuente: Manual de mininodo 8120.**

Además de las interfaces ópticas cada uno de los nodos está equipado con interfaces Puente Ethernet en modo transparente, en el capítulo dos explicamos el funcionamiento de este tipo de dispositivo, estos soportan los protocolos 802.3, SNAP, Novell 802.3 y Ethernet II, que son las interfaces que utilizaremos para introducir el tráfico Ethernet a los circuitos de transmisión, estas interfaces son las que hacen el encapsulamiento *Frame Relay* de la información, como indicamos anteriormente en esta interfaz es donde se le asigna permanentemente el DLCI que identifica el origen de la información. Como es de suponerse en nuestro caso la clase de circuito que se utiliza es un PVC.

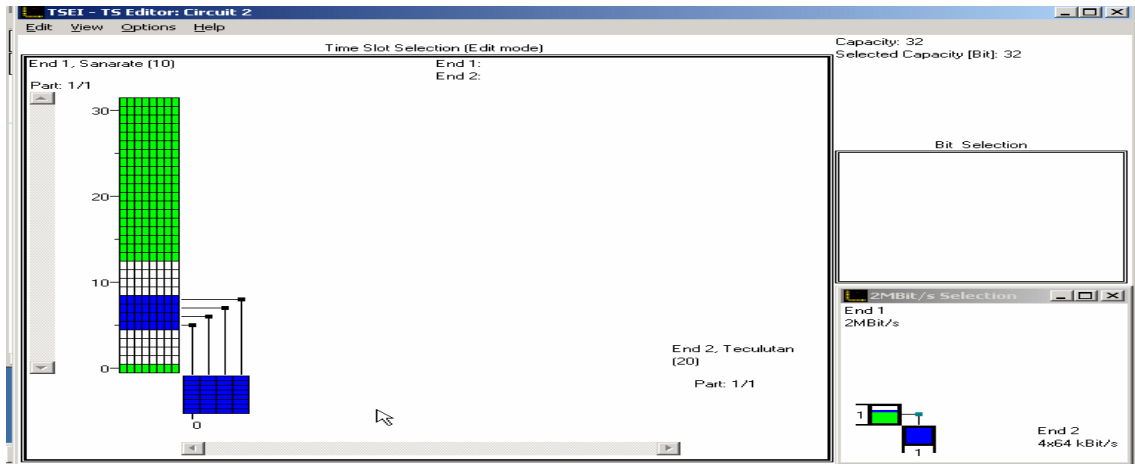
La encapsulación en TDM se hace en el nodo mediante el sistema de gestión al asignar las ranuras de tiempo, a cada uno de los circuitos en la matriz de Cross Conexión de los nodos intermedios hasta llegar a la interfaz a la interfaz tramada G.703 (E1) de Sanarate.

En la tabla XI se muestra un resumen de la asignación de las interfaces terminales de los circuitos en cada uno de los nodos, detallando su capacidad su dirección o identificador de *Frame Relay* y el numero de ranuras de tiempo en el cual están alojados cada uno de estos en la interfaz tramada de Sanarate, que dicho sea de paso para poder soportar esta configuración tuvo que ser declarada en el sistema de gestión como MUAP ( Multiple User Access Point).

**Tabla XI. Tabla resumen de asignación de interfaces y circuitos.**

| <b>Nombre</b> | <b>Capacidad en kbps</b> | <b>DLC I</b> | <b>Punto terminal 1</b>  | <b>Punto terminal 2</b>  | <b>Time-Slots asignados en E1 Sanarate</b> |
|---------------|--------------------------|--------------|--------------------------|--------------------------|--|
| OCSanarate    | 256                      | 16           | SMU Bridge<br>U1/IF3 N10 | G.703-75-M<br>U1/IF1 N10 | 1,2,3,4                                    |
| OCTeculután   | 256                      | 17           | SMU Bridge<br>U1/IF3 N20 | G.703-75-M<br>U1/IF1 N10 | 5,6,7,8                                    |
| OCPasabien    | 256                      | 18           | SMU Bridge<br>U1/IF3 N30 | G.703-75-M<br>U1/IF1 N10 | 9,10,11,12                                 |
| OCMorales     | 256                      | 19           | SMU Bridge<br>U1/IF3 N40 | G.703-75-M<br>U1/IF1 N10 | 13,14,15,16                                |
| OCChiquimula  | 256                      | 20           | SMU Bridge<br>U1/IF3 N50 | G.703-75-M<br>U1/IF1 N10 | 17,18,19,20                                |
| OCShoropin    | 256                      | 21           | SMU Bridge<br>U1/IF4 N50 | G.703-75-M<br>U1/IF1 N10 | 21,22,23,24                                |

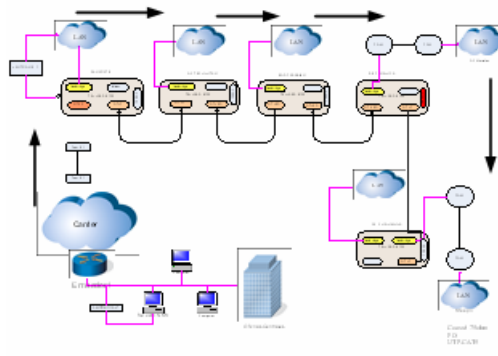
**Figura 105. Asignación de las ranuras de tiempo de los circuitos en la interfaz G.703 del nodo de Sanarate.**



Fuente: Programa NMS de TELLABS.

Como se menciona en los parámetros administrativos del nodo de sanarate se deriva el reloj de sincronía, este reloj se difunde hacia toda la red a través de las interfaces ópticas que se asignan en los parámetros de reloj maestro (Fig. 94), la obtención de la sincronía es en un solo sentido como se indica en la figura 106.

**Figura 106. Dirección de la señal de sincronización.**



En el nodo de Sanarate se inserta el tráfico de gestión de todos los nodos dentro de la interfaz LAN, mediante un convertidor de protocolo (marcado con el número 1 en la figura 97) de serial a ethernet, ya que la interfaz de administración del nodo se comunica con el NMS mediante el protocolo RS 232 mismo el cual es recuperado en la interfaz de salida ethernet del enrutador que recibe todo el tráfico de las diferentes oficinas mediante otro convertidor (marcado con el número 2) el cual es finalmente conectado al servidor que soporta el programa de administración de los equipos

En el enrutador que recibe el tráfico proveniente de las oficinas remotas se le configuró para que realizara un proceso denominado Enrutamiento y Puenteo Integrado (IRB), antes de seguir explicando este proceso debemos explicar ciertos detalles para poder entender en que consiste este proceso.

Como explicamos anteriormente la técnica del puenteo para hacer la transferencia entre dos redes locales es partir de las direcciones de capa 2 (MAC). Un puente típico entre dos redes Ethernet se dará cuenta de cuáles de las direcciones están siendo usadas en cada una de las redes y transferirá selectivamente de una red a otra, basados en la dirección de destino de los paquetes ethernet. Los puentes utilizan su propio conjunto de protocolos para comunicarse entre sí, previniendo lo que equivaldría a los ciclos cerrados de enrutamiento y ayudándolos a aprender como manejar paquetes de clientes que no están pegados directamente a sus puertos.

El puenteo es útil para ciertas soluciones como son:

- Antes de que los enrutadores fueran un producto popular, el puenteo era una forma de extender una red más allá de los límites de un medio

físico simple. En otras palabras es una manera de conectar redes locales a una red mas grande sin la complejidad del enrutamiento.

- Muchos protocolos, tales como Netbios, no pueden ser enrutados, si se debe lidiar con protocolos que no pueden ser enrutados, se debe considera el puenteo como una manera de propagar estos protocolos a través de una red más grande. Nótese que, sin embargo, que muchos de los protocolos no enrutables pueden ser encapsulados dentro de IP, lo que efectivamente los hace enrutables, este tipo de encapsulación puede resultar una mejor opción que el puenteo.
- El puenteo es a menudo usado para conectar redes remotas a un ISP, particularmente cuando se utiliza un modem ADSL o cable modem. El ADSL o cable modem es a menudo configurado como un puente, que es mucho menos caro usando un enrutador.

Usualmente el puenteo no escala tan bien como el enrutamiento y toma mucha de la memoria del enrutador.

#### **4.5.4 Enrutamiento y Puenteo Concurrente.**

El enrutamiento y puenteo concurrente le permite al enrutador enrutar y puentear el mismo protocolo. Sin embargo, el enrutamiento y el puenteo permanecen en islas separadas en el enrutador y no se les permite interactuar entre si en otras palabras el enrutamiento puede ser habilitado en algunas interfaces , y el puenteo puede ser habilitado en otras interfaces, pero los dos grupos no pueden interactuar. Cada interfaz puede ya sea puentear o enrutar un protocolo, pero no los dos; los paquetes nunca serán transferidos de las interfaces puenteadas a las interfaces enrutadas. En los párrafos

siguientes describiremos el Enrutamiento y Punteo Integrado (IRB por sus siglas en ingles) el cual permite mayor interacción y usualmente ofrece una mejor solución.

#### **4.5.5 Enrutamiento y Punteo Integrado (IRB)**

CRB fue un gran paso en el avance hacia la implementación del Enrutamiento y Punteo Integrado, el cual permite al enrutamiento y al Punteo cooperar. IRB permite al enrutador enrutar y puentea cualquier protocolo.

En orden de alcanzar esto, necesitamos una interfaz que se conoce como BVI, lo cual significa interfaz virtual de grupo de puenteo. Nosotros creamos una BVI por cada uno de los grupos de puenteo. La BVI es enrutable y maneja todas las tareas de enrutamiento del grupo de puenteo. Nuestras interfaces de grupo de puenteo trabajan en la capa 2 mientras los BVI trabajan en la capa 3 del modelo OSI. El enrutador puede ahora con esta modalidad puentear y enrutar nuestro tráfico IP al mismo tiempo, de acuerdo con la configuración de los grupos de puenteo.

A continuación presentamos la configuración del enrutador donde están definidos los BVI para cada oficina, los cuales nos permiten enrutar el tráfico proveniente de cada una de las oficinas hacia la intranet de la empresa.



```

User Access Verification
Password:
oficinascomerciales>en
Password:
oficinascomerciales#sh conf
Using 4249 out of 29688 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname oficinascomerciales
!
enable secret 5
$1$WjuH$2MXZIWQMiWPEp6.3gk0t/
0
!
ip subnet-zero
!
isdn voice-call-failure 0
bridge irb
!
controller E1 1/0
channel-group 1 timeslots 1-4
channel-group 2 timeslots 5-8
channel-group 3 timeslots 9-12
channel-group 4 timeslots 13-16
channel-group 5 timeslots 17-20
channel-group 6 timeslots 21-24
channel-group 7 timeslots 25
description E1 Oficinas Comerciales
Oriente
!
interface Ethernet0/0
ip address 10.40.66.112
255.255.248.0
no ip directed-broadcast
!
interface Serial1/0:1
description OC-Sanarate
no ip address
no ip directed-broadcast
encapsulation frame-relay IETF
no keepalive
fair-queue 64 256 0
arp arpa
arp snap
arp timeout 0
frame-relay local-dlci 16

```

```
!  
interface Serial1/0:1.1 point-to-point  
no ip directed-broadcast  
frame-relay interface-dlci 16 protocol  
ip 10.40.87.9  
bridge-group 1  
bridge-group 1 spanning-disabled
```

```
!  
interface Serial1/0:2  
description OC-Teculután  
no ip address  
no ip directed-broadcast  
encapsulation frame-relay IETF  
no keepalive  
fair-queue 64 256 0  
arp snap  
arp timeout 0  
frame-relay local-dlci 17
```

```
!  
interface Serial1/0:2.1 point-to-point  
no ip directed-broadcast  
frame-relay interface-dlci 17 protocol  
ip 10.40.88.133  
bridge-group 2  
bridge-group 2 spanning-disabled
```

```
!  
interface Serial1/0:3  
description OC-Pasabien  
no ip address  
no ip directed-broadcast  
encapsulation frame-relay IETF  
no keepalive
```

```
fair-queue 64 256 0  
arp snap  
arp timeout 0  
frame-relay local-dlci 18
```

```
!  
interface Serial1/0:3.1 point-to-point  
no ip directed-broadcast  
frame-relay interface-dlci 18 protocol  
ip 10.40.75.9  
bridge-group 3  
bridge-group 3 spanning-disabled
```

```
!  
interface Serial1/0:4  
description OC-Morales  
no ip address  
no ip directed-broadcast  
encapsulation frame-relay IETF  
no keepalive
```

```

fair-queue 64 256 0
arp snap
arp timeout 0
frame-relay local-dlci 19
!
interface Serial1/0:4.1 point-to-point
no ip directed-broadcast
frame-relay interface-dlci 19 protocol
ip 10.40.87.133
bridge-group 4
bridge-group 4 spanning-disabled
!
interface Serial1/0:5
description OC-Chiquimula
no ip address
no ip directed-broadcast
encapsulation frame-relay IETF
no keepalive
fair-queue 64 256 0
arp snap
arp timeout 0
frame-relay local-dlci 20
!
interface Serial1/0:5.1 point-to-point
no ip directed-broadcast
frame-relay interface-dlci 20 protocol
ip 10.40.74.3
bridge-group 5
bridge-group 5 spanning-disabled
!
interface Serial1/0:6
description OC-Shoropin
no ip address
no ip directed-broadcast
encapsulation frame-relay IETF
no keepalive
fair-queue 64 256 0
arp snap
arp timeout 0
frame-relay local-dlci 21
!
interface Serial1/0:6.1 point-to-point
no ip directed-broadcast
frame-relay interface-dlci 21 protocol
ip 10.40.76.133
bridge-group 6
bridge-group 6 spanning-disabled
!
interface Serial1/0:7
no ip address

```

```
no ip directed-broadcast
encapsulation ppp
fair-queue 64 256 0
!
```

```
interface BVI1
description OC-Sanarate
ip address 10.40.87.10
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
```

```
interface BVI2
description OC-Teculután
ip address 10.40.88.130
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
```

```
interface BVI3
description OC-Pasabien
ip address 10.40.75.10
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
```

```
interface BVI4
description OC-Morales
ip address 10.40.87.135
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
```

```
interface BVI5
description OC-Chiquimula
ip address 10.40.74.10
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
```

```
interface BVI6
description OC-Shoropin
ip address 10.40.76.130
255.255.255.128
```

```
no ip directed-broadcast
arp snap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.40.66.101
ip route 10.40.78.0 255.255.255.0
10.40.66.101
```

```
no ip http server
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 protocol ieee
bridge 2 route ip
bridge 3 protocol ieee
bridge 3 route ip
bridge 4 protocol ieee
bridge 4 route ip
bridge 5 protocol ieee
bridge 5 route ip

bridge 6 protocol ieee
bridge 6 route ip
!
line con 0
transport input none
line aux 0
line vty 0 4
password ufinet
login
!
no scheduler allocate
end
```

## 4.6 Métodos de Evaluación Financiera en Evaluación de Proyectos

La evaluación de proyectos por medio de métodos matemáticos, es una herramienta de gran utilidad para la toma de decisiones por parte de los administradores financieros, ya que un análisis que prediga de alguna forma los resultados de una inversión pueden evitar posibles desviaciones y problemas a largo plazo. Las técnicas de evaluación económica son herramientas de uso general debido a que pueden ser aplicadas a las situaciones más variadas lo mismo pueden aplicarse a las inversiones hoteleras que a inversiones de informática y telecomunicaciones como es nuestro caso. El valor presente neto y la tasa interna de rendimiento se mencionan a menudo juntos debido a que en realidad son el mismo método, solo que sus resultados se expresan de manera diferente. La tasa interna de rendimiento es el interés que hace el valor presente igual a cero, lo cual confirma la aseveración anterior.

### Ecuación 3.

**Valor presente neto (VPN):**

$$VPN = -P + \sum_1^n \frac{FNE}{(1+TMAR)^n} + \frac{VS}{(1+TMAR)^n}$$

### Ecuación 4.

**Tasa interna de rendimiento (TIR):**

$$TIR = \sum_1^n \frac{FNE_n}{(1+i)^n} + \frac{VS}{(1+i)^n}$$

Donde:

- $p$  = inversión inicial.
- FNE = Flujo neto de efectivo del periodo  $n$ , o beneficio neto después de impuesto más depreciación.
- VS = Valor de salvamento al final de periodo  $n$ .
- TMAR = Tasa mínima aceptable de rendimiento o tasa de descuento que se aplica para llevar a valor presente. los FNE y el VS.  
 $i$  = Cuando se calcula la TIR, el VPN se hace cero y se desconoce la tasa de descuento que es el parámetro que se debe calcular. Por eso la TMAR ya no se utiliza en el cálculo de la TIR. Así la (1) en la segunda ecuación viene a ser la TIR.

Recuérdese que los criterios de aceptación al usar estas técnicas son:

**Tabla XII. Criterios de aceptación y rechazo de VAN y el TIR.**

| Técnica | Aceptación         | Rechazo         |
|---------|--------------------|-----------------|
| VPN     | $\geq 0$           | $< 0$           |
| TIR     | $\geq \text{TMAR}$ | $< \text{TMAR}$ |

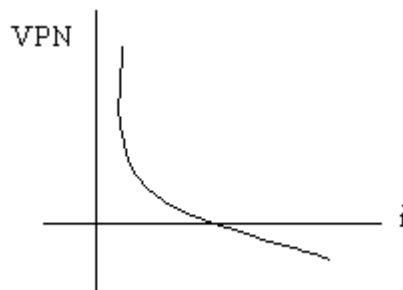
#### **4.6.1 Método del valor actual neto**

El método del valor presente es muy utilizado por dos razones la primera es porque es de muy fácil aplicación y la segunda porque todos los ingresos y egresos futuros se transforman a valores actuales y así pueden verse fácilmente, si los ingresos son mayores que los egresos o viceversa. Cuando el VPN es menor que cero implica que hay una pérdida a una cierta tasa de interés o por el contrario si el VAN es mayor que cero se presenta

una ganancia. Cuando el VPN es igual a cero se dice que el proyecto es indiferente. La condición indispensable para comparar alternativas es que siempre se tome en la comparación igual número de años, pero si el tiempo de cada uno es diferente, se debe tomar como base el mínimo común múltiplo de los años de cada alternativa.

En la aceptación o rechazo de un proyecto depende directamente de la tasa de interés que utilice, por lo general el VPN disminuye a medida que aumenta la tasa de interés, de acuerdo a la siguiente gráfica:

**Figura 107. Gráfica de comportamiento del VPN.**



En consecuencia para un mismo proyecto puede presentarse que a una cierta tasa de interés, el VPN puede variar significativamente, hasta el punto de llegar a rechazarlo o aceptarlo según sea el caso. Al evaluar proyectos mediante esta metodología se recomienda utilizar una tasa de interés superior a la Tasa de Interés de Oportunidad (TIO), con el fin de tener un margen de seguridad para cubrir ciertos riesgos, tales como liquidez, efectos inflacionarios o desviaciones que se tengan previstas.



#### **4.6.2 Método de la Tasa Interna de Retorno (TIR)**

Este método consiste en encontrar una tasa de interés en la cual se cumplen las condiciones buscadas en el momento de iniciar o aceptar un proyecto de inversión. Tiene como ventaja frente a otras metodologías como la del Valor Presente Neto (VPN) o el Valor Presente Neto Incremental (VPNI) por que en este se elimina el cálculo de la Tasa de Interés de Oportunidad (TIO), esto le da una característica favorable en su utilización por parte de los administradores financieros.

La Tasa Interna de Retorno es aquella tasa que está ganando un interés sobre el saldo no recuperado de la inversión en cualquier momento de la duración del proyecto. En la medida de las condiciones y alcance del proyecto estos deben evaluarse de acuerdo a sus características. Esta es una herramienta de gran utilidad para la toma de decisiones financiera dentro de las organizaciones

#### **4.6.3 Análisis financiero de la propuesta**

Ahora aplicaremos los métodos de análisis y los criterios mencionados anteriormente para determinar si la solución proyectada para la sustitución de los enlaces actuales resulta ser un proyecto rentable en comparación con la opción de continuar con los servicios contratados a los operadores, designaremos a la opción de continuidad de los servicios contratados como proyecto 1, y a la solución por medios propios como proyecto 2. El análisis consistirá en la comparación del costo entre ambas propuestas, proyectadas a cinco años de vida útil de los proyectos

#### 4.6.3.1 Análisis Financiero Proyecto 1

En la tabla XIII se desglosan los costos de de los enlaces actuales, de acuerdo con las capacidades de transmisión, asignadas a cada uno de los lugares interconectados por este medio actualmente. En la tabla XIV se establecen los costos de operación anual de los enlaces en cada uno de lo sitios interconectados, proyectados para cinco años.

**Tabla XIII. Desglose de gastos actuales.**

| Servicio del operador            | Costo      |
|----------------------------------|------------|
| Costo mensual de enlace 128 kbps | \$770.28   |
| Costo mensual de enlace 256 kbps | \$1,052.52 |

**Tabla XIV. Flujo de caja proyecto 1.**

| Lugar        | Año 1              | Año 2              | Año 3              | Año 4              | Año 5              |
|--------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| Sanarate     | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         |
| Pasabién     | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         |
| Teculután    | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         |
| Chiquimula   | \$12,630.24        | \$12,630.24        | \$12,630.24        | \$12,630.24        | \$12,630.24        |
| Choropín     | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         |
| Morales      | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         | \$9,243.36         |
| <b>TOTAL</b> | <b>\$58,847.04</b> | <b>\$58,847.04</b> | <b>\$58,847.04</b> | <b>\$58,847.04</b> | <b>\$58,847.04</b> |

Con esta información aplicamos la ecuación para el cálculo del VAN con una tasa de interés del 12 % para obtener el valor presente del proyecto 1.

|            |                     |
|------------|---------------------|
| <b>VAN</b> | <b>\$237,586.06</b> |
|------------|---------------------|

#### 4.6.3.2 Análisis económico del proyecto 2

Para el análisis del proyecto 2, debemos analizar la inversión inicial en la tabla XV se hace la separación en dos rubros, el primero hace referencia al costo total de las derivaciones desde el tendido principal de la fibra hasta los lugares que se pretenden interconectar, el segundo es el valor de los equipos activos que se instalarán en cada uno de los sitios a interconectar.

**Tabla XV. Costos iniciales del proyecto.**

| Desglose del proyecto     | Costos      |
|---------------------------|-------------|
| Costo de proyecto en F.O. | \$64,100.07 |
| Costos de equipos activos | \$49,022.21 |

Además para calcular el valor en el tiempo del proyecto también debemos tener los valores de depreciación anual que tienen los diferentes elementos para poderlos descontar del valor actual neto de la solución.

**Tabla XVI Cálculo de depreciaciones.**

| Concepto  | Año 1             | Año 2             | Año 3             | Año 4             | Año 5             |
|---|-------------------|-------------------|-------------------|-------------------|-------------------|
| Gasto de depreciación de F.O.                       | \$6,410.01        | \$6,410.01        | \$6,410.01        | \$6,410.01        | \$6,410.01        |
| Gasto de depreciación de equipos activos            | \$16,340.74       | \$16,340.74       | \$16,340.74       |                   |                   |
| <b>Escudos fiscales aplicables por depreciación</b> | <b>\$7,052.73</b> | <b>\$7,052.73</b> | <b>\$7,052.73</b> | <b>\$1,987.10</b> | <b>\$1,987.10</b> |

**Tabla XVII. Flujo de caja proyecto 2.**

| Lugar                                     | Año 1               | Año 2              | Año 3              | Año 4              | Año 5              |
|---|---------------------|--------------------|--------------------|--------------------|--------------------|
| Sanarate                                  | \$18,000.00         | \$18,000.00        | \$18,000.00        | \$18,000.00        | \$18,000.00        |
| Parabién                                  | \$0.00              | \$0.00             | \$0.00             | \$0.00             | \$0.00             |
| Teculután                                 | \$0.00              | \$0.00             | \$0.00             | \$0.00             | \$0.00             |
| Chiquimula                                | \$0.00              | \$0.00             | \$0.00             | \$0.00             | \$0.00             |
| Choropín                                  | \$0.00              | \$0.00             | \$0.00             | \$0.00             | \$0.00             |
| Morales                                   | \$0.00              | \$0.00             | \$0.00             | \$0.00             | \$0.00             |
| Costo anual mtto F.O.                     | \$5,400.00          | \$5,400.00         | \$5,400.00         | \$5,400.00         | \$5,400.00         |
| Escudos fiscales generados                | (\$7,052.73)        | (\$7,052.73)       | (\$7,052.73)       | (\$1,987.10)       | (\$1,987.10)       |
| Inversión inicial (chiquimula)            | \$6,510.69          |                    |                    |                    |                    |
| Inversión inicial (no incluye chiquimula) | \$106,611.59        |                    |                    |                    |                    |
| <b>TOTAL</b>                              | <b>\$129,469.55</b> | <b>\$16,347.27</b> | <b>\$16,347.27</b> | <b>\$21,412.90</b> | <b>\$21,412.90</b> |

Con esta información aplicamos la ecuación para el cálculo del VAN con una tasa de interés del 12 % para obtener el valor presente del proyecto 2.

|            |                     |
|------------|---------------------|
| <b>VAN</b> | <b>\$185,946.83</b> |
|------------|---------------------|

#### 4.6.3.3 Comparación de los dos proyectos.

Después de realizar el estudio económico de ambas propuestas, se puede tomar una decisión a cerca de la continuidad del primero y lo la implementación del segundo.

Como punto de referencia utilizaremos los VAN de ambos proyectos, en le caso del proyecto número 1 el VAN calculado para una vida útil de 5 años nos da como resultado **\$237,586.06**, por otro lado tenemos el valor actual neto del proyecto numero 2 que nos da un valor actual neto de **\$185,946.83**, esto nos indica que para un tiempo de vida similar el proyecto número uno tiene proyectados gastos que lo hacen mucho más oneroso

que el proyecto número dos. Si restamos los dos valores obtendremos el valor del ahorro que tendríamos en un periodo de 5 años si decidiéramos implementar el proyecto número dos, dicho valor es expuesto en la tabla de resumen.

**Tabla XVIII. Tabla resumen comparativo de ambos proyectos.**

| <b>CUADRO COMPARATIVO DE PROYECTOS</b> |                   |                   |
|--|-------------------|-------------------|
| <b>Concepto</b>                        | <b>Proyecto 1</b> | <b>proyecto 2</b> |
| <b>VAN</b>                             | \$237,586.06      | \$185,946.83      |
| <b>Ahorro en 5 años \$</b>             | 0                 | \$50,848.28       |
| <b>Ahorro en 5 años %</b>              | 0                 | 21.40%            |

En conclusión, basándome en los obtenidos al realizar la comparación de el estudio económico realizado a ambos proyectos que: la implementación de un sistema de comunicación basado parcialmente en medios propios es conveniente, dado los recursos de infraestructura que se poseen actualmente. Además de la ventaja de tener un valor económico menor, posee otras ventajas por ejemplo, el hecho de contar con infraestructura de fibra óptica hasta los puntos terminales, por la naturaleza del medio, permite la migración a equipo de transmisión con más capacidad de transporte de datos, esto hace posible en la expansión de negocios a tales como la venta de servicios de transporte a través del tendido principal de la empresa teniendo como punto de inserción cada uno de los puntos existentes actualmente, además por la topología en bus de la solución pueden ser agregados más puntos intermedios aumentando la cobertura de la solución, la cual puede ser útil a la empresa en otro ramo de negocio interno como lo es el telecontrol de las subestaciones eléctricas y su integración al sistema SCADA ya que en el paso del anillo principal de fibra se encuentran varias de estas.



## CONCLUSIONES

1. Las comunicaciones son parte esencial en las diversas actividades productivas del ser humano.
2. El proceso de diseño de una red debe un proceso sistemático y ordenado, que debe tomar en cuenta las capacidades y restricciones de los recursos que se poseen.
3. Un buen diseño de una red debe tomar en cuenta los siguientes aspectos: Funcionalidad, Escalabilidad, adaptabilidad y facilidad de administración.
4. El diseño de una aplicación es dictada por los requerimientos de la empresa. Las reglas de la empresa, los flujos de los procesos, los requerimientos de seguridad y los resultados esperados, todos estos factores afectan directamente el diseño de red.
5. Al diseñar una red se deben tener lo criterios suficientes para proponer una solución que se adapte tanto a las necesidades técnicas como a los recursos económicos que han sido asignados para la tarea.





## RECOMENDACIONES

1. Incentivar la creación dentro de la escuela de mecánica eléctrica una maestría, o en el mejor de los casos una ingeniería electrónica, con orientación en telecomunicaciones.
2. Actualizar el contenido de los cursos de telecomunicaciones incluidos dentro del pensum de estudio de la carrera de ingeniera electrónica.
3. Crear dentro laboratorios dedicados a al implementación de diferentes tecnologías de las redes LAN y WAN.
4. Actualización del pensum de ingeniería electrónica, que incluyan un área gerencial que permita la investigación, desarrollo y evaluación de proyectos.



## BIBLIOGRAFIA

### Libros

- 1 Martin Murhammer, Kok Keong Lee, Payam Motallebi, Paolo Borghi, Karl Wosaba IP NETWORK DESIGN GUIDE Segunda edición 1999. Editorial: IBM Redbooks
- 2 Freeman, Robert L. PRACTICAL DATA COMMUNICATION Segunda edición 2001 Editorial: John Wiley & Sons, Inc.
- 3 Freeman, Robert L. FUNDAMENTALS OF TELECOMUNICATIONS Primera edición 1999. Editorial: John Wiley & Sons, Inc.
- 4 Newall, Christopher SISTEMAS DE TRANSMISION SINCRÓNICA Edcion 3.1 Editorial: Northern Telecom (CALA) Corporation
- 5 Guichard, Jim Le Faucheur, François Vasseur, Jean-Philippe Definitive MPLS Network Designs, Cisco Press

### Referencia electrónica

- 7 <http://www.netcraftsmen.net/welcher/papers/mpsintro.html> 11/2/2006
- 8 [http://www.telecomm.net.mx/webmaster74/tutores/cap\\_01.html](http://www.telecomm.net.mx/webmaster74/tutores/cap_01.html) 20/3/2005
- 9 [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch\\_c/xcprt4/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch_c/xcprt4/index.htm) 30/3/2006
- 10 [http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/wa5/12\\_0/3a\\_11/config/tag.htm](http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/wa5/12_0/3a_11/config/tag.htm) 30/3/2006

- 11 [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch\\_c/xcp4r4/xcdtagc.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch_c/xcp4r4/xcdtagc.htm) 30/3/2006
- 12 [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/s witch_r/index.htm) 30/3/2006
- 13 <http://www.rediris.es/rediris/boletin/53/enfoque1.html> 5/4/2006
- 14 <http://www.convergedigest.com/tutorials/mps2/page1.htm> 5/4/2006
- 15 <http://www.eie.fceia.unr.edu.ar/~comunica/TBAApub/atmApunte.pdf> 4/4/2006
- 16 [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm) 10/8/2005
- 17 [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/routing.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm) 5/4/2005
- 18 [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm) 15/6/2006
- 19 [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/mps\\_tsw.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/mps_tsw.htm) 5/6/2006
- 20 <http://www.syrus.ru/files/doc> 5/4/2006
- 21 [http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm\\_ovr.pdf](http://www.cisco.com/univercd/cc/td/doc/product/mels/cm1500/dwdm/dwdm_ovr.pdf) 15/3/2006

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.