CONMUTACIÓN

Apuntes de la asignatura 2011-2012
Versión 1.0

Daniel Pérez Rodríguez

Noviembre, 2012

Este documento ha sido generado con LaTeX.

Para cualquier consulta, errata o sugerencia, por favor no dude en contactar con el autor en:

manuscrito.conmutacion@gmail.com

El autor quisiera recalcar que este documento se ha realizado con fines meramente didácticos y sin ánimo de lucro y por lo tanto declina cualquier responsabilidad sobre sus (más que) posibles fallos de contenido.

!DEDICADO

A mis padres, por ser responsables de ser como soy ...

... por eso nunca os dedicaría un libro como éste.

PRÓLOGO

Existen ciertos momentos en la vida, en los que los caminos se vuelven tenebrosos. Tal vez dentro de unos años cuando eche la vista atrás, éste no parecerá haber sido uno de esos momentos, pero a estas alturas de la película, lo parece, vaya que si lo parece.

Esta pequeña aventura personal no pretende ser sino una pequeña luz, para alumbrar este oscuro camino, en el que para algún que otro alumno desorientado (como un servidor en más de un momento) se ha convertido *CONMUTACIÓN*, la asignatura troncal de 6 créditos de quinto curso de la titulación de *Ingeniero de Telecomunicación*, plan de estudios de 1998, de la Escuela Superior de Ingenieros de la Universidad de Sevilla.

Este manuscrito se basa completamente en el trabajo realizado por los profesores de la asignatura, publicado en forma de transparencias de clase [16], que sin duda han conformado algo más que el esqueleto del mismo.

Se sigue la estructura ya planteada en dichos materiales, pero ampliando en conceptos y ejemplos, tratando de extraer todo el conocimiento posible de la bibliografía recomendada de cada tema, indicada en cada capítulo, e intentando siempre dar una coherencia narrativa y un cierto sentido docente al texto ...

Creo que nunca seré consciente de lo lejos que quedé de lograr este objetivo.

Por tanto, este texto no es sino un mero resumen, recopilación de un conjunto de textos, referencias reconocidas y utilizadas a nivel mundial, sobre cuyos respectivos autores debe recaer todo el mérito docente, superficialmente aquí plasmado.

Quisiera agradecer también a título personal al Dr. D. Juan Manuel Vozmediano Torres, su consentimiento para la utilización expresa del material creado por él para las transparencias de la asignatura [16].

AVISO PARA NAVEGANTES

A pesar de que espero haber plasmado en el prólogo anterior el alcance o utilidad de estos apuntes, prefiero no obstante destacar una serie de ideas antes de continuar, para evitar ... posibles malentendidos.

- *¿Este texto son unos apuntes oficiales de la asignatura?*

  NO.

- *¿Recogen todo el contenido necesario para aprobar la asignatura?* Difícil responder. La intención al realizar estos apuntes era sin duda aprobar la asignatura y por tanto deberían hacerlo. Repito, deberían. Sí puedo decir que el texto y el desarrollo se ajusta al contenido de la asignatura; ahora bien, recogerlo todo, todo ...

- *¿Tienen errores los apuntes?*

  SÍ.

  Por eso es importante, estudiar y leer con atención y capacidad crítica. Si encuentras algún error, por favor contacta conmigo para intentar solucionarlos.

- *¿Estudiando estos apuntes aprobaré la asignatura?* A pesar de no tener poderes adivinatorios (... de momento ...), me atrevería a decir que **NO**. Para aprobar la asignatura es necesario seguir las pautas que recomiendan los responsables de la misma, que como bien sabe, querido lector, las encontrará en `http://trajano.us.es/docencia/Conmutacion`.

Recalcar pues, que estos apuntes pueden ser una ayuda o referencia más a la hora de afrontar el contenido de la asignatura y que tal vez puedan resultar útiles a tal fin, al menos, ese ha sido el espíritu con el que se han redactado.

Por si aún no estuviera suficientemente claro, solo me resta citar a quién tú sabes diciendo:

*Si el alumno pretende utilizar este material como único apoyo para superar la asignatura, entonces «**caveat emptor**».*

ESTADO DE LOS APUNTES

Antes de comenzar con el contenido de los apuntes quisiera hacer una pequeña valoración personal del estado de los mismos.

Los capítulos correspondientes a los tres primeros temas de la asignatura, es decir RTC, RDSI y SS7 se encuentran en un estado que podríamos considerar como *RELEASE CANDIDATE*. Bastante trabajados y ordenados, aunque seguramente hayas cosas que se puedan mejorar y cualquier sugerencia será bien recibida.

El resto de temas de la asignatura, no están aún lo suficientemente depurados que yo quisiera, con lo que los considero que se encuentran en un estado *BETA*. Se ajustan al contenido de la asignatura, pero tienen un gran margen de mejora.

Respecto a los anexos, he incluido una serie de temas que considero resultan de interés repasar para el estudio de ciertas partes de la asignatura. Creo que también ayudan a clarificar el contexto en el que se mueve la asignatura y a dar una mejor visión de conjunto de los contenidos de la misma.

Por desgracia el tiempo es un bien valioso y no he podido dedicarles el trabajo necesario por lo que algunos de ellos se encuentran aún en estado *ALPHA* y he preferido directamente no incluirlos de momento y dejarlos para la siguiente revisión del manual.

Sí he incluido, a cambio, algunas referencias a dichos contenidos para poder repasar dichos conceptos.

Índice general

1. Introducción a la Red Telefónica Conmutada **33**
1.1. Introducción 33
1.2. La red telefónica conmutada 39
1.2.1. Red de Acceso 39
1.2.2. Red de Conmutación 46
1.2.3. Red de Transmisión 50
1.2.4. Red de Sincronización 55
1.2.5. Red de Señalización 59
1.2.6. Red de Gestión 62
1.2.7. Red Inteligente 63
1.3. Evolución 65

2. Introducción a RDSI y Q.931 **67**
2.1. Introducción 67
2.2. Términos y Definiciones 70
2.2.1. Canales de Acceso 70
2.2.2. Interfaces de Acceso 71
2.2.3. Grupos Funcionales y Puntos de Referencia 72
2.2.4. Arquitectura de Protocolos 75
2.3. Servicios en RDSI 77
2.3.1. Numeración y Direccionamiento 80
2.4. Nivel Físico 82
2.4.1. Conectores y Señales 83
2.4.2. Configuraciones de Cableado 85
2.4.3. Codificación y Entramado 86
2.4.4. Resolución de Contienda para configuraciones en Multidrop 89
2.4.5. Interfaz U 91
2.4.6. Acceso Primario 92
2.5. Nivel de Enlace 94
2.5.1. LAPD 94
2.6. Nivel de Red 99
2.6.1. Control Básico de Llamada 101

2.7. Control de Conexión en Modo Circuito 112
2.7.1. Conexión en Modo Circuito en Bloque 115
2.7.2. Conexión en Modo Circuito Solapada 117
2.7.3. Desconexión en Modo Circuito 118

3. Sistema de Señalización por Canal Común n^{o}7 121
3.1. Introducción 121
3.2. Sistema de Señalización N^{o}7 (CSS7 o SS7) 125
3.2.1. Generalidades 125
3.2.2. Arquitectura de SS7 129
3.3. MTP 132
3.3.1. MTP1 132
3.3.2. MTP2 133
3.3.3. MTP 3 147
3.4. SCCP 161
3.4.1. Direccionamiento 162
3.4.2. Arquitectura de SCCP 162
3.4.3. Clases de Servicios SCCP 164
3.4.4. Protocolos SCCP 168
3.4.5. Mensajes y Parámetros SCCP 169
3.5. ISUP 174
3.5.1. Mensajes ISUP 176
3.5.2. Ejemplos control de llamadas 181
3.5.3. Señalización Extremo a Extremo 184
3.5.4. Servicios ISUP 185
3.5.5. Portabilidad 185
3.6. TCAP 189
3.6.1. Estructura TCAP 190
3.6.2. Mensajes TCAP 194
3.6.3. Ejemplo de uso de TCAP 194
3.7. MAP 197
3.7.1. GSM: Global System for Mobile Communications . . . 197
3.7.2. MAP: Mobile Application Part 205

4. ATM y MPLS 209
4.1. Introducción 209
4.2. Principios generales de las redes ATM 210
4.3. Arquitectura de Protocolos ATM 213
4.4. Capa Física 214
4.4.1. Subcapa dependiente del medio físico (PMD) 215
4.4.2. Subcapa de convergencia de trasmisión (TC) 218
4.5. Capa ATM 221
4.5.1. Caminos y canales virtuales 222
4.5.2. Formato de Célula 226

4.6. Capa de Adaptación 229
4.6.1. AAL2 231
4.6.2. AAL5 237
4.7. Señalización en ATM 238
4.8. Datos sobre ATM 241
4.8.1. Encapsulado Multiprotocolo sobre AAL5 242
4.8.2. Resolución de direcciones 243
4.9. Fundamentos de control de tráfico 248
4.9.1. Parámetros de tráfico 249
4.9.2. Parámetros de Calidad de Servicio (QoS) 250
4.9.3. Tipos de conexiones ATM 251
4.10. MPLS. Conmutación de etiquetas multiprotocolo 252
4.10.1. Funcionamiento Básico de MPLS 258
4.10.2. Tratamiento de Etiquetas 261
4.10.3. Aspectos avanzados MPLS 270

5. Redes de Nueva Generación **277**
5.1. Introducción 277
5.2. Fundamentos de Transmisión de Voz en Redes de Paquetes . 280
5.2.1. RTP: Real-Time Transport Protocol 284
5.2.2. RTCP: Real-Time Transport Control Protocol 288
5.2.3. Aspectos de Calidad en el Servicio Telefónico 289
5.3. Transmisión de Señalización de Circuitos en Redes de Paquetes 300
5.3.1. SIGTRAN: Interfuncionamiento con Q.931/CSS7 . . . 300
5.3.2. Arquitectura SIGTRAN 300
5.3.3. El protocolo SCTP 305
5.3.4. Los agentes de usuario: IUA, M2UA, M3UA, SUA, V5UA 312
5.4. Arquitecturas Normalizadas: SIP, MEGACO 322
5.4.1. SIP: Session Initiation Protocol 322
5.4.2. MEGACO/H.248 334

6. Redes de Acceso **343**
6.1. Bucle Digital de Abonado 343
6.1.1. Antecedentes 344
6.1.2. G.991 - Transceptores de línea digital de abonado de alta velocidad binaria 346
6.1.3. G.992 - Transceptores de línea de abonado digital asimétrica, con y sin divisores 348
6.1.4. G.993.1 - Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria (VDSL) . . . 354
6.1.5. G.993.2 - Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria 2 (VDSL2) . 355
6.1.6. Comparativa tecnologías xDSL 359

6.1.7. Regulación y mercado 360
6.2. Redes de Telecomunicación por cable 370
6.2.1. Introducción 370
6.2.2. Aspectos de Mercado 370
6.2.3. Arquitectura de Red 374
6.2.4. El servicio de televisión digital 380
6.2.5. El servicio de telefonía 383
6.2.6. El servicio de datos. DOCSIS. 385
6.3. El acceso Ethernet (EFM) 389
6.3.1. IEEE: Ethernet para Operador (Carrier Ethernet) (I) 389
6.3.2. IETF: Marco Conceptual para Servicios Corporativos de Red Privada Virtual VPN 391
6.3.3. IEEE: Ethernet para Operador (Carrier Ethernet) (II) 404
6.3.4. Servicios de triple oferta y Acceso residencial basado en Ethernet 406

A. Normalización **419**

B. Recomendación I.120 (03/93) **421**
B.1. Principios de la RDSI 421
B.2. Evolución de las redes hacia la RDSI 422

C. El Modelo OSI **425**
C.1. Motivación 425
C.2. Conceptos 426
C.3. Capas 429
C.3.1. Capa Física 429
C.3.2. Capa de Enlace de Datos 431
C.3.3. Capa de Red 431
C.3.4. Capa de Transporte 432
C.3.5. Capa de Sesión 432
C.3.6. Capa de Presentación 432
C.3.7. Capa de Aplicación 433
C.4. Perspectivas en el modelo OSI 433

D. Repaso Conceptos Básicos en Telecomunicaciones **435**

E. Protocolos TCP/IP **437**
E.1. Introducción 437
E.2. Protocolo IP: Internet Protocol 438
E.3. Protocolo UDP: User Datagram Protocol 440
E.4. Protocolo TCP: Transmission Control Protocol 443
E.4.1. Desarrollo de TCP 448
E.5. Comparativa UDP - TCP 448

F. Ethernet y VLAN 802.1q **451**
F.1. Ethernet 451
F.2. VLAN 802.1q 453

G. IP Multicast **459**
G.1. Direcciones IP Multicast 459

Índice de figuras

1. Nomenclatura básica 29

1.1. Evolución RTC 34
1.2. Necesidad de Red (0) 35
1.3. Necesidad de Red (I) 36
1.4. Necesidad de Red (II) 36
1.5. Necesidad de Red (III) 37
1.6. Jerarquía Tradicional 38
1.7. Jerarquía Digital 38
1.8. Red de Acceso. Visión general 39
1.9. Uso de la Red de Acceso para otros servicios 41
1.10. Diafonía 42
1.11. Bucle de Abonado Analógico 43
1.12. SLTU 43
1.13. Codificación MIC (PCM) 44
1.14. Bucle de Abonado Digital 45
1.15. Formato de trama PCM (E1) 46
1.16. Strowger Switch 48
1.17. Conmutación Digital 50
1.18. Redundancia Red de Conmutación 50
1.19. Red de Transmisión: Estándar PDH Europeo 52
1.20. Red de Transmisión: Jerarquía Digital Síncrona (SDH) 54
1.21. Red de Transmisión: Formato Trama SDH 54
1.22. Red de Transmisión: Fluctuación de relojes 55
1.23. Red de Sincronización: Deslizamiento de Trama (slip) 56
1.24. Red de Sincronización: Funcionamiento Plesiócrono 57
1.25. Red de Sincronización: Funcionamiento Síncrono 58
1.26. Red de Señalización: Señalización por Canal Común (CCS) . 60
1.27. Red de Señalización: CCS en la Red 61
1.28. Red de Señalización: Ejemplo de Funcionamiento 62
1.29. Red de Inteligente 64
1.30. Evolución 65

2.1. Acceso a RTC mediante RDSI 67

2.2. Recomendaciones Serie I de la UIT-T 68
2.3. Grupos Funcionales y Puntos de Referencia 72
2.4. Grupos Funcionales: TE2 y TA 74
2.5. TE1s en Multidrop a NT1 75
2.6. Conexiones Múltiples entre TE1s y NT2 75
2.7. Arquitectura de Protocolos RDSI 76
2.8. Protocolos RDSI interfaz usuario-Red 77
2.9. RDSI: Tipos de Servicios 79
2.10. RDSI: Conmutación de Circuitos sobre Canal B 81
2.11. Dirección RDSI 81
2.12. Configuración de Referencia para Transmisión de Señal y Alimentación en Operación Normal 83
2.13. Acceso Básico: Conector y Medio Físico 84
2.14. Acceso Primario: Conector y Medio Físico 85
2.15. Configuración Punto a Punto 86
2.16. Configuración Bus Pasivo Corto 86
2.17. Configuración Bus Pasivo Largo 86
2.18. Código Pseudoternario 87
2.19. Estructura de Trama Acceso Básico RDSI 87
2.20. Resolución de contienda: Bit de Eco 90
2.21. Trama Interfaz U 92
2.22. Acceso Primario 2.048 Mbps 93
2.23. Estructura Trama LAPD 96
2.24. Modelado de Servicios Básicos y Suplementarios 100
2.25. Empaquetado de Mensaje Q.931 101
2.26. Formato mensaje Q.931 103
2.27. Referencia de Llamada 105
2.28. Significación mensajes Q.931 108
2.29. Capacidad del Servicio Portador 111
2.30. Conexión en Modo Circuito en Bloque 116
2.31. Conexión en Modo Circuito Solapada 118
2.32. Desconexión en Modo Circuito 119

3.1. Señalización Asociada al Canal 122
3.2. Señalización por Canal Común 123
3.3. CCS Modo Asociado 123
3.4. CCS Modo No Asociado 124
3.5. Señalización de Red y de Usuario 124
3.6. Tipos de nodos SS7 127
3.7. Ejemplo modos de señalización 129
3.8. Arquitectura de SS7 130
3.9. Formato Unidad de Señalización MTP2 134
3.10. Formato Unidad de Señalización LSSU MTP2 136
3.11. Alineamiento MTP2 141

3.12. Ejemplo de Control de Errores MTP2 145
3.13. Funciones red de señalización MTP3 148
3.14. Formato Unidad de señalización MSU 150
3.15. Paso a enlace de reserva 157
3.16. Paso a enlace de reserva: Ejemplos 157
3.17. Ejemplo control de congestión de rutas 159
3.18. Ejemplo control de congestión de rutas: temporizadores . . . 159
3.19. Ejemplo control de disponibilidad de rutas 160
3.20. Arquitectura SCCP 163
3.21. Secuencia de Primitivas Servicios Orientados a Conexión . . . 167
3.22. Formato mensaje SCCP 171
3.23. SCCP: Transferencia Clase 1 172
3.24. SCCP Primitivas establecimiento conexión 172
3.25. SCCP: Transferencia Clase 2 173
3.26. SCCP: Mecanismo Asignación de Crédito Transferencia Clase 3174
3.27. Idea básica ISUP 176
3.28. Encapsulado mensaje ISUP 177
3.29. Formato mensaje ISUP 179
3.30. Llamada por Conmutación de Circuitos 181
3.31. ISUP: Llamada ordinaria completa, en bloque 182
3.32. ISUP: Llamada ordinaria completa, solapado 183
3.33. ISUP: Liberación de llamada normal 183
3.34. Portabilidad: Encaminamiento hacia adelante (OR) 186
3.35. Portabilidad: Encaminamiento con retroceso (RTP) 187
3.36. Portabilidad: Consulta tras las liberación (QoR) 188
3.37. Portabilidad: Consulta de toda la llamada (ACQ) 188
3.38. Estructura TCAP 191
3.39. Mensajes subcapa TCAP 194
3.40. Estructura mensajes TCAP 195
3.41. Escenario ejemplo uso TCAP (I) 196
3.42. Escenario ejemplo uso TCAP (II) 196
3.43. Arquitectura Sistema GSM 198
3.44. Arquitectura UMTS R99 205
3.45. Protocolos MAP-X 206
3.46. MAP: Ejemplo actualización localización 207

4.1. Evolución de equipos y servicios ATM 210
4.2. Célula ATM 211
4.3. Arquitectura de protocolos ATM 213
4.4. Tipos de células ATM 216
4.5. Estructura de trama de STM-1 217
4.6. Multiplexado inverso de ATM (IMA) 218
4.7. Célula ATM: Header Error Control 219
4.8. HEC: Protección contra errores y ráfagas 220

4.9. Delimitación de célula 221
4.10. Conmutador ATM 222
4.11. ATM: Caminos y Canales Virtuales 223
4.12. ATM: Conmutación de VPs (Repartidor digital) 224
4.13. ATM: Conmutación de VCs (Conmutador) 224
4.14. ATM: Ejemplo Conmutación de VCs y VPs 225
4.15. ATM: Ejemplo VC distinto para cada nodo B frente a VP compartido) 226
4.16. Formato de célula ATM 227
4.17. Estructura Genérica AAL 230
4.18. Arquitectura de Protocolos AAL2 232
4.19. Multiplexión AAL2 (I) 233
4.20. Multiplexión AAL2 (II) 234
4.21. Señalización Q.2630.1 para canales AAL2 236
4.22. Formato AAL5 CPCS-PDU 237
4.23. Torre de Protocolos Señalización ATM 239
4.24. Arquitectura SAAL 240
4.25. IP cásico sobre ATM 241
4.26. IPoATM: Encapsulado en LLC/SNAP 243
4.27. IPoATM: Formato cabeceras LLC/SNAP 244
4.28. IPoATM: Encapsulado sobre Canal Virtual 244
4.29. IPoATM: Resolución de direcciones 246
4.30. IPoATM: Ejemplo de encaminamiento con varias LIS 247
4.31. Flujo de Células ATM 249
4.32. Parámetros de Tráfico 250
4.33. Parámetros de QoS 251
4.34. Funcionamiento de un encaminador 256
4.35. Red MPLS 257
4.36. Funcionamiento de un LSR 258
4.37. Ejemplo funcionamiento básico MPLS 259
4.38. Etiqueta MPLS 260
4.39. Ubicación etiqueta MPLS 260
4.40. Establecimiento de vecindades en MPLS 264
4.41. Ejemplo distribución etiquetas MPLS 266
4.42. Jerarquías MPLS 267
4.43. Uso de Implicit Null Label 269
4.44. Ejemplo de conservación de etiquetas MPLS (I) 271
4.45. Ejemplo de conservación de etiquetas MPLS (II) 272
4.46. Soporte Multicast en MPLS 274
4.47. Ejemplo Fast Reroute MPLS 275
4.48. Ejemplo de protección local y restauración MPLS 276

5.1. Muestra vocal y espectro de frecuencia 281
5.2. Transmisor típico VOIP 281

5.3. Detección de Actividad Vocal 282
5.4. Receptor Típico VOIP 283
5.5. Torre de Protocolos Básica VOIP 284
5.6. Formato Cabecera RTP 285
5.7. Perfiles Pay Load Type RTP para Audio 287
5.8. Formato Cabecera RTP/UDP/IP 288
5.9. Skype Quality Feedback 289
5.10. Contribuciones al Retardo 291
5.11. Comparativa Mean Opinion Square (MOS) en diferentes Codecs 293
5.12. MOS en función del factor de determinación de índices R . . 295
5.13. Modelo E: uso pasivo 296
5.14. MOS en función del factor de determinación de índices R . . 297
5.15. Esquema Funcionamiento Modelo P.862 298
5.16. Esquema Funcionamiento Modelo P.563 299
5.17. SIGTRAN: Arquitectura de Red Integrada (Acceso por MG y SG) 302
5.18. SIGTRAN: Arquitectura de Red Integrada (Acceso por AG) . 302
5.19. Torre de Protocolos Conceptual SIGTRAN 304
5.20. Ejemplo de escenario SCTP con 2 direcciones IP y 3 flujos . . 307
5.21. Separación de flujos en SCTP 307
5.22. Formato de mensaje SCTP 308
5.23. Establecimiento asociación SCTP 312
5.24. Liberación asociación SCTP 312
5.25. Arquitectura Comparada (I): Plano de Control 313
5.26. Arquitectura Comparada (II): Plano de Control de Dispositivo 314
5.27. Ejemplo terminología UA 315
5.28. Arquitectura M2UA 316
5.29. Arquitectura M2PA 317
5.30. Arquitectura M3UA 318
5.31. Arquitectura SUA 319
5.32. Ejemplo IUA 320
5.33. ASPs Dominantes o Balanceados 321
5.34. Estados AS/ASP 321
5.35. Arquitectura de Protocolos SIP 325
5.36. Arquitectura de Sistema SIP 326
5.37. Establecimiento de llamada SIP 328
5.38. Llamada cancelada SIP 329
5.39. Llamada rechazada SIP 329
5.40. Suscripción SIP 331
5.41. Referencia SIP 331
5.42. Establecimiento de llamada con redirección SIP 332
5.43. Ejemplo SDP 334
5.44. Motivación MeGaCo: Pasarela Descompuesta 335
5.45. Arquitectura Sistema MeGaCo 335

5.46. MeGaCo: Asociación de terminaciones 337
5.47. MeGaCo: ADD 339
5.48. MeGaCo: MODIFY 340
5.49. Torre de protocolos MeGaCo 341
5.50. Ejemplo establecimiento de llamada MeGaCo 341

6.1. Pares HDSL 346
6.2. Red de Acceso SHDSL 348
6.3. G.992.1: Modelo de referencia ADSL con splitters 350
6.4. G.992.2: Modelo de referencia ADSL sin splitters 351
6.5. módem ADSL - DSLAM 352
6.6. Alcance VDSL 355
6.7. Comparativa VDSL2/VDSL/ADSL2+ 356
6.8. Plan de frecuencias VDSL2 comparado 356
6.9. Armonización Plan de frecuencias VDSL2 357
6.10. Perfiles VDSL2 357
6.11. Arquitectura de Referencia VDSL2 358
6.12. Instalación VDSL2 358
6.13. Espectros Comparados Tecnologías xDSL 360
6.14. Evolución en la red 361
6.15. Modos desagregación bucle de abonado 363
6.16. Acceso a Internet por ADSL 365
6.17. Acceso a Internet por ADSL 366
6.18. Modem de abonado USB 366
6.19. Router de abonado 367
6.20. Arquitectura de Protocolos Acceso Internet ADSL 367
6.21. Encapsulados Acceso Internet ADSL 368
6.22. Red de Agregación ATM (I) 368
6.23. Red de Agregación ATM (II): Alternativas 369
6.24. Ejemplo Acceso HTTP 369
6.25. Ejemplo PPPoE: Establecimiento de Sesión (I) 370
6.26. Ejemplo PPPoE: Establecimiento de Sesión (II) 371
6.27. Ejemplo IPoE: DHCP 371
6.28. Operadores de Cable en España 372
6.29. Situación Actual Cable frente a xDSL 372
6.30. Arquitectura Sistemas CATV 374
6.31. Arquitectura de Red HFC 375
6.32. Funciones Cabecera de Red HFC 376
6.33. Espectro en Red Troncal 376
6.34. Equipamiento Nodo Primario 377
6.35. Equipamiento Nodo Secundario 377
6.36. Red de distribución: Segmento Coaxial 378
6.37. Acometida 379
6.38. Cabecera TV Digital 381

6.39. Equipamiento de Cabecera 382
6.40. Arquitectura de Protocolos MPEG2 383
6.41. Servicio de Telefonía en redes HFC 384
6.42. Servicio IP sobre redes HFC 385
6.43. Servicio IP sobre redes HFC: Arquitectura Lógica 386
6.44. Arquitectura de Protocolos DOCSIS 387
6.45. Trama Capa de Enlace DOCSIS 388
6.46. 802.1ad Apilado VLAN - QinQ 390
6.47. Ejemplo 802.1ad Apilado VLAN - QinQ 391
6.48. Clasificación Servicios VPN 392
6.49. Arquitectura RFC 4664 394
6.50. Pseudocable Ethernet para MPLS 396
6.51. L2VPN VPLS 397
6.52. L2VPN VPWS 398
6.53. L2VPN Visión global con un sólo abonado 398
6.54. L2VPN Hierarchical VPLS 399
6.55. Aspectos Comunes VPN 400
6.56. L3VPN PE Based y CE Based 400
6.57. L3VPN basadas en PEs/MPLS 402
6.58. L3VPN Visión con un sólo abonado 403
6.59. Escenario Mixto L2VPN/L3VPN 403
6.60. Etiquetas 802.1ah PBB Provider Backbone Bridge (Mac-in-Mac) 404
6.61. Interpretación física 802.1ah PBB Provider Backbone Bridge (Mac-in-Mac) 405
6.62. Estructura general agregación Ethernet 407
6.63. Acceso y agregación mediante red IP 408
6.64. Arquitectura general servicios triple oferta (I) 409
6.65. Arquitectura general servicios triple oferta (II) 410
6.66. VLAN Salida DSLAM (I): VLAN por Servicio 412
6.67. VLAN Salida DSLAM (II): VLAN por DSLAM 412
6.68. VLAN Salida DSLAM (III): VLAN por Protocolo 413
6.69. VLAN Salida DSLAM (IV): VLAN por abonado con QinQ . 414
6.70. Servicio triple play: distribución de TV 414
6.71. Servicio triple play: Video On Demand 415
6.72. Servicio triple play: RTSP 416
6.73. Servicio triple play: Diálogo RTSP 416

B.1. Recomendaciones Serie I de la UIT-T 423

C.1. Nomenclaturas y conceptos modelo OSI 428
C.2. Modo Operación modelo OSI 429
C.3. Protocolos TCP/IP frente modelo OSI 433
C.4. Perspectivas en el modelo OSI 434

E.1. Formato Cabecera IP V4 441
E.2. Formato Cabecera UDP 441
E.3. Checksum en UDP 442
E.4. Segmento TCP 444

F.1. Formato Trama MAC Ethernet 802.3 451
F.2. Formato Trama MAC Ethernet 455
F.3. Usos Etiqueta 802.1q (1) 455
F.4. Usos Etiqueta 802.1q (2)t 456
F.5. Usos Etiqueta 802.1q (3) 456

G.1. Red local IEEE 460
G.2. IPv4 Direcciones clase D 460
G.3. IP Multicast sobre Ethernet 460
G.4. Multicast entre Redes 461
G.5. Encaminamiento multicast 462

Índice de tablas

2.1. RDSI: Servicios Suplementarios 79
2.2. Valores SAPI 97
2.3. Asignación de TEIs 98
2.4. Tipos de Tramas LAPD 99
2.5. Valores discriminador de protocolo 104
2.6. Mensajes Q.931 para Conexión en Modo Circuito 107
2.7. Elementos de Información Mensajes Q.931 para Conexión en Modo Circuito 108
2.8. Elementos de Información Mensaje CONNECT en Modo Circuito 112
2.9. Elementos de Información Mensaje CONNECT ACKNOWLEDGE en Modo Circuito 113
2.10. Elementos de Información Mensaje CALL PROCEEDING en Modo Circuito 113
2.11. Elementos de Información Mensaje ALERTING en Modo Circuito 113
2.12. Elementos de Información Mensaje PROGRESS en Modo Circuito 113
2.13. Elementos de Información Mensaje SETUP en Modo Circuito 114
2.14. Elementos de Información Mensaje SETUP ACKNOWLEDGE en Modo Circuito 114
2.15. Elementos de Información Mensaje DISCONNECT en Modo Circuito 114
2.16. Elementos de Información Mensaje RELEASE en Modo Circuito 115
2.17. Elementos de Información Mensaje RELEASE COMPLETE en Modo Circuito 115

3.1. LSSU: Valores en Campo SF 136
3.2. Descripción Campos Unidades de Señalización MTP2 137
3.3. Valores campo Indicador de Servicio 151
3.4. SCCP: Números de Subsistema 163
3.5. SCCP: Primitivas Servicio Orientado a Conexión 166

3.6. SCCP: Primitivas Servicio No Orientado a Conexión 169
3.7. Función de los mensajes SCCP 170
3.8. Parámetros Mensaje IAM 181
3.9. Interfaces y Protocolos en GSM 203

4.1. Capas Físicas ATM estandarizadas 216
4.2. Jerarquía TDM 218
4.3. Valores campo Payload Type (PT) 228
4.4. Tipos de AAL 231
4.5. Categorías de Servicio ATM 253

5.1. Codecs Vocales 283
5.2. Modelo E: definición de categorías de calidad de transmisión de conversación 295
5.3. Características principales modelos predictivos 300
5.4. SCTP: Tipos de Pedazos 309
5.5. SCTP: Parámetros opcionales 309
5.6. RFC 1466: Telephony Signalling Transport over SCTP Applicability Statement 315
5.7. URIs SIP 324
5.8. Atributos SDP 333

6.1. Recomendaciones ITU-T para DSL 345
6.2. Capacidad sobre el par ADSL 351
6.3. Velocidades Tecnologías xDSL 360
6.4. Asignación VPI/VCI operadores 365
6.5. Características de ejemplo de canales descendente y retorno . 380
6.6. Características Capa Física DOCSIS 387
6.7. Diferencias MPLS - IEEE (QinQ/MinM) 406

C.1. Capas del Modelo OSI 430

NOMENCLATURA

A continuación recogemos en la siguiente figura la nomenclatura básica utilizada en el manual.

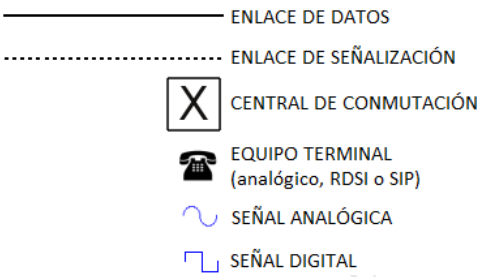

Figura 1: Nomenclatura básica

Y a ti, Frodo Bolsón, te entrego la Luz de Eärendil, nuestra más preciada estrella. Que ella te ilumine en los lugares oscuros cuando las demás luces se apaguen ...

Capítulo 1

Introducción a la Red Telefónica Conmutada [1]

1.1. Introducción

La red telefónica conmutada (RTC) se define como *un conjunto ordenado de medios de transmisión y conmutación que facilitan la comunicación oral entre dos abonados mediante el empleo de aparatos telefónicos.*

De la definición se deduce que el terminal telefónico forma parte de la propia red.

La RTC, completamente analógica en sus orígenes, ha sufrido un paulatino progreso de digitalización, ofreciendo cada vez un mayor número de servicios a los usuarios. Pero esta transición o digitalización no ha sido brusca, sino que se ha ido realizando poco a poco, en un proceso dependiente tanto del avance de la tecnología como de la rentabilidad de los costes de implementación o adaptación a dichas nuevas tecnologías. En esta evolución, se pueden definir ciertas etapas, recogidas en la figura 1.1, donde se comprueba como la red ha evolucionado desde el interior hacia el exterior de la misma.

El primer estado definible de la red telefónica conmutada, sin entrar en las fases de temprana implantación, experimentación o de explotación pre-tecnológica de la misma, se caracteriza por ser un sistema completamente analógico, es decir, todos los elementos de red eran analógicos. Los elementos conmutadores, denominados centrales por razones históricas, eran inicialmente elementos de conmutación manuales para ser reemplazados posteriormente por dispositivos electromecánicos. Los sistemas de transmisión eran explotados a baja frecuencia y usando técnicas de multiplexado por

[1] Este capítulo está basado en los trabajos [7], [12], [15] y [13].

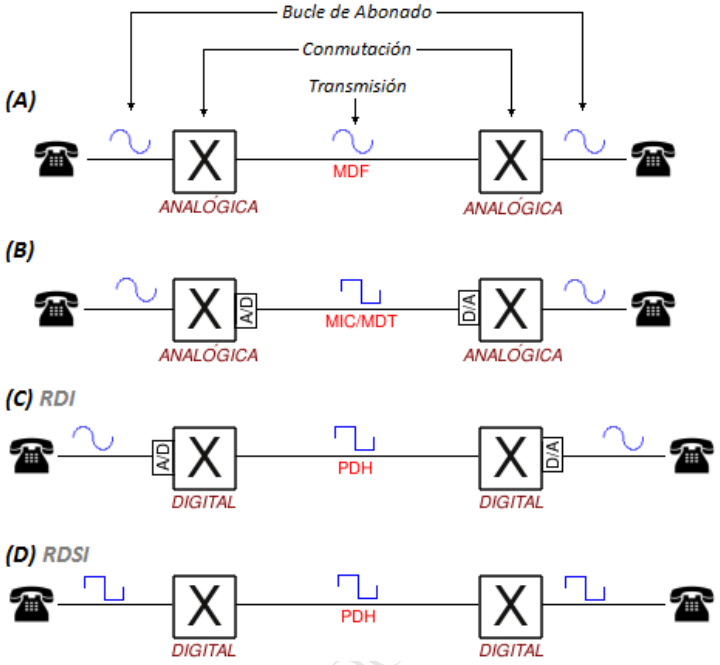

Figura 1.1: Evolución RTC

división de frecuencia. La conmutación era siempre espacial, usando matrices de conexiones para dar continuidad o conectividad eléctrica a la señal hacia el enlace apropiado, inclusive extremo a extremo de la conversación. Esta situación de la red, recogida en la figura 1.1.A, duró desde finales del siglo XIX hasta aproximadamente finales de los años 60 del siglo pasado, momento en que comienzan a digitalizarse algunos elementos.

La segunda etapa caracterizable en la evolución de la red telefónica conmutada, se basa en la digitalización de los sistemas de transmisión. Se introducen convertidores analógico/digital en los enlaces entre centrales de la red y se empiezan a utilizar técnicas de multiplexado por división de tiempo, por lo que desaparece la conectividad eléctrica entre los extremos de la conversación, aunque la conmutación se sigue realizando mediante elementos electromecánicos. Por tanto, fue el núcleo de la red el primer elemento en beneficiarse de las ventajas clásicas proporcionadas por la tecnología digital, como capacidad de regeneración de la señal y mayor capacidad, situación recogida en figura 1.1.B.

A partir de los años 80 y hasta la actualidad, la tecnología digital empieza a ser económicamente viable, permitiendo la digitalización de la conmutación. En este nuevo escenario, se realiza la conversión analógico/digital antes de entrar en el conmutador, por lo que es más fácil dotar a los nodos de

funciones de conmutación temporal. Las centrales son ahora pues digitales, siendo el conmutador un ordenador de propósito específico con un funcionamiento basado en SPC, Stored Program Control. Esta red en la que todo, salvo el bucle de abonado, es digital se conoce como la Red Digital Integrada, RDI, recogida en la figura 1.1.C. Al digitalizarse el bucle de abonado, se da paso a la Red Digital de Servicios Integrados, RDSI (figura 1.1.D).

Es decir, en la actualidad encontramos dos modalidades en despliegues de red, zonas en las que el bucle de abonado aún es analógico, y que denominamos RDI y otras zonas donde el bucle desplegado es digital, denominado RDSI, siendo el resto de la red el mismo para ambos despliegues.

Actualmente en España coexisten ambos bucles, mientras que la evolución ha sido diferente en otros países, como Francia o Alemania, donde predomina el acceso mediante RDSI.

Hemos realizado una pequeña introducción, a la evolución que la red telefónica conmutada ha sufrido desde su implantación a finales del siglo XIX hasta la situación actual, pero antes de eso cabría preguntarse, *¿por qué es necesaria una red?*

Las primeras comunicaciones telefónicas se llevaban a cabo uniendo los teléfonos directamente, por lo que dos personas que deseen hablar, tan sólo debían disponer de sendos terminales telefónicos y unirlos utilizando un cableado directo apropiado.

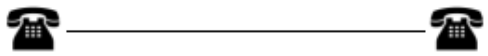

Figura 1.2: Necesidad de Red (0)

Si consideramos N personas, el número de cables necesarios será de *N(N-1)/2*, es decir del orden de N^2, como se muestra en la figura 1.3.

Así mismo será necesario en principio disponer de *N(N-1)* aparatos telefónicos, por lo que el coste de la instalación crecerá rápidamente a medida que incrementamos el número de usuarios. Para disminuir costes, y teniendo en cuenta que en un instante determinado sólo se está hablando con una persona, es posible tener un teléfono que incorpore un dispositivo (conmutador) que permita seleccionar la línea que se pretende utilizar, por lo que tan sólo hará falta un teléfono y un conmutador por usuario, aunque continuamos necesitando aproximadamente N^2 líneas telefónicas.

No obstante el coste de la instalación sigue siendo elevado debido al pre-

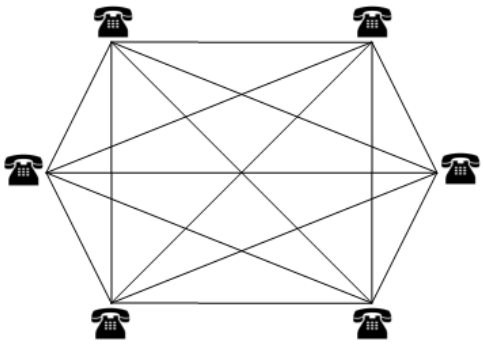

Figura 1.3: Necesidad de Red (I)

cio de las líneas, que es proporcional a la distancia entre usuarios. Además, resulta ineficiente pues un usuario sólo puede utilizar una línea en un instante de tiempo, quedando el resto ociosas. Pensemos que para 10.000 usuarios sería necesario instalar 50 millones de líneas, lo que dificulta la escalabilidad de la solución, que tan sólo será válida para pocos usuarios y siempre que no se encuentren muy alejados.

Un paso adelante en la solución de este problema se puede llevar a cabo alejando la conmutación de los usuarios. De esta forma todos los usuarios de una determinada zona, delimitada por el alcance óhmico de la señal, llevan una línea hasta el conmutador, disminuyendo el número de líneas necesarias hasta N. En el conmutador terminarán todas las líneas en unos conectores, o puntos terminales. En el conmutador se realiza la labor de conectar los dos puntos terminales correspondientes a los usuarios que deseen mantener una comunicación, como muestra la figura 1.4.

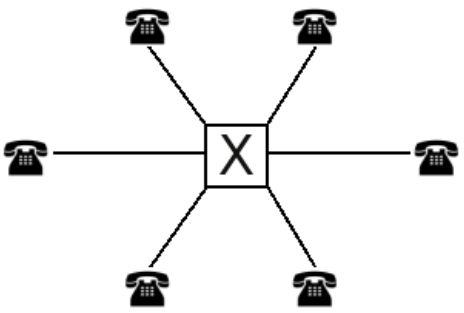

Figura 1.4: Necesidad de Red (II)

De esta forma, pasamos de tener una línea dedicada para cada usuario destino, a tener líneas compartidas entre todos los usuarios, con lo que el rendimiento aumenta. En 1878 aparece el primer tablero de conmutación

manual con capacidad para 21 abonados, mientras que los últimos tableros utilizados tenían una capacidad de hasta 10.500 abonados.

Cuando el número de abonados crece en exceso, y la distancia entre estos y la central de conmutación resulta elevada, se hace rentable tener una nueva central de conmutación y dividir a los abonados entre ambas, como recoge la figura 1.5, donde ya se aprecia una cierta jerarquía innata en la red.

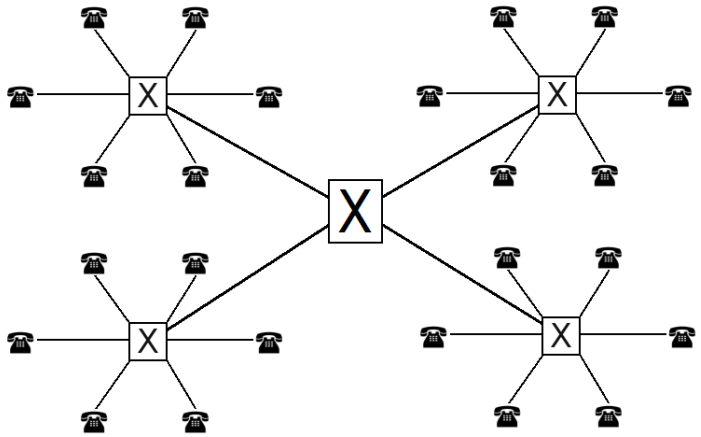

Figura 1.5: Necesidad de Red (III)

Así por ejemplo, para 240 abonados podemos pasar a disponer de 265 líneas, frente a las 26860 según el modelo anterior, justificándose así histórica y evolutivamente la **necesidad de implantación de las redes de comunicaciones** para dar soporte a la población.

Para facilitar la comunicación entre dichas centrales se establecen enlaces. A las líneas que conectan los abonados con sus centrales se les denomina extensiones o bucles de abonado (subscriber loop, local loop).

El objetivo fundamental de la es conseguir la conexión entre todos los usuarios de la red, a nivel geográfico local, nacional e internacional, por lo que por motivos tecnológicos (principalmente de alcance y de facilidad de tarificación) y también geopolíticos, se establece una jerarquía en la red.

La **estructura tradicional** de la red es jerárquica, como muestra la figura 1.6 donde se recoge la *jerarquía tradicional* de la RTC en España. Los nodos normalizados que forman parte de ella se conocen como: centrales locales, primarias, secundarias y finalmente terciarias o de tránsito internacional, donde debemos destacar que en países más extensos, la jerarquía se ampliaba hasta centrales de nivel cuaternario e incluso quinario.

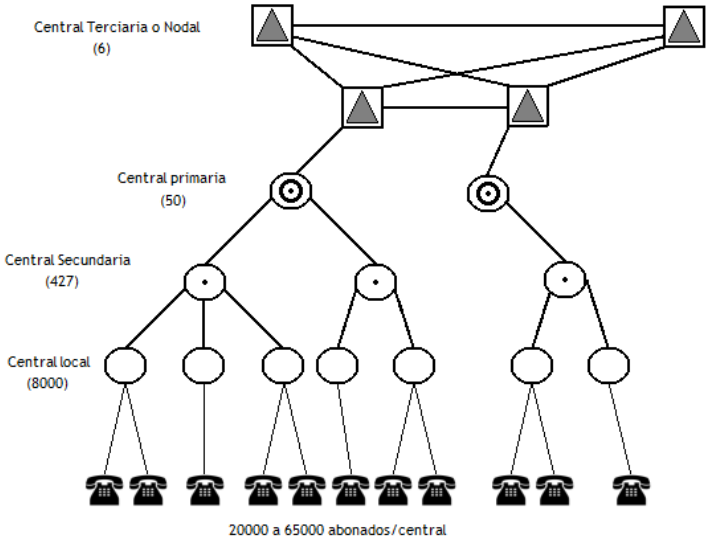

Figura 1.6: Jerarquía Tradicional

En la actualidad, con la introducción de los sistemas digitales, la jerarquía de la red ha evolucionado a una *jerarquía digital*, recogida en la figura 1.7 más sencilla que la tradicional, donde se distinguen únicamente dos tipos de centrales, las locales y las de tránsito. Para mejorar el despliegue hacia los usuarios se normaliza también el uso de concentradores remotos, que se encargan de digitalizar el tramo final de conexión con la central local para los usuarios de bucle analógico, algo por supuesto innecesario para los usuarios con bucle de acceso digital.

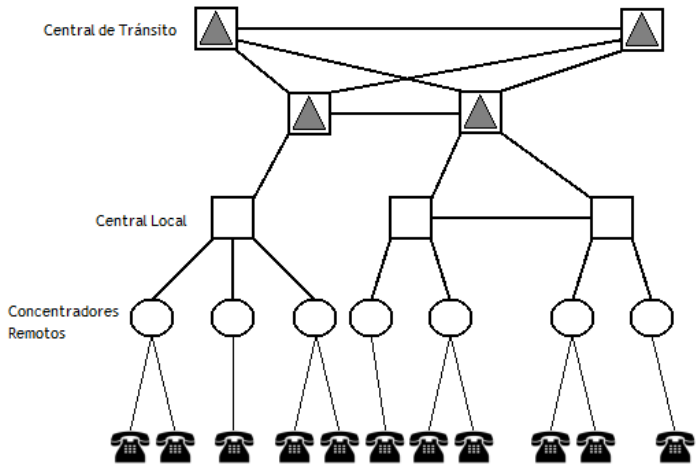

Figura 1.7: Jerarquía Digital

1.2. La red telefónica conmutada

La RTC es una red muy compleja, por lo que es habitual su estudio entendiendo la misma como un conjunto de subsistemas o subredes que interoperan entre sí y que pasamos a explicar a continuación.

1.2.1. Red de Acceso

También llamada planta exterior, está formada por la central de abonado (local o remota) y los bucles de abonado (analógicos o digitales), constituyendo el 90 % del coste total de la red.

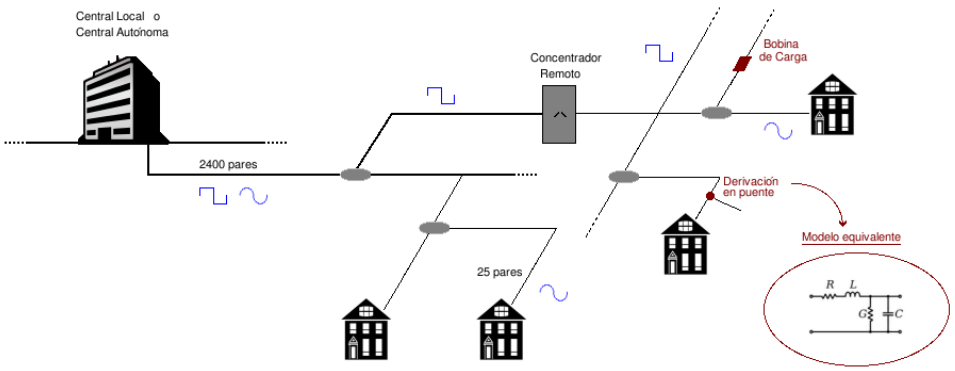

Figura 1.8: Red de Acceso. Visión general

Permite llevar la señal analógica desde el último nodo de la red hasta un punto denominado Punto de Terminación de Red, PTR, que se sitúa dentro de la vivienda del abonado. Como vemos en la figura 1.8, desde la galería de cables de la central, situada a nivel de subsuelo, salen líneas de usuarios agrupadas en cables multipares (2400, 4800, 9600 pares) a través de unas canalizaciones subterráneas llamadas ductos.

Estas canalizaciones intercalan, cada 150 m aproximadamente, distintas cámaras de registro que permiten el acceso al cableado y se encuentran protegidas contra la humedad y el agua. Desde estas cámaras de registro se realiza la segregación de pares, para el despliegue hacia los abonado de una zona, dividiéndose en cables multipares de menor número, y realizando posteriores segregaciones para poder alcanzar finalmente al usuario con un único par que finaliza en el PTR. A partir de este punto la instalación depende del abonado, pudiendo conectar un teléfono principal y varios supletorios.

Debemos destacar en también la presencia de otros elementos como las *bobinas de carga*, que logran disminuir la atenuación y la distorsión a frecuencias vocales, con el consiguiente aumento del alcance de la comunica-

ción, así como las *derivaciones en puente*, segmentos de cable no finalizados (sin resistencia de adaptación) utilizados para proveer de servicio a nuevos usuarios.

La distribución de las líneas de abonados, tal y como se recoge en la figura 1.9 se realiza utilizando concentradores remotos aunque pueden existir abonados directamente conectados a la central. Los concentradores remotos están formados por dos elementos principales, el denominado **SLTU, Subscriber Line Termination Unit** o Unidad de Terminación de Línea de Abonado, cuyas características estudiaremos junto con las tecnologías de bucle de abonado, el cual es utilizado para conectar las distintas líneas de abonado con la central, empleando para ello unos **multiplexores**, que permiten compartir enlaces hacia la central.

Es habitual el uso de marcos de distribución o bastidores (**Main Distribution Frames, MDF**) tanto en los concentradores remotos como en las centrales para facilitar el acceso y conexionado de las líneas con los distintos SLTUs y otros equipos.

Para reducir las capacidades de conmutación de la central, y por tanto el coste y mantenimiento de las mismas, es habitual utilizar concentradores que multiplexan a los distintos abonados, algo que permite el correcto funcionamiento de la red, dado que no se producen accesos masivos a la misma salvo en ocasiones excepcionales.

Sin embargo, en la figura 1.9 también se introduce como se ha reutilizado la red de acceso de la RTC para proporcionar nuevos servicios de telecomunicaciones. Principalmente se muestra como, sin modificar la planta existente es posible dar acceso a servicios de datos mediante tecnologías ADSL, por acceso indirecto en este ejemplo aunque existen otras configuraciones, mediante el uso de filtros que permiten separar los servicios en banda baja de los servicios en banda alta así como con la instalación en las centrales y concentradores de un nuevo tipo de equipo denominado **DSLAM, Digital Subscriber Line Access Multiplexer**.

El estudio completo de las distintas tecnologías y principales redes de acceso utilizadas actualmente se pospone para el capítulo 6 del texto.

El medio físico utilizado en la red de acceso de la RTC, el cable de pares dista mucho de ser el medio óptimo para el despliegue de una red de telecomunicaciones. Así pues, la red de acceso, conformada por múltiples cables de par trenzados sufre de numerosos problemas que afectan a su comportamiento. Las principales **fuentes de imperfecciones** que afectan al cable de par trenzado son:

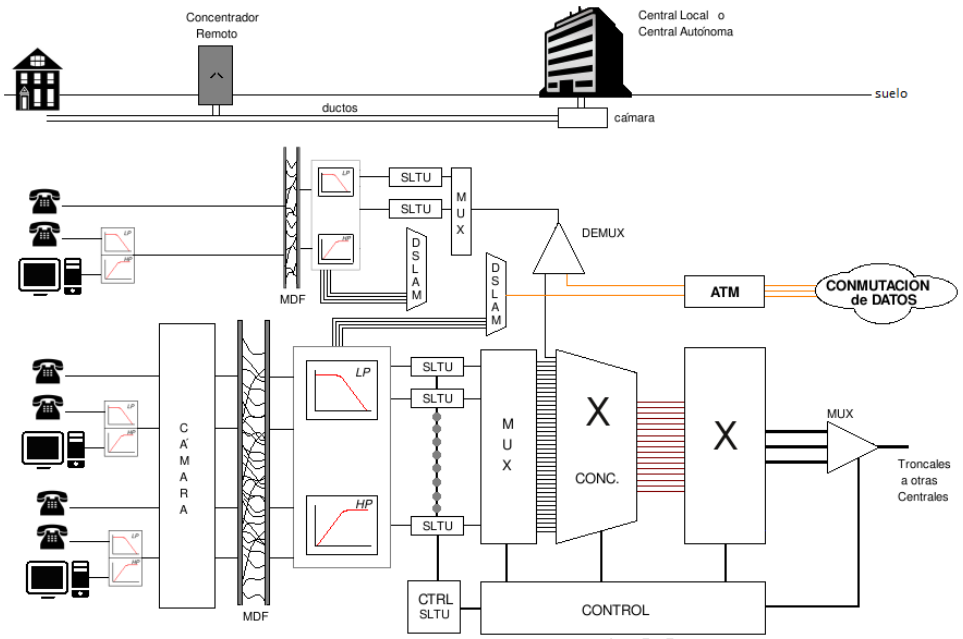

Figura 1.9: Uso de la Red de Acceso para otros servicios

- **Derivaciones en Puente.** Son segmentos de cable de longitud indeterminada que permiten obtener una mayor flexibilidad a la hora de asignar los cables de pares a los distintos abonados. Sin embargo, al ser terminaciones no adaptadas provocan la inserción de polos y ceros indeseados en la respuesta en frecuencia del sistema. Este filtrado indeseado (algunas frecuencias se eliminan y otras se amplifican) no es particularmente nocivo para los servicios en bandas bajas de frecuencia, como el servicio de voz, pero sí es agresivo para servicios en bandas altas, como el servicio de datos por tecnologías xDSL.

- **Edad del Cable.** Con el paso del tiempo se van produciendo microroturas e imperfecciones, que terminan produciendo un incremento en la atenuación que sufre la señal al recorrer el cable.

- **Multiplicidad de calibres en el mismo bucle.** Al realizar las instalaciones se utilizan cables de distintos grosores (es físicamente imposible utilizar siempre el mismo grosor de cable) y por tanto, de impedancias intrínsecas distintas, que se traducen en la aparición de distintas reflexiones de la señal.

- **Empalmes.** Igualmente, se producirán también reflexiones, al no estar correctamente adaptados dichos empalmes.

La red de acceso ha utilizado tradicionalmente señales a baja frecuencia

(servicio de voz) pero al tener un gran alcance, se comporta como un medio de transmisión, y se verá afectado por las **degradaciones** clásicas que afectan a cualquier otro sistema de transmisión. Típicamente:

- **Ruido.** Las comunicaciones se ven afectadas de forma genérica por el *ruido térmico*, fácil de modelar y combatir así como por otras fuentes de ruido de carácter impulsivo y por tanto más difíciles de evitar, como pueden ser los impulsos electromagnéticos provocados por motores (vehículos, maquinaria, ...), tormentas, marcación en la RTC, etc.

- **Interferencias.** Por ejemplo la provocada por los sistemas de radiodifusión AM (bandas de 10 KHz entre 560 y 1600 KHz, con -100 a -120 dBm/Hz) o también por los sistemas de radioaficionados (banda de 2.5 KHz). Debemos destacar eso sí, que las interferencias entre todos estos sistemas son recíprocas, es decir, los sistemas nombrados como ejemplo (y otros por supuesto) sufren asimismo interferencias provocadas por la transmisión de señales en la red de acceso.

- **Diafonía.** Se dice que entre dos circuitos existe diafonía, denominada en inglés Crosstalk (XT), cuando parte de la señal presente en uno de ellos, denominado circuito perturbador, aparece en el otro, denominado circuito perturbado.

  La diafonía, en el caso de cables de pares trenzados se presenta generalmente debido a acoplamientos magnéticos entre los elementos que componen los circuitos perturbador y perturbado o como consecuencia de desequilibrios de admitancia entre los hilos de ambos circuitos.

Figura 1.10: Diafonía

  Se distingue típicamente entre dos tipos de diafonía, representadas en la figura 1.10.

  - *Paradiafonía o Near End Crosstalk, NEXT.* Cuando la perturbación presentada está más próxima a la fuente perturbadora que a la fuente esperada (fuente del sistema perturbado). Es decir, se produce un acoplamiento eléctrico en el extremo cercano.
  - *Telediafonía o Far End Crosstalk, FEXT.* Cuando la perturbación presentada está más alejada de la fuente perturbadora que de

la fuente esperada (fuente del sistema perturbado). Es decir, se produce un acoplamiento eléctrico en el extremo lejano.

El **bucle de abonado** es aquella parte de la red de acceso que une al abonado/usuario con el primer nodo de la red de comunicación en cuestión, es decir, con el concentrador remoto o bien directamente con la central. Podemos encontrar dos modelos de bucle de abonado, según la tecnología utilizada:

Bucle de Abonado Analógico

Es el que caracteriza la denominada RDI. Utiliza dos hilos por abonado (un par trenzado), permitiendo transmisión y recepción simultánea por el mismo cable, distinguiendo las señales mediante el uso de la la bobina híbrida, que encontramos tanto en los terminales telefónicos como en el SLTU del abonado.

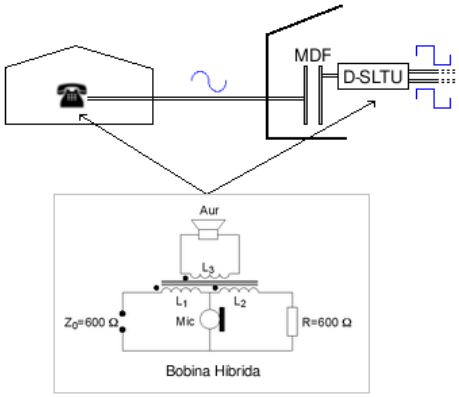

Figura 1.11: Bucle de Abonado Analógico

Se distingue como elemento fundamental el SLTU, Suscriber Line Termination Unit, ó Unidad de Terminación de Línea de Abonado, cuyas funciones principales son:

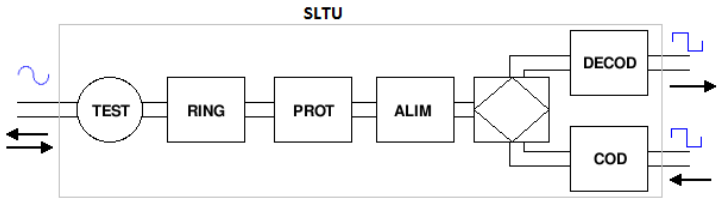

Figura 1.12: SLTU: Subscriber Line Termination Unit

- Alimentación (Battery feeding, los terminales telefónicos analógicos se alimentan a -48 V remotamente).

- Protección (Over voltage protection, para proteger las instalaciones del operador).
- Llamada (Ringing).
- Supervisión (Supervision).
- Codificación A/D (Coding).
- Conversión 2 a 4 hilos (Hybrid).
- Pruebas (Testing)

Dado que la red es digital, la señal analógica debe digitalizarse. Este proceso, en el caso del bucle de abonado analógico se realiza en el concentrador remoto o en la propia central, en cualquier caso *siempre antes de la conmutación*, realizando el siguiente proceso secuencial:

- Filtrado paso bajo 300-3400 Hz, para evitar el aliasing y usando un ancho de banda suficiente para conversaciones vocales.
- Muestreo a 8 KHz, cumpliendo el teorema de Nyquist. Este muestreo a 8 KHz es el que justifica que el período de trama en numerosas estructuras de datos de comunicaciones sea de 125 μs.
- Codificado logarítmico (Ley A) a 8 bits/muestra.

Por tanto, la señal digital resultante tiene una tasa de 64 Kbps, y es llamada Pulse Code Modulation, PCM o Modulación por Impulsos Codificados, MIC.

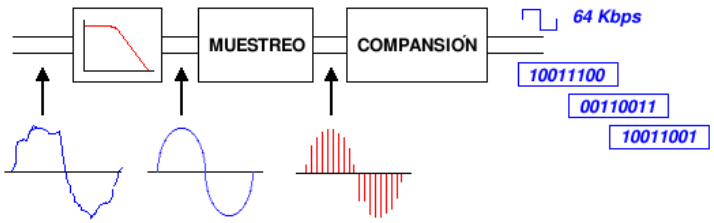

Figura 1.13: Codificación MIC (PCM)

Bucle de Abonado Digital

Utilizado en la denominada RDSI, se utilizan nuevamente dos hilos por abonado, pero en este caso la multiplexión se realiza en el dominio del tiempo, usando técnicas de multiplexión por división en el tiempo, MDT.

Encontramos en este caso una versión digital del SLTU, D-SLTU, donde las labores que realiza son similares a su equivalente analógico, como alimentación, protección, supervisión, pruebas, etc., aunque algunas no son necesarias, dada la naturaleza completamente digital de este escenario.

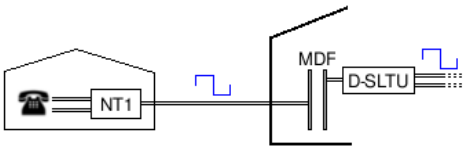

Figura 1.14: Bucle de Abonado Digital

Los primeros sistemas PCM fueron desarrollados para transmisión telefónica sobre cables que originalmente estaban diseñados para transmisión en frecuencias de audio. Se encontró que dichos cables eran aptos, usando una adecuado codificación bipolar, para una transmisión binaria de hasta 2 Mbit/s. Consecuentemente, los canales telefónicos son combinados mediante técnicas de multiplexión por división en el tiempo para formar un ensamblado de 24 o 30 canales.

Este ensamblado, correspondiente con una trama de capa física, se conoce como Grupo Múltiplex Primario. Se utiliza como bloque constructivo básico para el ensamblado de un mayor número de canales, en Grupos Múltiplex de mayor orden, como veremos más adelante.

El funcionamiento de un multiplexor primario se muestra en la figura 1.15. La longitud (duración) de la trama es de 125 μs, que se corresponde lógicamente con el período de muestreo de una señal de voz. Contiene una muestra de cada canal telefónico, junto con algunos dígitos (intervalo 16) usados para sincronización y señalización.

Existen dos configuraciones ampliamente utilizadas, el sistema Europeo de 30 canales, comúnmente denominado E1 y el Sistema DS1 de 24 canales, utilizado en Norteamérica y Japón.

Ambos sistemas emplean una codificación de 8 bits, diferenciándose en que el sistema europeo utiliza la Ley A de compresión mientras que el sistema DS1 utiliza la Ley μ de Compresión.

Como vemos en la figura 1.15, la trama de 30 canales se divide en 32 intervalos de tiempo (time-slots), cada uno de 8 dígitos binarios. Por lo

tanto, la tasa binaria resultante es de

$$8 \text{ KHz} \times 8 \times 32 = 2{,}048\text{Mbit/s} \tag{1.1}$$

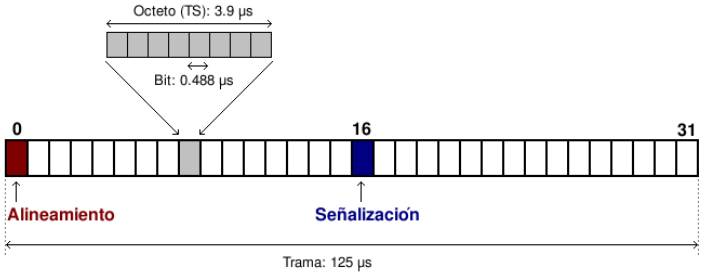

Figura 1.15: Formato de trama PCM (E1)

Los intervalos de tiempo 1 a 15 y 17 a 31 están asignados para canales de voz. El intervalo 0 se usa para alineamiento, mientras que el intervalo de tiempo 16 se utiliza para señalización, como veremos más en profundidad a lo largo del texto.

1.2.2. Red de Conmutación

Los sistemas de conmutación y los sistemas de señalización asociados, son esenciales para el funcionamiento de las redes de telecomunicación. Las funciones realizadas por los sistemas de conmutación, o un subsistema de ellos, con el fin de proporcionar servicios a los clientes se suelen denominar facilidades (facilities).

A lo largo de los años, el diseño de sistemas de conmutación se ha vuelto más sofisticado, con el fin de proveer facilidades adicionales que permitan a las redes proveer de más servicios a los clientes, a la vez que facilitan las labores de operación y mantenimiento.

A pesar de loa complejidad de los modernos sistemas de conmutación, existen una serie de funciones básicas que deben ser realizadas por todos los sistemas de conmutación y que pasamos a comentar brevemente:

- **Attending o Asistencia.** El sistema debe monitorizar de forma continua todas las líneas para detectar peticiones de llamada. La señal 'calling' se conoce a menudo como señal 'seize' (apoderar), ya que obtiene un recurso del intercambio.
- **Recepción de Información.** Además de las señales de llamada y liberación, el sistema debe ser capaz de recibir información del llamante

para la línea llamada, o cualquier otro servicio. Esto se suele llamar como la señal de dirección.

- **Procesamiento de Información.** El sistema debe procesar la información recibida para determinar las acciones a realizar y controlar el desarrollo de dichas acciones. Dado que tanto el origen como la terminación de la llamada, son manejadas de forma diferente por diferentes clientes, la información del tipo de servicio debe ser procesada junto con la información de direccionamiento.

- **Busy Testing o Test de Ocupación.** Habiendo procesado la información recibida para determinar el requerido circuito de salida, el sistema debe realizar un test de ocupación para determinar si el circuito está libre o está siendo utilizado por otra llamada.

- **Interconexión.** Para una llamada entre dos clientes, se realizan tres conexiones en el siguiente orden:

  - *Conexión al terminal llamante.*
  - *Conexión al terminal llamado.*
  - *Conexión entre los dos terminales.*

- **Alerting o Aviso.** Habiendo realizado las pertinentes conexiones, el sistema envía una señal para avisar al cliente llamado de la llamada, por ejemplo, enviando la señal de aviso (RINGING) al teléfono del cliente.

- **Supervisión.** Después de que el terminal llamado haya respondido, el sistema continua monitorizando la conexión para poder ser capaz de liberarla cuando la llamada finalice y poder aplicar la tarificación correspondiente.

- **Envío de información.** Si la línea del cliente llamado está localizada en otra central se requiere del uso de la función de envío de información adicional. La central generadora debe señalizar la dirección requerida a la otra central (o centrales intermedias si es que fuera necesario).

Es un hecho, que los sistemas de conmutación han ido evolucionando a la par que evolucionaba la tecnología. En este punto del texto, nos es suficiente con recopilar una breve evolución de los sistemas de conmutación, con sus hitos tecnológicos más destacados:

- **Sistemas manuales (1878):** se utiliza conmutación espacial. Fue un trabajo realizado por mujeres, las denominadas operadoras, dado que ofrecían mejor rendimiento en este trabajo que el realizado por hombres. Las operadoras realizaban la conmutación de los circuitos

manualmente interconectando los distintos *dicordios* para establecer el circuito físico entre los usuarios. Históricamente consistió asimismo uno de los primeros trabajos que permitieron el acceso al mundo laboral técnico de la mujer.

- **Sistemas automáticos electromecánicos:** la primera gran evolución de la RTC fue el cambio de conmutación manual a automática en las centrales, permitiendo a estas realizar las tareas de conmutación mediante autómatas electromecánicos y eliminando la necesidad de operadores humanos. Distinguimos:

  - *Sistema rotatorio Strowger (1891).*

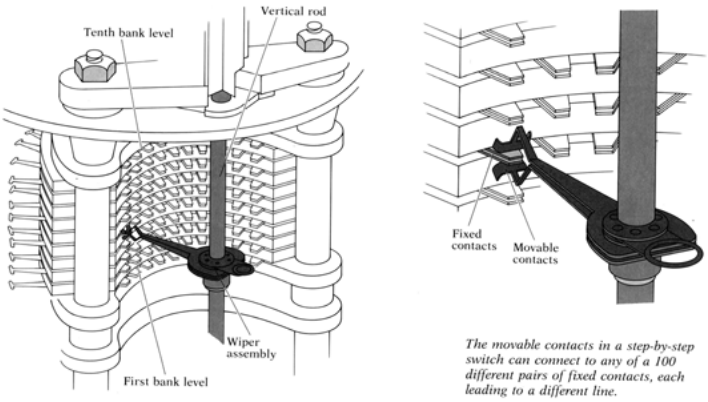

Figura 1.16: Strowger Switch [2]

  - *Sistema de barras cruzadas Betulander (1938).*
  - *Sistemas Reed (1965):* destacaron por ser los primeros en no incluir partes móviles, lo que facilitó el mantenimiento logrando a la vez mejorar la velocidad y capacidad de conmutación.

- **Sistemas electrónicos:** son los sistemas de conmutación utilizados actualmente. Se propició el uso de los mismos conforme las tecnologías electrónicas digitales comenzaron a ser rentables económicamente. Se caracterizan por:

  - *Conmutación Temporal:* la conmutación consiste en realizar copias de muestras de voz digitalizada desde una cierta entrada, canal o time slot de una trama PCM, hacia su correspondiente salida, otro intervalo de tiempo de otra múltiplex.

[2] `http://people.seas.harvard.edu/~jones/cscie129/nu_lectures/lecture11/switching/strowger/strowger.html`

  - *Generalización del control por programa o Stored Program Control, SPC,* ordenador de propósito específico para el control de la conmutación digital.
  - *Conmutadores de paquetes:* la última evolución en la conmutación digital, donde las muestras de voz son conmutadas intrínsecamente al ir encapsuladas en datagramas IP, que atraviesan la red.

- **Sistemas fotónicos:** próxima evolución de los sistemas de conmutación, aún en fase de investigación y experimentación.

Evidentemente, un estudio detallado de estos sistemas y su evolución tecnológica (mecánica, eléctrónica, óptica) se escapa del field of view de este manuscrito, no dejando de ser una interesante lectura, para lo que se remite al lector interesado al capítulo 3 de la referencia [7].

La conmutación automática, hace necesaria la aparición de un método que permita a usuarios y conmutadores ponerse de acuerdo para establecer y liberar las comunicaciones, ya que la interfaz humana de las operadoras es suprimida, lo que imposibilita el uso del lenguaje oral. Nace la señalización, que consta inicialmente de señales eléctricas sencillas basadas en corriente continua, que permiten al usuario saber si el abonado destino está libre, cuándo debe marcar, etc. y a los conmutadores conocer el abonado destino mediante una sucesión de pulsos que equivalen a dígitos.

Las mejoras en las tecnologías de conmutación facilitaron el incremento de capacidad en la red, en cuanto a número de abonados, de forma rápida y ordenada. Con el crecimiento del número de usuarios en la red, los enlaces entre centrales se hacían necesarios cada vez en mayor número, lo que propició la aparición de técnicas de multiplexión que permiten compartir un mismo medio de transmisión entre varias comunicaciones, disminuyendo de esta forma el coste de despliegue de la red.

Actualmente, toda la conmutación que se realiza en las redes de telecomunicación es inherentemente digital, acorde a la tecnología predominante. Tal y como hemos ya anticipado, la conmutación consiste en realizar copias de los bits de entrada (correspondientes a las muestras de un canal telefónico) hacia la salida correspondiente.

Como muestra la figura 1.17, es una práctica habitual utilizar concentradores en la entrada a la matriz de conmutación, es decir, existen menos entradas a la matriz de conmutación que líneas de abonado activas. Este aparente subdimensionamiento es factible ya que los usuarios no acceden de manera simultánea a la red.

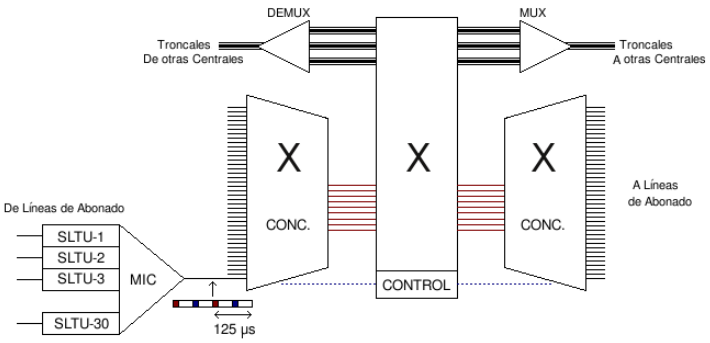

Figura 1.17: Conmutación Digital

Debido a la criticidad de los sistemas de conmutación para el funcionamiento de la red, se consigue una alta fiabilidad mediante la redundancia (duplicación) de equipos, donde como dato representativo podemos decir que la red telefónica ha estado únicamente 2 horas sin servicio en un período de 40 años.

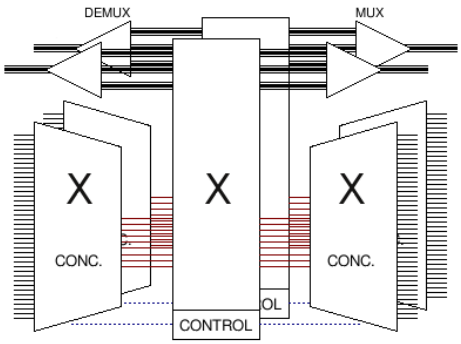

Figura 1.18: Redundancia Red de Conmutación

1.2.3. Red de Transmisión

A pesar de que el contenido del texto se centra principalmente en los conceptos y aspectos relacionados con los sistemas de conmutación utilizados en las redes de comunicaciones, es imposible no hacer al menos algunas apreciaciones y repaso de conceptos relacionados con la transmisión de señales para poder entender en su conjunto el funcionamiento de dichas redes.

Los sistemas de transmisión proveen de circuitos entre los distintos nodos de las redes de telecomunicación. Si un circuito utiliza caminos o medios de transmisión diferentes en cada sentido de la transmisión, dichos caminos suelen llamarse canales.

Actualmente existe una amplia variedad de tecnologías utilizadas como sistemas de transmisión, partiendo desde un básico sistema de circuitos de audio frecuencia sin amplificar, hasta complejos sistemas de comunicaciones vía satélite.

Tanto los canales como las señales que los ocupan, pueden ser clasificados en dos amplios grupos: Sistemas Analógicos y Sistemas Digitales. Actualmente en la RTC se mantiene la transmisión analógica únicamente en el bucle de abonado, siendo digital en el resto de la red. Es interesante volver a destacar que la transmisión fue el primer elemento o subsistema digitalizado en las redes telefónicas.

Dicha transmisión digital se basa en el uso del bloque constructivo básico ya comentado del Multiplex Primario (E1), compuesto por 30 canales MIC.

El multiplex primario no es por si sólo suficiente y es necesario agrupar por motivos prácticos más de 30 canales en los enlaces existentes entre distintas centrales de la red. El modo en que se realizan dichas agrupaciones está definido, encontrando dos modos principales de hacerlo, mediante la Jerarquía Digital Plesiócrona (PDH) y la Jerarquía Digital Síncrona (SDH).

Jerarquía Digital Plesiócrona, PDH

En una red de transmisión que no ha sido diseñada para un funcionamiento síncrono, las entradas en un multiplexor digital generalmente no serán exactamente síncronas. A pesar de que tengan la misma tasa binaria nominal, normalmente provienen de fuentes con distintos osciladores, que pueden o suelen mostrar una cierta variación en su frecuencia nominal de oscilación. Estos sistemas se denominan plesiócronos.

La primera generación de multiplexores digitales de alto orden descritos en este apartado se diseñaron para funcionar en este tipo de situaciones. Ellos conforman la Jerarquía Digital Plesiócrona, comunmente nombrada como PDH, por sus siglas en inglés *Plesiochronous Digital Hierarchy*.

Si las entradas a un multiplexor síncrono tienen todas las misma tasa de transmisión y están en fase, dichas entradas pueden ser entrelazadas tomando un bit o grupo de bits de cada una de ellas en cada turno. Este proceso se puede realizar por un switch que muestree cada entrada bajo el control del reloj del multiplexor.

Existen dos métodos generales para realizar el entrelazado de señales digitales: el entrelazado de bit y el entrelazado de palabra.

En el entrelazado de palabra, se toma únicamente un bit por cada canal tributario en cada turno. Si tenemos N entradas, cada una de ellas con una tasa binaria de f_t bits/s, la señal combinada tendrá una tasa final de $N \times f_t$ bits/s y cada elemento de la señal combinada tendrá una duración equivalente a 1/N de un dígito de entrada.

En el entrelazado de palabra, se toma un grupos de bits por cada canal tributario en cada turno, lo cual implica la necesidad de disponer de un almacenamiento o memoria para cada canal de entrada, donde guardar los bits que aún esperan a ser entrelazados.

Dado que el entrelazado de bits es más sencillo de realizar fue el elegido para los sistemas PDH, que fueron los primeros en aparecer históricamente.

Existen actualmente tres conjuntos de estándares para la multiplexación PDH, centradas en Europa, América del Norte y Japón. El estándar europeo, recogido en la figura 1.19, se basa en el multiplex primario de 30 canales (trama MIC o PCM o E1), mientras que los estándares americano y japonés se basan en el multiplex primario de 24 canales.

Los tres sistemas utilizan entrelazado de bits. La longitud (duración) es la misma que para el multiplex primario, es decir 125 μs, herencia de la tasa básica de muestreo del canal vocal a 8 KHz.

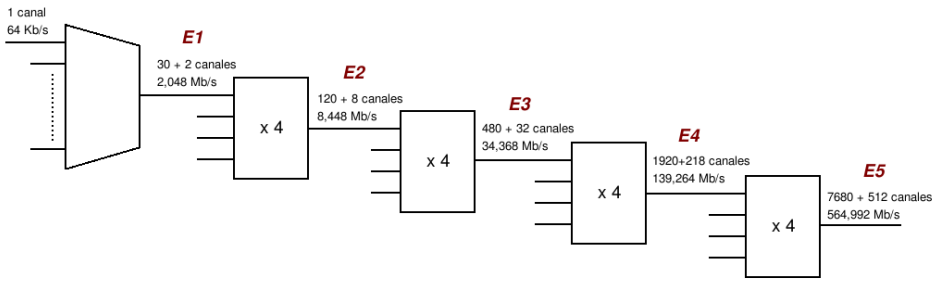

Figura 1.19: Red de Transmisión: Estándar PDH Europeo

Sin embargo, tal y como se aprecia en la figura, cuando los N flujos tributarios son combinados, el número de dígitos contenidos en las tramas de orden superior es mayor que N veces el número de dígitos en cada trama tributaria. Esto ocurre porque es necesario añadir dígitos de encabezamiento extra por dos motivos.

El primero de ellos es el **alineamiento de trama**. El demultiplexor de orden superior debe reconocer el comienzo de cada trama para poder enca-

minar los posteriores dígitos recibidos hacia sus correspondientes flujos de salida (de menor orden), tal y como debe realizar el multiplexor primario hacia los respectivos canales vocales finales y se utiliza por tanto la misma técnica que en este caso. Un código único es enviado como palabra de alineamiento de trama (Frame Alignment Word, FAW), que es reconocida por el demultiplexor y utilizada para mantener su funcionamiento en sincronismo con la señal de entrada. El estándar europeo utiliza un bloque FAW al comienzo de cada trama, mientras que el resto de estándares utilizan FAWs distribuidos.

El segundo motivo que justifica el relleno de bits extra en la trama es la realización de un proceso que denominamos **justificación**. Este proceso permite habilitar al multiplexor y al demultiplexor para mantener un funcionamiento correcto, aún cuando las señales tributarias de entrada al multiplexor puedan presentar una deriva (drift) o fluctuación relativa entre ellas.

Si una entrada tributaria es lenta, se introduce un dígito de justificación o relleno (dummy) que permite mantener la tasa binaria correcta de salida. Si el canal tributario aumenta su velocidad, no se hace necesaria la justificación. Estos bits de justificación deben ser eliminados por el multiplexor para enviar la secuencia correcta de bits al canal de salida. Por lo tanto, más bits adicionales llamados bits de Servicio de Justificación deben ser añadidos a la trama por el multiplexor para indicar al demultiplexor si se han utilizado bits de justificación en cada canal tributario.

Jerarquía Digital Síncrona, SDH

La introducción de redes de comunicaciones digitales integradas resultó en la necesidad de una transmisión totamente sincronizada, provocando el surgimiento de la denominada Jerarquía Digital Síncrona, o SDH, de sus siglas en inglés *Synchronous Digital Hierarchy*, definida por el CCITT en 1990.

En los Estados Unidos esta jerarquía se denomina Synchronous Optical Network, SONET, desde que los multiplexores utilizan interfaces ópticas. La jerarquía SDH utiliza una tasa binaria básica de 155.52 Mbit/s y múltiplos de ella en factores de 4N, tal y como vemos en la figura 1.20.

Cualquiera de los flujos plesiócronos existentes definidos por el CCITT de hasta 140M bit/s pueden ser multiplezados en la tasa básica de tansporte de SDH de 155.52 Mbit/s. SDH incluye también canales de gestión, los cuales tienen un formato estándar de mensajes para gestión de red.

La señal básica SDH, llamada *Synchronous Transport Module at Level 1,*

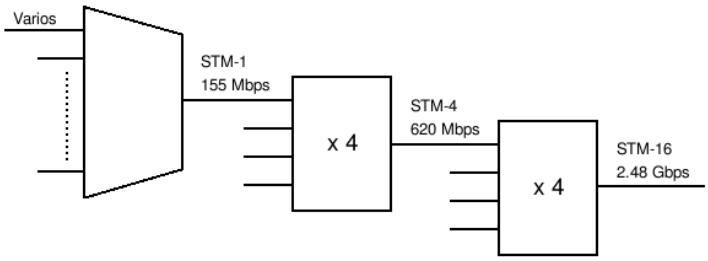

Figura 1.20: Red de Transmisión: Jerarquía Digital Síncrona (SDH)

STM-1 y contiene 9 segmentos iguales con octetos de cabecera al comienzo de cada uno de ellos. El resto de octetos son una mezcla de cabeceras y tráfico, que depende del tipo de tráfico cursado. La longitud total es de 2430 octetos, donde cada puntero ocupa 9 octetos. Así, la tasa binaria final es de 155520 Kbit/s, que normalmente se denomina 155 Mbit/s.

Esta trama se suele representar como una tabla de 9 filas y 270 columnas de 8 bits, como se muestra en la figura 1.21.

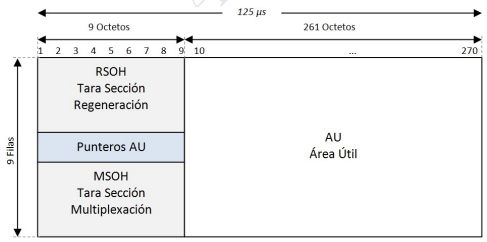

Figura 1.21: Red de Transmisión: Formato Trama SDH

Las primeras 9 columnas conforman la sección de cabeceras (Section Overheads, SOH), con funciones de alineamiento de tramas, monitorización de errores y datos. Las restantes 261 columnas comprenden la carga útil, donde se pueden mapear una gran variedad de señales.

Cada flujo tributario al multiplex tiene su propia zona de carga útil, conocida como Unidad Tributaria (Tributary Unit, TU). En América del Norte, se le denomina Tributario Virtual (Virtual Tributary, VT). Cada columna contiene 9 octetos, uno de cada fila, donde cada octeto tiene una capacidad de 64 Kbit/s. Tres columnas (27 octetos) pueden sostener una señal PCM de 1.5 Mbit/s, con 24 canales vocales y algunas cabeceras. Cuatro columnas pueden mantener una señal PCM de 2 Mbit/s con 32 intervalos de tiempo.

La trama STM-1 puede incluso llevar cargas de las tasas europeas de 8.34 y 140 Mbit/s y las tasas americanas de 6 y 45 Mbit/s.

En el proceso de multiplexión, los octetos de un afluente son ensamblados dentro de un contenedor, al que se le añade un puntero de cabecera, formando en conjunto un contenedor virtual (Virtual Container, VC). El contenedor virtual viaja a través de toda la red como un paquete completo hasta que es demultiplexado. Dado que el contenedor virtual puede no estar totalmente sincronizado con la trama STM-1, su punto de comienzo está indicado por un puntero. El contenedor virtual junto con su puntero constituyen la Unidad Tributaria, así que es la Unidad Tributaria la que está fijada a la trama STM-1.

los punteros ocupan unas posiciones fijas en la trama STM-1 y son sus valores numéricos los que muestran donde comienzan los contenedores virtuales, permitiendo así que la demultiplexión pueda realizarse.

Concluimos haciendo hincapié, tal y como hemos visto en los 2 subapartados anteriores, que tanto PDH como SDH disponen de tácticas para contrarrestar posibles fluctuaciones en los relojes de las señales afluentes a la entrada del multiplexor.

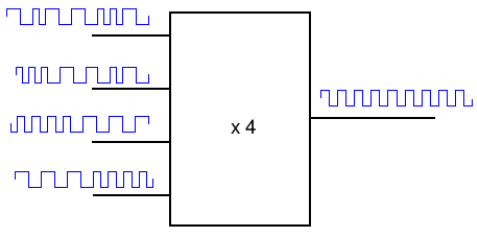

Figura 1.22: Red de Transmisión: Fluctuación de relojes

Como se aprecia a modo de resumen en la figura 1.22, en PDH esto se lograba utilizando bits de relleno o justificación, mientras que en SDH, se utiliza un desplazamiento de octeto en la carga útil mediante un puntero.

1.2.4. Red de Sincronización

Hemos introducido algunos aspectos implicados en el proceso de conmutación digital y de operación de una red, donde se supone de forma general que todos los sistemas de transmisión conectados a una central de conmutación se encuentran operando a la misma velocidad (tasa binaria), que es la misma a la que opera toda la lógica digital dentro de la propia central. Esta condición, conocida como sincronismo, es necesaria para cualquier proceso de conmutación en enlaces digitales.

En este apartado realizaremos una pequeña introducción a su problemática y enfoques para solventarla.

En primer lugar, suponiendo que todos los relojes implicados en un sistema digital complejo como es una red de telecomunicación (o parte de ella) funcionan a la misma velocidad nominal, *¿cómo se produce la falta de sincronismo?*

La falta de sincronización en un sistema Transmisor/Receptor viene provocada por las fluctuaciones de fase que aparecen en los relojes[3] del sistema. Dichas fluctuaciones se pueden producir por muchos motivos, entre ellos:

- Imperfecciones.
- Envejecimiento.
- Exactitud en la sintonización (ajuste).
- Ruido e interferencias.
- Elongaciones del medio.
- Cambios en la velocidad de propagación.
- Efecto Doppler (apreciable cuando las distancias son significativas, como en los sistemas de comunicaciones por satélite.

Los deslizamientos de trama o *slips*, ocurren de forma periódica en un sistema digital en el que hay un desajuste entre las frecuencias de entrada y salida de línea. La tasa de deslizamiento depende del grado de desajuste.

Cada deslizamiento comprende un error digital resultante de la inserción o pérdida de uno o más bits.

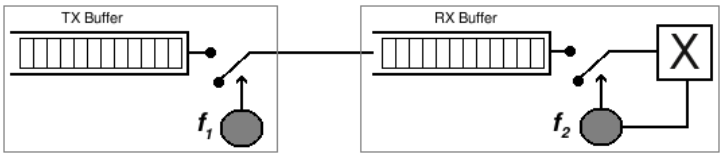

Figura 1.23: Red de Sincronización: Deslizamiento de Trama (slip)

Utilizando la figura 1.23, vemos que si las frecuencias de los relojes no son las mismas, se producirán desplazamientos de tramas, concretamente, y suponiendo que inicialmente el buffer de recepción se encuentra inicialmente ocupado a la mitad de su capacidad:

[3]Reloj implica aquí información de temporización: *cuánto dura un segundo.*

- $f_1 > f_2$. El buffer de recepción termina por desbordarse, por lo que habrá que purgar el buffer eliminando una trama completa.
- $f_1 < f_2$. El buffer de recepción termina por vaciarse, por lo que será necesario repetir la trama anterior entera o bien, rellenar con ruido.

La aparición de deslizamientos de trama en las comunicaciones, tiene una serie de efectos que dependen del tipo de servicio o aplicación envuelta. Por ejemplo en una comunicación vocal, un slip puede producir un efecto «CLIC» mientras que en puede producir un error de trama si el tráfico cursado es de datos, siendo por tanto más nocivo para el tráfico de datos.

Normalmente se exigen unos requisitos de calidad mínimos para el sincronismo bastante restrictivos. En conexiones en un mismo país, y para tasas de 64 Kbit/s el límite es de 5 slips/24 horas, mientras que para conexiones internacionales el límite permitido es de 4 slips/1000 horas.

¿Cómo se combate la aparición de slips? Existen dos enfoques para mantener el sincronismo en una red de comunicaciones, es decir, para reducir la ocurrencia de desplazamientos de tramas en redes digitales. Dichos enfoques son el *funcionamiento plesiócrono* y el *funcionamiento síncrono*.

Funcionamiento Plesiócrono

En el modo de funcionamiento plesiócrono, cada reloj opera de forma independiente, es decir no existe una red de sincronización y los relojes por tanto no se ajustan entre sí. Los desplazamientos de trama se mantienen en un nivel permitido utilizando relojes de alta estabilidad, los cuales son periódicamente resintonizados o reajustados, de manera que todos operan dentro de unos márgenes de frecuencia nominal establecidos para la red.

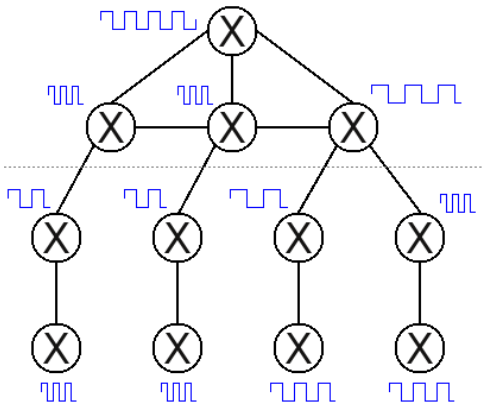

Figura 1.24: Red de Sincronización: Funcionamiento Plesiócrono

Este enfoque se suele utilizar para conexiones internacionales y para conexiones entre diferentes operadoras.

Funcionamiento Síncrono

Una red síncrona tiene todos sus relojes controlados por un mecanismo automático, de manera que todos ellos operan a la misma frecuencia de red, normalmente definida por un reloj atómico de cesio de alta precisión (reloj propio, o del sistema GPS, o de otros sistemas de navegación, ...). En realidad, los relojes se mantienen a la misma frecuencia media, pero con pequeñas variaciones a corto plazo.

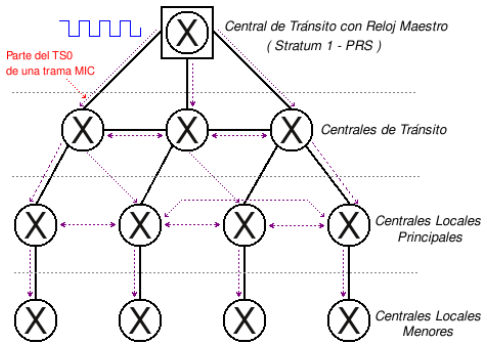

Figura 1.25: Red de Sincronización: Funcionamiento Síncrono

Como vemos en la figura 1.25, superpuesta a la red de transmisión encontramos una red de sincronización, que es el comentado mecanismo de ajuste de los relojes. Dicha red de sincronización no es una red independiente, sino que esta formada por cierta capacidad sobrante existente en la red de transmisión, típicamente en el intervalo de tiempo 0 del multiplex primario.

Comentar también que existen múltiples filosofías dentro del enfoque síncrono. Se puede apostar por una sincronización tipo Maestro-Esclavo (entre centrales de distinto nivel jerárquico) o bien por una filosofía de sincronización mutua (entre centrales del mismo nivel jerárquico). Por supuesto, en la práctica existen aún más variantes dentro de cada tipo.

Este enfoque es el que suele ser utilizado en redes pertenecientes a un mismo operador. Es decir, entre centrales de un mismo operador se utiliza un funcionamiento síncrono, y entre centrales de distintos operadores se utiliza un mecanismo plesiócrono.

1.2.5. Red de Señalización

En las redes de telecomunicación, los sistemas de señalización (o Red de Señalización) son tan esenciales como los sistemas de conmutación (Red de Conmutación) y los sistemas de Transmisión (Red de Transmisión).

La red de señalización es la que permite el diálogo entre las distintas entidades dentro de una red telefónica (terminales, centrales, centros de gestión, ...).

En una conexión multienlace, es necesario enviar señales en ambas direcciones, entre la línea llamante y la central origen, entre la línea llamada y la central destino, y por supuesto entre las posibles centrales intermedias.

Es decir, la señalización es el medio que permite al abonado establecer y liberar llamadas, es por tanto una de las funciones de la interfaz de línea. Permite también a las distintas centrales dialogar entre sí, algo necesario ya que como hemos dicho los abonados pueden estar en centrales diferentes y por tanto pueden ser varias las centrales que se vean involucradas en una única llamada.

Vamos a realizar dos clasificaciones de los sistemas de señalización, una primera ligada al modo en que físicamente se cursa la señalización y otra clasificación en que distinguimos el tipo de señalización según quien la ejecute.

La señalización en una red puede seguir dos caminos distintos. Puede usar los mismos circuitos que la voz, lo que se conoce como *Señalización Asociada al Canal o Channel Associated Signalling, CAS* o bien utilizar para su transporte una red o canales específicos, que es el caso de la *Señalización por Canal Común o Common Channel Signalling, CCS.*

- **Señalización Asociada al Canal, CAS.** Históricamente fue la primera en aparecer (por facilidad tecnológica en su implementación), aunque actualmente presenta una serie de limitaciones considerables:
  - Repertorio de señales reducido: decolgar, respuesta, ...
  - Difícil de expandir.
  - Válido solo para telefonía.
  - Audible al Usuario [4].
  - Ineficiente uso de la capacidad.
  - Cada canal de voz necesita y porta su señalización.

[4] `http://http://es.wikipedia.org/wiki/Joybubbles`

- **Señalización por Canal Común, CCS.** Los sistemas CCS son ampliamente utilizados hoy en día en las redes de comunicaciones públicas tanto nacionales como internacionales. Basada en el envío de paquetes por un canal de datos independiente de los canales de comunicación vocal, lo cual confiere una serie de importantes ventajas respecto a la señalización CAS, como por ejemplo:

  - Amplio repertorio de mensajes
  - Facilidad de extensión para nuevos servicios
  - Válido entre centrales y para el abonado
  - Totalmente digital, por lo que es independiente de la transmisión
  - Ineficiente uso de la capacidad
  - Cada canal de voz necesita y porta su señalización
  - Un sólo canal de señalización sirve para muchos canales de voz

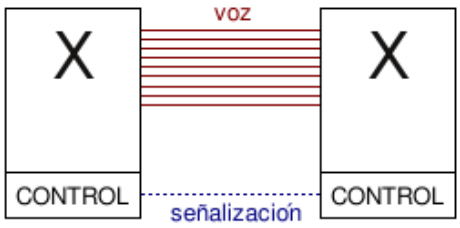

Figura 1.26: Red de Señalización: Señalización por Canal Común (CCS)

El otro método de clasificación para los sistemas de señalización diferencia en qué roles se ven implicados en la misma. Así pues, será diferente la *señalización de usuario* de la *señalización de red.*

- **Señalización de Usuario**.

  - *Analógica (CAS)*: utilizada en los bucles de abonado analógicos, es decir en RDI, Dependiendo de la tecnología empleada en la SLTU podemos encontrar:
    - Señalización Decádica, donde cada dígito se representa por un número de pulsos (apertura-cierre del bucle) consecutivos, era utilizado en los primeros terminales telefónicos.
    - Multifrecuencia (Dual Tone Multi Frequency, DTMF) donde cada dígito se representa por dos tonos simultáneos de entre 8 posibles, dentro de la banda vocal. Se utilizan dos tonos por motivos de seguridad.

- *Digital (CCS).* Como por ejemplo la señalización Q.931, formado por un canal dedicado de 16 Kbit/s de capacidad. Utilizada en RDSI y que se estudiará a fondo en el tema 2.

Actualmente coexisten los tres sistemas de señalización de usuario.

- **Señalización en la Red**. La señalización en el interior de la red es totalmente digital, mediante técnicas de CCS, lo que permite separar la señalización de la voz. Se han definido tres modos de explotación de señalización por canal común, recogidos en la figura 1.27:

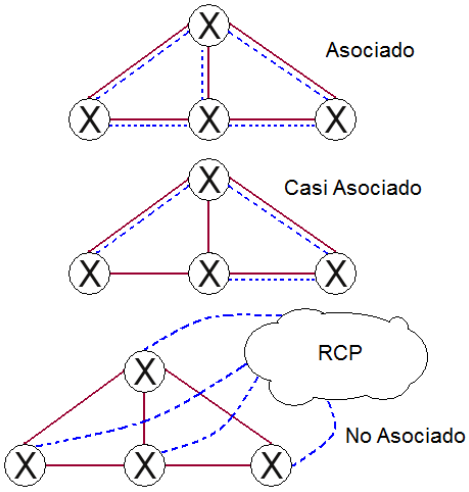

Figura 1.27: Red de Señalización: CCS en la Red

- *Modo asociado:* la red de señalización recorre los mismos caminos que la red de transmisión. Es decir, la señalización sigue el mismo flujo que los circuitos de voz, aunque por supuesto por canales independientes.
- *Modo no asociado:* existe una red de conmutación de paquetes para señalización totalmente incorrelada con el flujo de los circuitos vocales.
- *Modo casi asociado:* un modelo de explotación híbrido entre los dos anteriores. Podría considerarse un caso particular de modo no asociado.

Para finalizar este apartado, veremos un ejemplo básico de señalización, recogido en la figura 1.28. Como veremos en el tema 3, en la red de señalización se distinguen dos tipos de nodos:

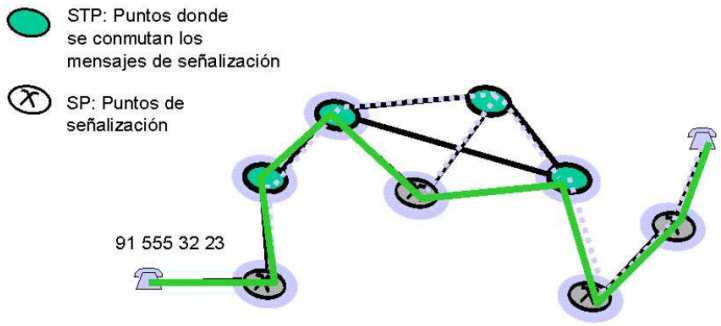

Figura 1.28: Red de Señalización: Ejemplo de Funcionamiento

- SP: puntos de señalización. Son puntos donde se generan y consumen mensajes de señalización. Haciendo una analogía básica con el mundo IP, los SP se comportarían como *hosts*.
- STP: puntos donde únicamente se conmutan los mensajes de señalización. Siguiendo la analogía con el mundo IP, se comportarían como *routers*.

En el ejemplo, se muestra como al marcar el abonado un número de teléfono, los mensajes de señalización (líneas punteadas) van recorriendo la red, reservando los recursos necesarios (círculos alrededor de las centrales) para cursar la llamada al destino. Destacamos que el modo de explotación es no asociado, o casi asociado, ya que la señalización recorre un camino distinto al circuito de la llamada.

1.2.6. Red de Gestión

Se puede definir la gestión de red, como *las labores de planificación, organización, supervisión y control de elementos de comunicaciones para garantizar un nivel de servicio, y de acuerdo a un coste.*

Históricamente la gestión de red se articula entorno a cinco áreas clásicas: *fallos, configuración, prestaciones, contabilidad y seguridad.* Aunque también es común englobar las funciones de gestión de red en otra clasificación de más alto nivel:

1. **Nivel de Negocio.** Consiste en la gestión de la red como negocio. Incluye por tanto aspectos tales como ventas, facturación, asistencia al cliente, control de inventario o planificación de inversiones.
2. **Nivel de Servicio.** Consiste en la gestión de los servicios provistos a los clientes, incluyendo los servicios básicos (telefonía) y los servicios de valor añadido.

3. **Nivel de Red.** Trata aspectos como la optimización de rutas, gestión del tráfico, planes de contingencia, planificación de cambios, planificación de extensiones, ...

4. **Nivel de Elementos de Red.** Incluyendo la instalación de equipos, diagnóstico de problemas, gestión del mantenimiento, reparaciones y alteraciones.

En todas estas actividades es muy común el uso de herramientas informáticas y manejo de grandes cantidades de datos, que permitan realizar simulaciones, predicciones, etc.

Mantener una eficiente red de gestión es fundamental de cara a ahorrar costes y ofrecer una buena calidad de servicio.

En redes complejas interactuan muchos sistemas propietarios diferentes, con lo cual se hace necesario el uso de interfaces estándar para poder realizar una gestión de red efectiva. La cooperación internacional en la definición de estándares ha resultado en un conjunto de estándares de sistemas abiertos para estos propósitos.

1.2.7. Red Inteligente

En la era de la conmutación electromecánica, la introducción de nuevos servicios necesitaba del diseño de un nuevo hardware y por supuesto aplicar modificaciones físicas a todas las centrales de la red.

Este procedimiento era altamente costoso e intrusivo para la red. Cuando se propuso la introducción de los sistemas de conmutación electrónica (ó computerizada SPC), parecía que el despliegue de nuevos servicios únicamente requeriría de pequeñas modificaciones en los programas de conmutación y que este proceso sería barato y rápido de implementar.

La práctica demostró sin embargo que la realización de actualizaciones software en todas las centrales interconectadas de la red es casi igual de costoso que las modificaciones hardware realizadas en la era electromecánica, con lo cual la introducción de nuevos servicios no se vio incrementada por el cambio de la tecnología de conmutación.

La solución encontrada para facilitar el despliegue de nuevos servicios consistió en separar el software que controla las funciones básicas, es decir la conmutación, del software requerido para la implementación de servicios más complejos por parte de la red.

Por lo tanto, partiendo del requisito fundamental de **no modificar la base instalada**, los servicios complejos son controlados por un procesador/programa centralizado, llamado *Punto de Control de Servicio (Service Control Point, SCP)*, remoto y común para todas las centrales.

Las redes que implementan esta arquitectura, mostrada en la figura 1.29, se denominan Redes Inteligentes.

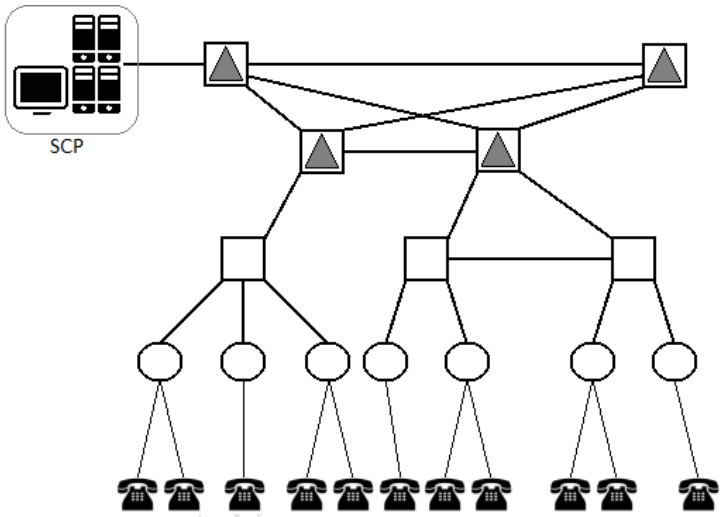

Figura 1.29: Red Inteligente

El procedimiento es sencillo. Cuando un usuario solicita un servicio avanzado que su central de abonado no es capaz de proveer, ésta realiza una consulta al SCP que le responderá a la central como proceder.

Comentar para finalizar recogemos algunos de los servicios avanzados que puede ofrecer una red inteligente:

- Cobro revertido automático (Números 900/800).
- Pago compartido (Números 901).
- Pago por el llamante sin retribución para el llamado (Números 902).
- Tarificación adicional (Servicios Premium) (Números 803/806/807).
- Llamadas masivas (Números 905).
- Encaminamiento flexible (según origen y hora).
- Distribución de llamadas.

1.3. Evolución

Hemos estudiado o introducido al menos, los distintos elementos que conforman una red de telecomunicaciones compleja como es la red telefónica conmutada. Entendiendo como tal una superposición de distintas subredes (acceso, transmisión, conmutación, sincronización, señalización, red inteligente y gestión de red), cada una con una serie de cometidos específicos que permiten la correcta explotación y el acceso de los usuarios a los distintos servicios ofrecidos.

Sin embargo, la RTC clásica ha alcanzado su límite de rendimiento **económico** y ha sido necesario evolucionar la misma hacia un nuevo modelo de funcionamiento. Para mejorar los costes y márgenes de explotación se ha generado un nuevo modelo tecnológico, donde tanto la señalización como la transmisión de conversaciones de usuario es soportada por una red de paquetes basada en IP, donde aparecen en escena nuevos elementos de gestión y un nuevo paradigma de explotación, cuya estructura se anticipa en la figura 1.30.

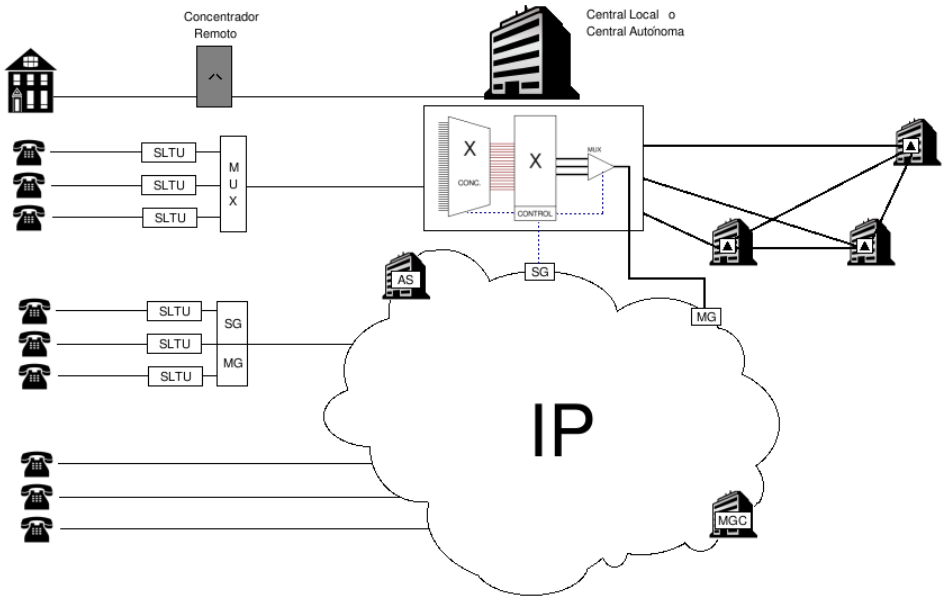

Figura 1.30: Evolución

Actualmente aún coexisten ambos modelos de explotación aunque la tendencia es a eliminar el modelo clásico y evolucionar hacia el paradigma de explotación completamente basado en IP, arquitectura comúnmente conocida como redes de nueva generación o *New Generation Networks, NGN.*

En cualquier caso, se mantiene el bucle de abonado, realizando modifi-

caciones únicamente en el SLTU donde se sustituyen los multiplexores por pasarelas, una para los medios y otra para la señalización.

La jerarquía de centrales clásica se sustituye por una red distribuida IP, donde aparecen en escena elementos como el servidor de aplicaciones (Application Server, AS) encargado de gestionar toda la señalización, las ya mencionadas pasarelas de medios (Medium Gateway, MG) y de señalización (Signaling Gateway, SG) al que se debe añadir un nuevo elemento denominado Controlador de Pasarela de Medios (Medium Gateway Controler, MGC).

El capítulo 5 de este texto está dedicado al estudio de las redes de nueva generación y por tanto de todos estos elementos y de su interfuncionamiento.

Capítulo 2

Introducción a RDSI y Q.931[1]

2.1. Introducción

La Red Digital de Servicios Integrados (RDSI) se define como *Red que procede, por evolución, de la Red Digital Integrada telefónica (RDI), que proporciona conexiones digitales extremo a extremo, que soporta una amplia gama de servicios, tanto de voz como de otros tipos y a la que los usuarios acceden a través de un conjunto limitado de interfaces normalizadas de propósito general.*

Es decir, RDSI proporciona conexiones digitales entre interfaces usuario-red.

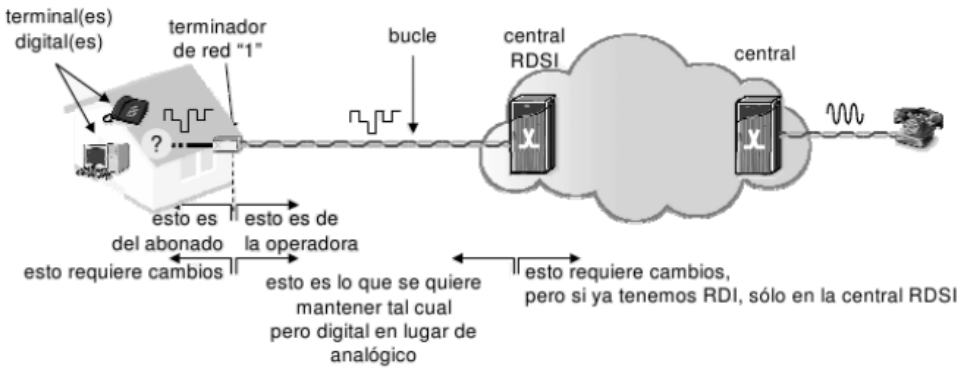

Figura 2.1: Acceso a RTC mediante RDSI

Al ser una red que proviene de la evolución de las redes ya existentes,

[1]Este capítulo está basado en los trabajos [2] y [14].

existe un principio de aprovechamiento de la planta existente, es decir, *se mantiene el bucle de abonado existente en RTC*, pero, al utilizar una banda de frecuencias 100 veces más ancha que la usada en comunicaciones vocales, se hacen necesarias ciertas modificaciones, como por ejemplo introducir canceladores de eco y algunas medidas adicionales en los pares para poder usar el cableado existente, que básicamente consistirán en cambiar a D-SLTU en el bucle de abonado. El resto de cambios necesarios para la explotación completamente digital deben realizarse en las instalaciones de los abonados.

La UIT-T (ver anexo A) ha ido recogiendo los estándares en los que se sustenta la RDSI, en su Serie I[2], ordenando dichas recomendaciones atendiendo a diferentes aspectos de la implementación de la RDSI, tal y como se recoge en la figura 2.2.

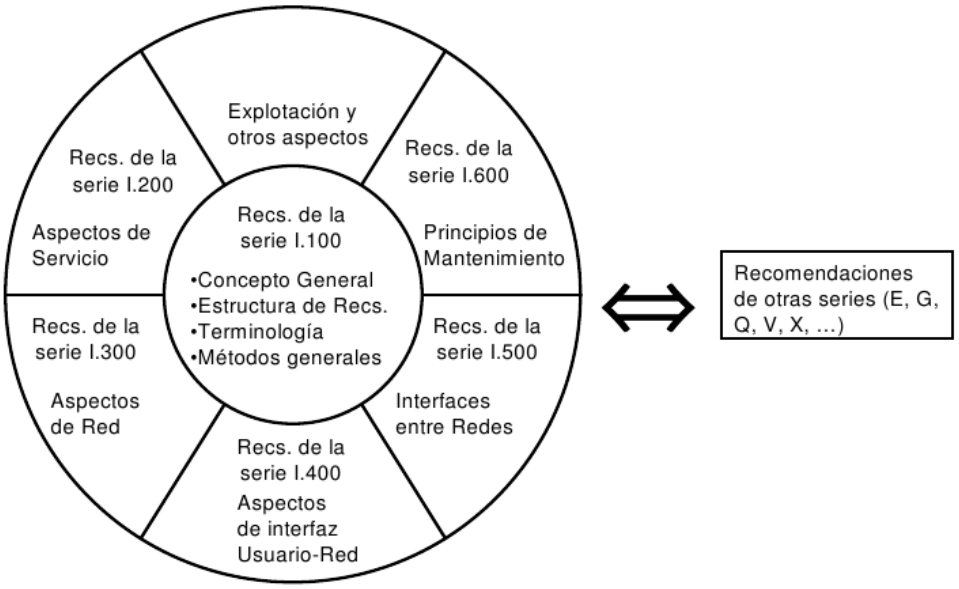

Figura 2.2: Recomendaciones Serie I de la UIT-T

- **Series I.100.** La serie 100 sirve como introducción general a la RDSI. Recoge la estructura de todas las recomendaciones de la RDSI (Serie I), ofreciendo una descripción inicial de la RDSI y su evolución estimada. Las Recomendaciones I.130 introducen la terminología y los conceptos que se usan posteriormente en la Serie I.200 para especificar los distintos servicios que soporta la RDSI.
- **Series I.200: Aspectos de Servicio**. En esta serie de recomendaciones se especifican los servicios que serán proporcionados a los usuarios,

[2] `http://www.itu.int/rec/T-REC-I/e`

algo que debemos interpretar como una serie de requisitos que la RDSI debe satisfacer. En el glosario (I.112), el término servicio se define como: *Aquello que es ofrecido por una administración o EER (Empresa de Explotación Reconocida) a sus clientes a fin de satisfacer una necesidad de telecomunicación específica.*

En RDSI el término servicio ha tomado un significado muy específico en el contexto de la UIT-T diferente de su significado habitual en el contexto OSI. Más adelante en este tema profundizaremos en estos aspectos.

- **Series I.300: Aspectos de Red.** La serie 300 se centra en como la red actúa para proveer los servicios definidos en la serie 200. Se presenta un protocolo modelo de referencia, basado en el modelo OSI, en un intento de dar cuenta de la complejidad de una conexión que puede involucrar dos o más usuarios, junto con su diálogo de señalización por canal común. Recoge también aspectos relacionados con la numeración y el encaminamiento.

- **Series I.400: Aspectos de interfaz Usuario-Red.** Dividido en tres aspectos principales:
  - *Configuración Física:* ordena cómo las funcionalidades de RDSI se implementan en equipos físicos. Se especifican los distintos Grupos Funcionales y define Puntos de Referencia entre dichos grupos.
  - *Tasas de Transmisión:* tasas binarias básicas y combinaciones de ellas que pueden ser ofrecidas a los usuarios.
  - *Especificaciones de protocolos:* protocolos de las capas 1 a 3 del modelo OSI que especifican la interacción usuario-red.
- **Series I.500: Interfaces entre Redes.** RDSI debe soportar servicios que son provistos por redes anteriores de conmutación de circuitos o de paquetes. Por lo tanto, es necesario de proveer a RDSI de capacidad para operar con estas redes, permitiendo comunicaciones entre terminales que dan el mismo servicio, ofrecido entre redes de distinto tipo. Es decir, un teléfono conectado a la RTC clásica debe poder comunicarse con un terminal RDSI. Todos estos aspectos de comunicación entre redes heterogéneas se recoge en las series 500.
- **Series I.600: Principios de Mantenimiento.** Se recogen guías de mantenimiento para línea de abonado RDSI, para la parte de red del

acceso básico RDSI, para el acceso primario y para servicios de tasas superiores.

A las recomendaciones de la Serie I hay que añadir recomendaciones sobre explotación y otros aspectos, además de recomendaciones de otras series (E ,G, Q, V, X,...).

Todos estos términos y aspectos aquí introducidos serán definidos y ampliados a lo largo del capítulo.

Recomendamos en este punto la lectura del Anexo B, que es una recopilación literal de la Recomendación I.120 (03/93). Se recomienda su lectura por un doble motivo, en primer lugar porque es el documento donde se recogen los principios básicos de la RDSI, lo cual es una excelente introducción al estudio de la misma y en segundo lugar, porque la lectura de documentación desarrollada (atendiendo a su estructura, lenguaje utilizado, ...) por un organismo internacional en el ámbito de las telecomunicaciones como la UIT-T, resulta de interés práctico para un futuro ingeniero.

2.2. Términos y Definiciones

En este apartado iremos recogiendo una serie de definiciones, conceptos y vocabulario habituales en el contexto de RDSI.

2.2.1. Canales de Acceso

Se define el canal de acceso como la *parte designada de la capacidad de transferencia de información, con características especificadas y suministrada en la interfaz usuario red.* En RDSI se definen tres tipos de canales:

- **Canal D o Canal de Datos (Data).** Su función principal es para *señalización por canal común*, aunque puede ser usado también de forma esporádica para transmisión de datos por conmutación de paquetes o tramas. Se definen dos velocidades estandarizadas para canales D, de 16 Kb/s y 64 Kb/s.
- **Canal B o Canal Portador (Bearer).** Su función principal es el transporte de datos de usuario. Dichos datos podrán ser de voz, vídeo o datos. Su tasa binaria está definida y fijada en 64 Kb/s. Se permiten tres tipos de conexiones sobre canales B, según el tipo de conmutación, ya sea de circuitos, paquetes o de tramas.
- **Canal H o Canal Portador (High Speed).** Se utilizan para transmisión de datos de usuario a velocidades superiores a las anteriores. Se ofrecen velocidades de 384 (H0), 1536 (H11) y 1920 (H12) Kb/s.

Estos canales de acceso son agrupados en una serie de estructuras de transmisión, llamadas *Interfaces de Acceso*, que se ofrecen finalmente como un paquete al usuario. Existen dos interfaces de acceso ampliamente extendidas, que expondremos a continuación.

2.2.2. Interfaces de Acceso

Podemos definir la Interfaz de Acceso como la *conexión física ente el usuario y la red que permite a aquél solicitar y obtener los servicios proporcionados por la red.*

Dicha conexión digital entre el usuario y la red será usada para portar una serie de canales de comunicaciones. La capacidad de la conexión, es decir, el número de canales soportados variará según las necesidades del usuario.

Sin embargo, se intenta mantener un número mínimo de ellos, lo que facilita la gestión por parte del proveedor del servicio, de forma que se han definido dos interfaces flexibles y adaptables y que se ajustan razonablemente al uso de la mayor parte de usuarios. Dichas interfaces son:

- **Acceso Básico o Basic Rate Access, BRA.** Definido en la I.430, está formado por 2 canales B y un necesario canal D a 16 Kb/s. Estos canales son todos dúplex y funcionan de forma independiente.

  Por tanto tenemos una velocidad de datos de usuario en línea de

  $$2 \times 64 \text{ Kb/s } + 16 \text{ Kb/s } = 144 \text{ Kb/s} \tag{2.1}$$

  A lo que hay que sumar 48 Kb/s de entramado y sincronización haciendo un total de 192 Kb/s.

  Este tipo de acceso es apropiado para usuarios individuales (instalaciones residenciales) y pequeñas oficinas.

- **Acceso Primario o Primary Rate Access, PRA.** Definido en la I.431, está formado por 30 canales B y un necesario canal D a 64 Kb/s. Coincide con el primer nivel de jerarquía plesiócrona (E1 o DS1).

  Por tanto tenemos una velocidad de datos de usuario en línea de

  $$30 \times 64 \text{ Kb/s } + 64 \text{ Kb/s } = 1,984 \text{ Mb/s} \tag{2.2}$$

Nuevamente hemos de sumar relleno de entramado y sincronización, 64 Kb/s para el acceso primario, que hacen un total de 2,048 Mb/s[3].

Es decir, tenemos 30 canales de datos de usuario que comparten un único canal D de señalización para todo el conjunto.

Este tipo de accesos son convenientes en la instalación de centralitas de mayor capacidad (grandes oficinas, hoteles, ...) y era necesaria la instalación de un nuevo bucle de abonado.

Es habitual nombrar a los accesos básicos BRA y PRA como BRI y PRI respectivamente, Basic/Primary Rate Interface.

2.2.3. Grupos Funcionales y Puntos de Referencia

Para definir los requisitos para el acceso de usuarios RDSI, es fundamental una comprensión de la configuración prevista de equipos locales de usuarios y de las interfaces estándar que serán necesarias.

El primer paso consiste en agrupar las funciones que puedan existir en las instalaciones del usuario, de modo que se deduzcan de las configuraciones físicas. La UIT-T se aproxima a este enfoque definiendo:

- *Grupos Funcionales:* ciertas configuraciones de equipos físicos o combinaciones de equipamientos.
- *Puntos de Referencia:* puntos conceptuales utilizados para separar los distintos grupos funcionales..

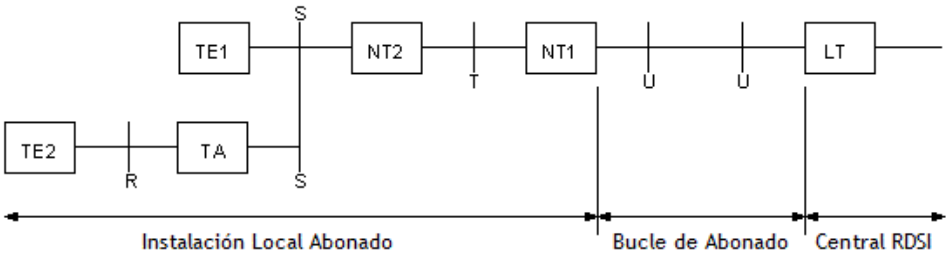

Figura 2.3: Grupos Funcionales y Puntos de Referencia

Pasamos a continuación a estudiar cada uno de estos grupos funcionales y puntos de referencia.

[3]En Estados Unidos y Japón, el bit rate final, al ser los sistemas DS1 de 23 canales de usuario, es de 1,544 Mbit/s

- **Grupo Funcional NT1, Network Termination 1.** El NT1, que puede puede ser controlado por el proveedor de la RDSI, constituye la frontera hacia la red y aisla al usuario de la tecnología de transmisión del bucle de abonado. El grupo funcional NT1 realiza funciones pertenecientes a la capa 1 del modelo OSI, es decir, funciones tales como:

  - Terminación eléctrica y física de la línea.
  - Temporización.
  - Alimentación.
  - Multiplexación de capa 1, para los canales B y D.
  - Ayuda a la resolución de contienda para el acceso al canal D.

  El NT1 realizará labores de mantenimiento de la línea, como testeo de bucle de abonado y monitorización de rendimiento. El NT1 soporta múltiples canales (por ejemplo 2B + D), siendo el flujo de bits a nivel físico multiplexado conjuntamente, utilizando multiplexión síncrona por división en el tiempo.

  El NT1 es capaz de soportar varios dispositivos conectados en configuración multipunto. Por ejemplo, una instalación residencial puede incluir un teléfono, un ordenador personal y un sistema de alarma, todo ello conectado a la misma interfaz NT1, mediante una única línea multipunto. Para este tipo de configuraciones, el NT1 incluye un algoritmo de resolución de contienda para controlar el acceso al canal D, que sera estudiado en el apartado 2.4.4.

- **Grupo Funcional NT2, Network Termination 2.** Es un dispositivo inteligente que puede incluir, dependiendo de los requerimientos, funciones pertenecientes hasta la capa 3 del modelo OSI, como por ejemplo:

  - Gestión de protocolos de las capas 2 y 3.
  - Funciones de terminación de interfaz y otras de capa 1.
  - Multiplexación en capas 2 y 3.

  Es decir, el NT2 puede realizar labores de conmutación y concentración, además de mantenimiento que caen fuera de los planos de control y usuario que estudiaremos en el siguiente apartado. Ejemplos de NT2 pueden ser una pequeña centralita digital, comúnmente denominadas PBX o PABX, una LAN o un controlador de terminales.

- **Grupo Funcional TE1, Terminal Equipment type 1.** Dispositivos terminales de usuario que soportan la interfaz RDSI estándar. Es

decir, realiza funciones de manejo de protocolos, mantenimiento, de interfaz y de conexión con otros equipos. Ejemplos de TE1 pueden ser un teléfono RDSI, terminales integrados de voz/datos o equipamiento de fax digital.

- **Grupos Funcionales TE2 y TA.** *Terminal Equipment type 2* engloba a cualquier equipamiento no RDSI que pueda ser utilizado en la RDSI, gracias al uso de un *Teminal Adaptor, TA*. La combinación de un TE2 + TA equivale a un TE1. Como ejemplos podemos citar equipos con interfaces como RS-232 u ordenadores con interfaz X.25 o ETHERNET, o sencillamente un teléfono analógico.

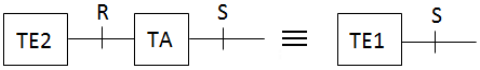

Figura 2.4: Grupos Funcionales: TE2 y TA

Las definiciones de los distintos grupos funcionales también incluyen implícitamente la definición de los denominados Puntos de Referencia.

- **Punto de Referencia T.** Se corresponde con la mínima terminación de red RDSI admisible en la instalación de usuario. Separa la instalación del usuario de la instalación de red.
- **Punto de Referencia S.** Se corresponde con las interfaces individuales de los distintos terminales RDSI. Separa los equipos terminales de usuario de las labores de comunicaciones de red.
- **Punto de Referencia R.** Es la interfaz definida entre equipos de usuario no RDSI y su equipo adaptador. Es habitual que esta interfaz cumpla con las series V o X de las recomendaciones de la UIT-T.
- **Punto de Referencia U.** Esta interfaz describe la señal de datos full duplex soportada en el bucle de abonado. Realmente, este punto de referencia no está definido en la I.411, pero es habitual recogerlo por motivos docentes. Es decisión del operador la tecnología física a utilizar.

Para finalizar este apartado es importante recoger los modos en que se agrupan estos Grupos Funcionales y Puntos de Referencia, desde un punto de vista lógico o estructural[4]:

- TE1s en Multidrop a NT1.
- Conexiones Múltiples entre TE1s y NT2.

[4]Más adelante lo estudiaremos teniendo en cuenta connotaciones físicas de las instalaciones.

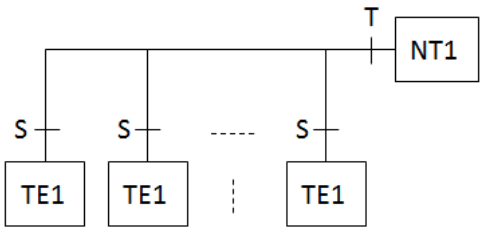

Figura 2.5: TE1s en Multidrop a NT1

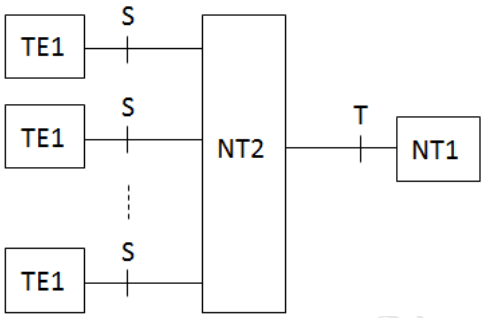

Figura 2.6: Conexiones Múltiples entre TE1s y NT2

2.2.4. Arquitectura de Protocolos

El desarrollo de estándares para RDSI incluye el desarrollo de protocolos para la interacción entre la RDSI y un usuario de la misma, así como protocolos para la interacción entre dos usuarios RDSI.

Sería deseable encajar estos nuevos protocolos RDSI dentro del modelo OSI, lo cual permitiría identificar rápidamente problemas críticos en la arquitectura, facilitando el desarrollo de los propios protocolos RDSI.

Sin embargo, el modelo OSI no es suficiente por sí solo para representar todas las necesidades que se plantean en una RDSI, En particular, una pila de 7 capas no es capaz de capturar la relación entre un protocolo de control en el canal D, usado para configurar, mantener y terminar una comunicación sobre los canales B o H.

Para acomodar este tipo de funcionalidad, la UTI-T ha desarrollado un modelo de protocolos de referencia más complejo, definido en la I.320 y mostrado en la figura 2.7.

Como vemos, encontramos definidas dos pilas de entidades de protocolos:

- **Bloque de Protocolos de Usuario**. Para la transferencia en modo transparente de la información de usuario.

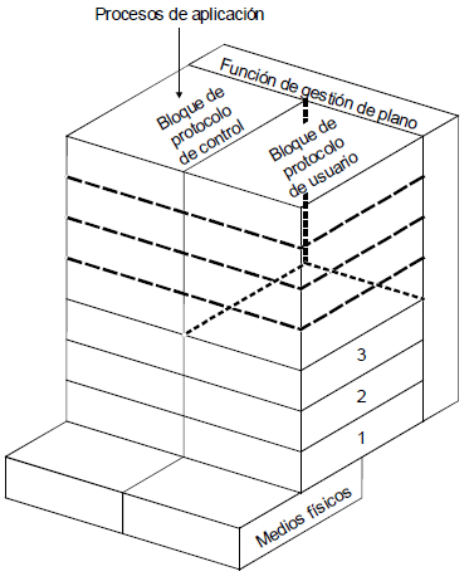

Figura 2.7: Arquitectura de Protocolos RDSI

- **Bloque de Protocolos de Control**. Para la tarea exclusiva de la señalización RDSI.

Los protocolos de usuario son los protocolos tradicionales como X.25, que son modelados completamente por el modelo OSI. Los protocolos de control realizan tareas como:

- Control de conexión a red (establecimiento y terminación).
- Control de llamadas multimedia.
- Control del uso de conexiones ya establecidas, por ejemplo, el cambio de características del servicio.
- Provisión de servicios suplementarios.

Tal y como indica la figura 2.7 el modelo de referencia de protocolo está principalmente relacionado con las capas 1 a 3 del modelo OSI (físico, enlace y red), aunque el principio de los protocolos de usuario y control en capas superiores también se muestra. Es decir, el acceso a la red involucra sólo a las capas 1 a 3, mientras que tiene poco que ver con las capas más altas 4 a 7, del modelo OSI.

Por último, el modelo de referencia de protocolo RDSI incluye un **plano de gestión**, que corta a través de todas las capas de protocolos. El termino plano, se refiere a la interacción cooperativa entre protocolos en la misma

capa en diferente sistemas. El plano de gestión incluye una variedad de funciones que permiten a los sistemas de gestión de red controlar los parámetros y el funcionamiento de los distintos sistemas.

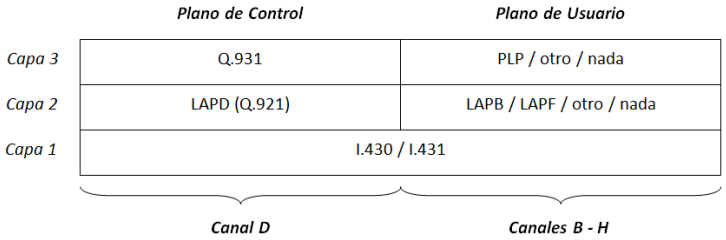

Figura 2.8: Protocolos RDSI interfaz usuario-Red

Finalizamos este apartado, recogiendo en la figura 2.8, los protocolos que aparecen en la interfaz Usuario-Red en RDSI y que serán descritos de forma precisa en próximas secciones.

2.3. Servicios en RDSI

El concepto de Servicio en RDSI se define en tres etapas. La primera etapa involucra una descripción del servicio desde el punto de vista del usuario, sin cubrir aspectos relativos a la implementación del mismo.

En esta descripción cada servicio se define en base a una serie de atributos. Un atributo representa una característica específica de un servicio. Por tanto, usando un número suficiente de atributos el servicio será perfectamente descrito o definido. Los atributos, no tienen por qué ser exclusivos de un único servicio, es decir, distintos servicios pueden tener un mismo atributo, como por ejemplo la tasa de transferencia, que es un atributo común a todos los servicios de conmutación de circuitos.

Sin embargo, el valor del atributo, la tasa de transmisión en el ejemplo anterior, sí que puede variar entre los distintos servicios. Para una mayor profundidad en el uso y descripción de servicios mediante atributos es recomendable acudir directamente a la recomendación I.140 de la UIT-T.

La segunda etapa cubre la funcionalidad requerida de la red y, por extensión, del equipamiento terminal para la correcta implementación del servicio.

La tercera y última etapa consiste en una especificación detallada de los protocolos y formatos requeridos para dicha implementación.

Los servicios en RDSI pueden ser clasificados en dos categorías:

- **Servicios Básicos.** Los servicios básicos se clasifican a su vez en Servicios Portadores y Teleservicios. Los servicios se ofrecen a los usuarios, no sólamente a través de la funcionalidad implementada por el equipamiento residente en su instalación, sino también por la capacidad funcional que ofrece la red de interconectar a los distintos usuarios mediante conexiones conmutadas. Por lo tanto, es importante caracterizar e identificar los requerimientos o tareas que debe realizar la parte de red para proporcionar dichos servicios.

  - Los *Servicios Portadores* son significativos en este contexto pues en ellos se define la capacidad de transmisión y las funcionalidades requeridas a la red. La funcionalidad que proporcionan los terminales de usuario no se incluye en los servicios portadores, sino que estos simplemente proveen la capacidad y se encargan de la transmisión de la información entre las interfaces usuario-red de la RDSI.
  - Los *Teleservicios* dotan de capacidad de servicio justo hasta su punto de uso, es decir, hasta el usuario y en consecuencia, se incluyen las funciones realizadas por los terminales de usuario. El servicio de Telefonía, fax, telex o teletex son ejemplos de Teleservicios.

  Es importante destacar, que un Teleservicio requiere del uso de un apropiado servicio portador, ya que este es el responsable final de dar el subyacente soporte de red.

- **Servicios Suplementarios.** Tal y como indica su nombre, los servicios suplementarios, suplementan/complementan/aumentan un servicio básico, añadiéndole características o capacidades adicionales. Por lo tanto, un servicio suplementario no puede ser ofrecido por sí solo y será siempre ofrecido junto con algún servicio básico al que complementar.

En la figura 2.9 se recoge un esquema con los distintos servicios ofrecidos en una RDSI y su área de influencia o responsabilidad ya comentada.

Recogemos en la tabla 2.1 los principales servicios suplementarios soportados en una RDSI.

Respecto a los servicios portadores, encontramos definidos seis tipos de servicio portador, para comunicaciones extremo a extremo:

- Conmutación de Circuitos sobre Canal B.
- Conexiones Semipermanentes sobre Canal B.

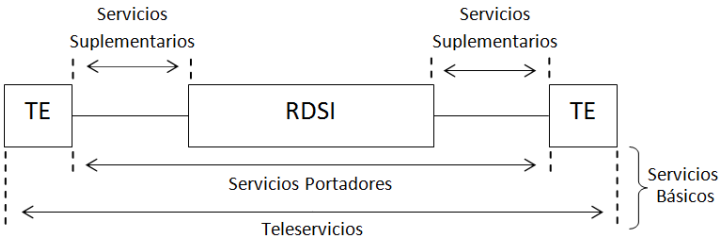

Figura 2.9: RDSI: Tipos de Servicios

DDI	Marcación Directa de Extensiones
MSN	Múltiples Números de Abonado
CLIP	Identificación de Línea Llamante
CLIR	Restricción de la Identificación de Línea Llamante
COLP	Identificación de Línea Conectada
COLR	Restricción de la Identificación de Línea Conectada
MCID	Identificación de Llamada Maliciosa
SUB	Subdireccionamiento
ECT	Transferencia de Llamada
CFB	Reenvío por Ocupado
CFNR	Reenvío por Ausencia
CFU	Reenvío Incondicional
CD	Desvío de Llamada
LH	Búsqueda de Línea
CW	Indicación de llamada en Espera
HOLD	Retención y Recuperación de Llamadas
CCBS	Llamada Completada Sobre Abonado Ocupado
3TPY	Conferencia a Tres
CUG	Grupo Cerrado de Usuarios
AOC	Información de Tarificación
UUS	Señalización Usuario-Usuario
CRED	Llamada a Crédito
RC	Cobro Revertido

Tabla 2.1: RDSI: Servicios Suplementarios

- Conmutación de Paquetes sobre Canal B.
- Conmutación de Paquetes sobre Canal D.
- Retransmisión de Tramas (Frame Relay) sobre Canal B.
- Retransmisión de Tramas (Frame Relay) sobre Canal D.

De todos estos servicios,estudiaremos únicamente el primero de ellos, de **Conmutación de Circuitos sobre Canal B.** La configuración de red y protocolos para realizar conmutación de circuitos involucra a los canales B y D. El canal B se utiliza para el intercambio transparente de datos de usuario. Los usuarios pueden utilizar cualquier protocolo que deseen para su comunicación punto a punto.

El canal D se utiliza para el intercambio de información de control entre el usuario y la red, para el establecimiento de llamada, terminación de llamada y acceso a recursos de la red.

La figura 2.10 representa la torre de protocolos para implementar la conmutación de circuitos sobre canal B.

El canal B es mantenido por un NT1 (o NT2), utilizando únicamente funciones de capa 1. Los usuarios finales pueden usar cómo hemos dicho cualquier protocolo, aunque generalmente sin llegar a la capa 3.

En el canal D, se implementa una torre de protocolos de hasta nivel 3. Finamente, el proceso de establecimiento de un circuito a través de la RDSI involucra la cooperación de conmutadores internos de la red, para configurar la conexión. Dicha cooperación se realiza mediante el *Sistema de Señalización Nº 7* (Signaling System SS#7), al que dedicamos el tema 3.

2.3.1. Numeración y Direccionamiento

El sistema de numeración y direccionamiento en RDSI está basado en el Plan de Numeración E.164, tal y como se recoge en la recomendación I.330, cumpliendo una doble función. La primera, como es lógico es lograr el encaminamiento de la llamada, mientras que la segunda es de soporte a la tarificación, es decir, el usuario sabe el tipo de tarificación que se le aplicará según el número llamado (prefijo local, nacional, servicios 90X, etc.).

La UIT-T realiza una distinción entre número y dirección. Un **Número RDSI** es uno que únicamente tiene sentido para la red RDSI y su plan de numeración. Contiene por sí sólo información suficiente para que la red

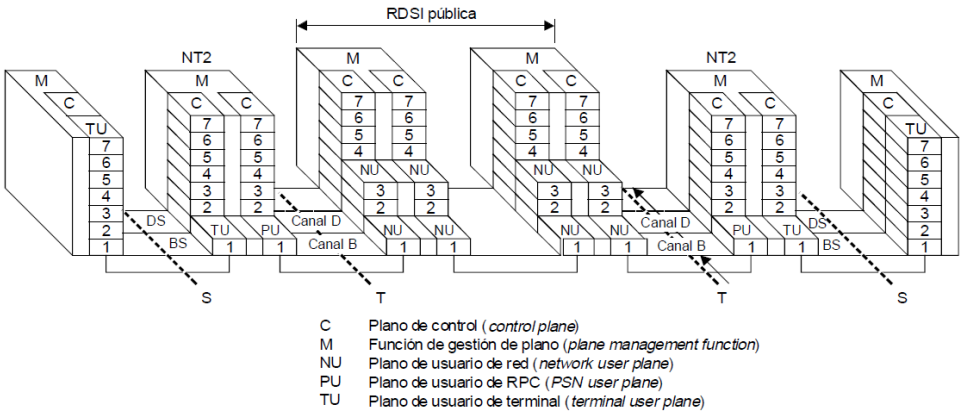

Figura 2.10: RDSI: Conmutación de Circuitos sobre Canal B

pueda encaminar la llamada. Normalmente, aunque no siempre, un número RDSI se corresponde con el punto de suscripción del usuario a la RDSI, es decir, con el punto de referencia T, y en consecuencia, asociado a un canal D.

Por otro lado, una **Dirección RDSI** comprende el número RDSI y una información adicional de direccionamiento, que puede ser obligatoria u optativa, según el caso. Esta información adicional no es necesaria para que la RDSI encamine la llamada, como hemos dicho a la red le basta con el número RDSI, pero puede ser necesaria en la instalación del abonado llamado, para distribuir la llamada internamente de forma apropiada.

Es habitual, aunque no siempre, que una dirección RDSI se corresponda con un equipo terminal específico, es decir, con un punto de referencia S.

La figura 2.11 muestra el formato completo de una dirección RDSI. Este formato de dirección aparece en los mensajes de SETUP de los protocolos de señalizacón por canal común, como SS7 que se estudiará más adelante.

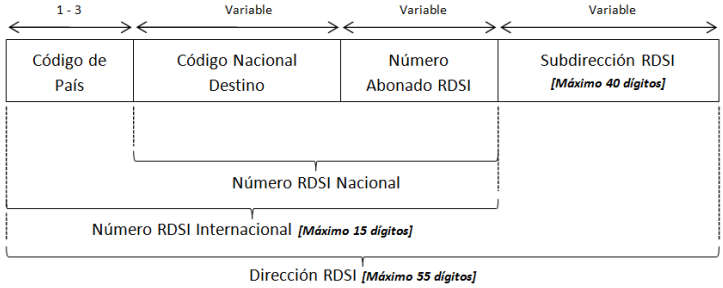

Figura 2.11: Dirección RDSI

Los elementos de una dirección RDSI son:

- **Código de País:** Especifica el país destino, o área geográfica, de la llamada. Se compone de un número variable de dígitos decimales (entre 1 y 3) y están definidos en la Recomendación E.164, junto con el plan de numeración de telefonía ya existente. El código de país para España es 34.
- **Código Nacional Destino:** de longitud variable, forma parte del número nacional RDSI. Si los abonados en un país, reciben servicio de más de un proveedor o red telefónica conmutada, puede ser usado para elegir la red de destino dentro del país. También se puede utilizar como un código de significado geográfico, para encaminar una llamada en la red hacia una zona específica de la misma. Evidentemente, también puede cumplir simultáneamente las dos funciones comentadas.
- **Número de Abonado RDSI:** también de longitud variable, constituye el resto del número nacional RDSI. Normalmente, el número de abonado es el número a marcar para alcanzar a usuarios en la misma red local o área de numeración.
- **Subdirección RDSI:** provee información adicional de direccionamiento y con un máximo de 40 dígitos. La subdirección, tal y como hemos comentado, no se considera parte del plan de numeración, pero constituye una parte intrínseca de las capacidades de direccionamiento existentes en RDSI.

El código nacional destino junto con el número de abonado RDSI forman el número nacional RDSI. Si a éste le sumamos el código de país tenemos el número internacional RDSI, que tiene un máximo de 15 dígitos[5]. La subidrección RDSI se añade al código internacional, formando la Dirección RDSI completa, con un máximo de 55 dígitos.

2.4. Nivel Físico

El nivel físico en RDSI se presenta al usuario en sendos puntos de referencia S o T. En ambos casos se incluyen la siguientes funciones, todas ellas correspondientes al nivel 1 del modelo OSI:

- Codificación de datos digitales para transmisión a través de la interfaz.
- Transmisión de datos Full-Duplex por canal B.
- Transmisión de datos Full-Duplex por canal D.

[5]La UIT-T está considerando aumentar a 16 o 17 dígitos

- Multiplexación de canales para formar la estructura de transmisión de Acceso Básico o Primario.
- Activación y desactivación del circuito físico.
- Alimentación de equipos desde la terminación de red.
- Identificación de terminales.
- Aislamiento de terminación defectuosa.
- Control de Acceso por Contienda al Canal D.

Estudiaremos a continuación los conectores y señales utilizadas en la capa física RDSI, las distintas configuraciones de cableado posibles en la instalación del abonado y terminaremos el estudio de este apartado viendo aspectos relacionados con la codificación de línea.

2.4.1. Conectores y Señales

La conexión física entre el equipo terminal (TE) y el terminador de red (NT), ya sea un punto de referencia S o T, no se especifica en ninguna recomendación de la UIT-T, sino que se utiliza un estándar ISO, concretamente el ISO 8877. Este estándar especifica un conector físico de 8 pines, cuya configuración y aspecto se muestra en la figura 2.12.

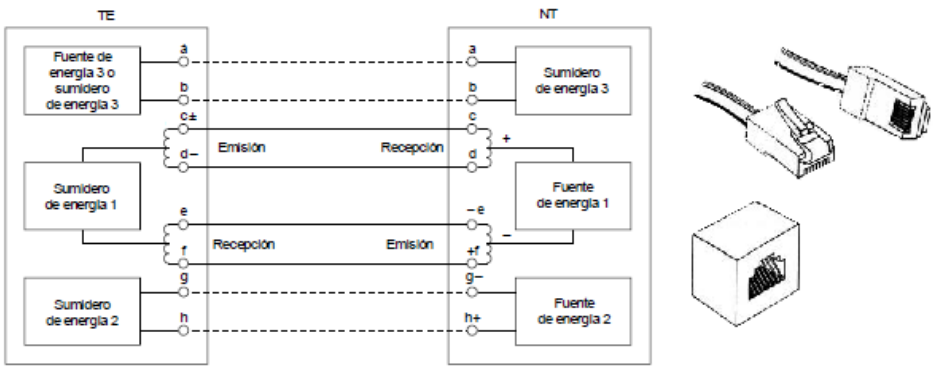

Figura 2.12: Configuración de Referencia para Transmisión de Señal y Alimentación en Operación Normal

Es importante destacar la diferente asignación de pines para el caso del TE y del NT. Se necesitan dos pines para una transmisión balanceada en cada dirección (transmisión y recepción). Estos pines se utilizan para conectar pares trenzados, provenientes del TE o del NT.

La Recomendación recoge también la capacidad para transmitir potencia a través del interfaz. Normalmente el NT utiliza uno de las dos fuentes para alimentar a los equipos terminales por circuito fantasma, tanto en condiciones de funcionamiento normal como en condiciones de restricción por fallo en la alimentación local.

Por lo tanto, la interfaz física RDSI utiliza finalmente 6 hilos de los 8 disponibles.

El medio físico está formado por pares metálicos trenzados, de dos a cuatro. Tienen una impedancia característica de 75 Ω 96 KHz, utilizando en la instalación una topología en bus, formado por un segmento de cable terminado en sus dos extremos por resistencias terminadoras de 100 Ω.

En el **acceso básico**, los equipos terminales se conectan al bus mediante segmentos no superiores a los 10 metros y terminados por conectores idénticos en ambos extremos.

Como se muestra en la figura 2.13 las posibles colisiones o contiendas no se detectan de forma directa, pues como vemos, *los terminales no se escuchan entre ellos*. Es físicamente imposible que los terminales se escuchen directamente pues ambos transmiten únicamente al NT1 o NT2, siendo este equipo el encargado de ayudar a solucionar la contienda, que se resolverán como veremos en el apartado 2.4.4.

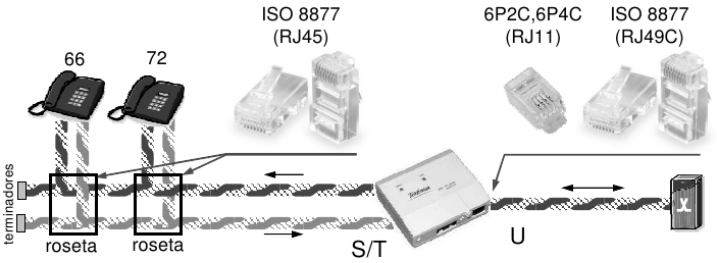

Figura 2.13: Acceso Básico: Conector y Medio Físico

En el acceso básico se utilizan por tanto 4 hilos retorcidos 2 a 2, un par en cada sentido de la transmisión, con la opción ya comentada de telealimentar los equipos terminales utilizando otro par de los disponibles.

El bucle de abonado se mantiene exactamente igual que en RDI, utilizando únicamente dos hilos retorcidos.

Respecto al **acceso primario**, cuya configuración de conexionado físico se recoge en la figura 2.14, únicamente se permite la interfaz S/T con cone-

xión punto a punto[6], con o sin conector (BNC, EN 60603-7/ISO 10173) y que por lo tanto, es posible utilizar un cable de pares retorcidos (apantallados o no) o cables coaxiales (un par o coaxial en cada sentido).

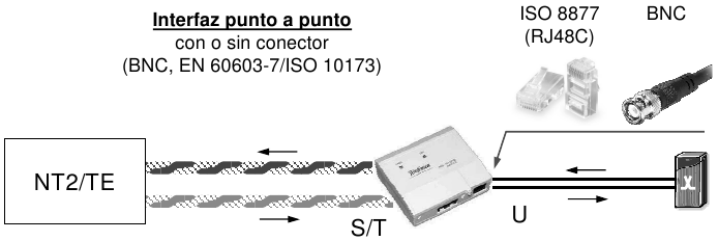

Figura 2.14: Acceso Primario: Conector y Medio Físico

Por su parte, históricamente el bucle de abonado tradicional era incapaz de soportar un acceso primario, con lo cual era necesario modificarlo susituyéndolo bien por dos coaxiales o o bien por cables de pares apantallados, en una configuración de 4 hilos con pantalla. El conector por tanto, dependería del tipo de configuración utilizada.

Con la evolución de la tecnología y mejoras de la electrónica, actualmente es posible soportar un acceso primario con el bucle de abonado tradicional. Incluso se permiten accesos a muchas mayores velocidades con el bucle de abonado tradicional utilizando la familia de tecnologías DSL, que se estudiarán en el capítulo 6 del texto.

A continuación estudiaremos las diferentes configuraciones de cableado que se utilizan en el acceso al bus.

2.4.2. Configuraciones de Cableado

Existen varias configuraciones definidas, y todas ellas se ven afectadas por una serie de limitaciones físicas a la hora de realizar la instalación. Las principales limitaciones son el tiempo de propagación y la atenuación del cable[7].

- **Punto a Punto**. La configuración más sencilla posible, donde únicamente tenemos un ET conectado al NT. La limitación en este caso, para la distancia máxima de 1000 metros viene dada por el tiempo de propagación.

[6]Si hay NT2 entonces S y T pueden ser de distinta tasa (BRA o PRA). Si no hay NT2, S, T y U deben ser de la misma

[7]En los siguientes gráficos, los TR representan la resistencias de terminación.

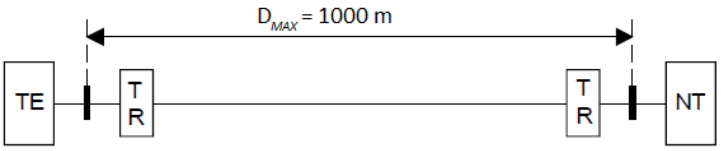

Figura 2.15: Configuración Punto a Punto

- **Bus Pasivo Corto**. Se permiten hasta 8 ETs conectados al NT. En este caso, la limitación fundamental aparece por el tempo de propagación.

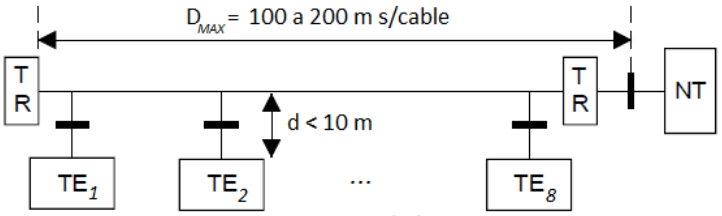

Figura 2.16: Configuración Bus Pasivo Corto

- **Bus Pasivo Largo**. Se puede tener un número indeterminado de terminales, siempre que dicho número sea inferior a 8, permitiendo aumentar la longitud del bus a cambio de tener todos los terminales reunidos en un extremo del bus.

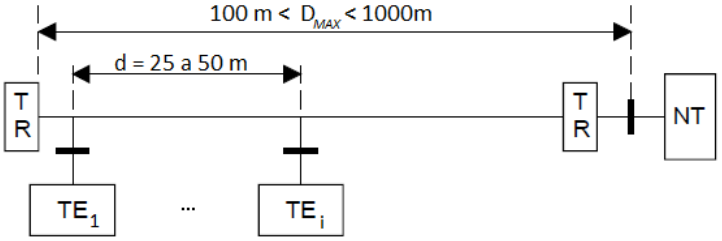

Figura 2.17: Configuración Bus Pasivo Largo

2.4.3. Codificación y Entramado

Para entender el intercambio de datos existente entre el NT y los distintos TEs es necesario considerar dos aspectos:

1. *Codificación (Coding)*: es decir, el modo en que un dato binario es representado como señal eléctrica en el bus. Se utiliza un código pseudoternario en el que el '1' binario se codifica como ausencia de señal (voltaje nulo) mientras que el '0' binario se codifica con un valor positivo o negativo alternante.

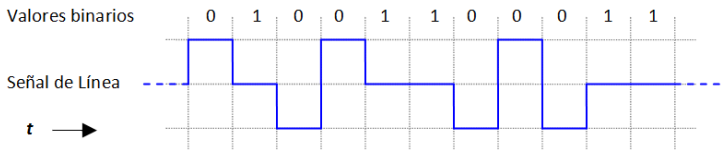

Figura 2.18: Código Pseudoternario

Esta alternancia facilita la sincronización y el equilibrado DC (disminución del nivel de continua).

2. *Entramado (Framing)*: que especifica el modo en que la información binaria es organizada y agrupada en distintas tramas. Los datos intercambiados entre el NT y los TEs se organiza en grupos de bits llamados tramas. Aparte de la tasa binaria disponible para el usuario de 144 Kb/s para el acceso básico RDSI, se añade información adicional a intercambiar entre el NT y los TEs para realizar ciertas tareas de gestión.

   Funciones como mantener un número par de '0's binarios para lograr el equilibrado de continua y evitar también el envío de '0's de la misma polaridad por los terminales.

   Para llevar a cabo todas estas funcionalidades la tasa binaria en el punto de referencia S se mantiene a 192 Kb/s. Una trama se compone de 48 bits, que se transmiten en 250 μs. Por lo tanto, 4000 tramas se transmiten en un segundo en cada sentido.

   La estructura de tramas para transmisión y recepción se muestra en la figura 2.19.

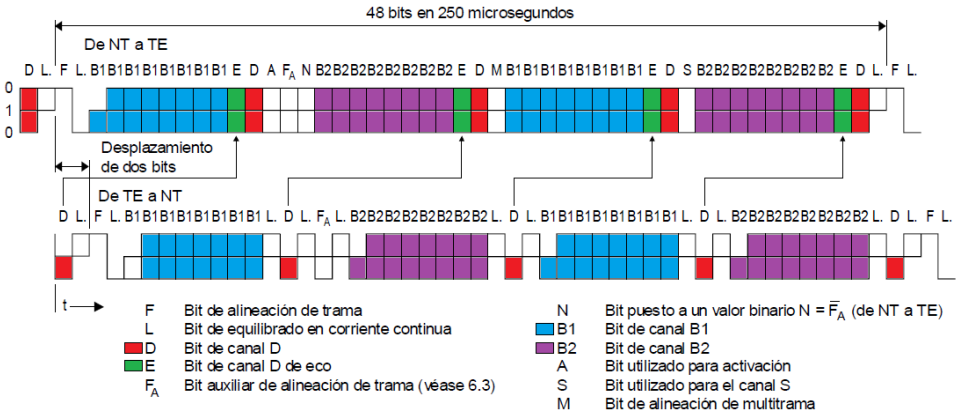

Figura 2.19: Estructura de Trama Acceso Básico RDSI

Es importante destacar que existen ciertas diferencias en las tramas transmitidas en cada dirección. No obstante, comentaremos en primer lugar los aspectos comunes.

Se transmiten 16 bits del canal B1 por trama. Al transmitir 4000 tramas/s, se logra un canal B1 de 64 Kb/s, y lo mismo se aplica al canal B2. Para el canal D, sin embargo se transmiten 4 bits por trama, que darán un total de 16 Kb/s.

Un requisito fundamental para el entramado es la delimitación de inicio y final de trama, es decir, saber cuando termina una trama y empieza otra. Esto se logra introduciendo una violación de código al principio de cada trama.

Entendemos por violación de código un incumplimiento en la alternancia de polaridad para los '0's binarios. un bit de entramado F de valor lógico '0' que incumpla la alternancia de polaridad indicará el comienzo de una nueva trama.

Por tanto, si el último '0' lógico en la anterior trama era un pulso alto, el bit F será un pulso alto. Para evitar la presencia del nivel de continua (DC) en la línea, producido por el bit F, se introduce un bit de balanceo L, inmediatamente después del bit F y de polaridad inversa al mismo.

Para asegurar que un error de transmisión (que puede resultar en una violación de código) no se confunde con el comienzo de una trama, se introduce una segunda violación de código en el primer '0' lógico encontrado en el canal B1 o en el canal D. Si, sin embargo, ocurriera que tanto el canal B1 como el D fueran todo '1', la segunda violación de código se introduce en el bit F_A, llamado bit auxiliar de entramado.

El bit F_A aparece en la decimocuarta posición, en ambas tramas. Por tanto, en el peor de los casos, se detecta un comienzo de trama en el decimocuarto bit recibido.

Para finalizar el apartado, veamos las diferencias existentes entre ambas tramas.

En el sentido NT hacia el TE, el bit de balanceo L se envía como el último bit de la trama. En el sentido contrario, del TE hacia el NT,

por contra, el balanceo se realiza justo detrás de cada octeto de canal B y cada bit de canal D.

Encontramos además 5 bits en el formato de trama en el sentido NT hacia TE. Son los bits N,A,M,E y S. El bit N, que va inmediatamente seguido al bit F_A se fija al valor del bit F_A. El bit A se usa para la activación de los terminales, el bit M para el multientramado mientras que el bit E, bit de ECO, se utilizar para resolver el acceso al canal D como veremos a continuación. El bit S no tiene un uso definido (future purposes).

Los equipos terminales determinan el comienzo de cada trama recibida del NT detectando las violaciones del código de línea que son literalmente introducidos en las tramas, tal y como hemos explicado un par de párrafos antes. El alineamiento de trama se presupone que ocurre cuando tres pares consecutivos de violaciones de código de línea son detectadas y las dos violaciones en cada par no están espaciadas por más de 14 bits.

Un equipo terminal asume que ha perdido el alineamiento de trama cuando han transcurrido 500 μs, que se corresponde con el período de dos tramas, sin detectar pares de violaciones de código válidas.

2.4.4. Resolución de Contienda para configuraciones en Multidrop

En la interfaz de acceso básico es posible disponer de más e un dispositivo terminal conectados en configuraciones de bus pasivo, tal y como hemos visto anteriormente reflejado en las figuras 2.16 y 2.17.

Los **mecanismos de resolución de contienda** son necesarios cuando encontramos varios equipos terminales compartiendo la misma línea física, es decir, conectados a la misma interfaz S/T.

Encontramos tres tipos de tráfico a considerar:

- **Tráfico en Canal B:** no requiere funcionalidad extra para controlar el acceso al canal B, pues en cada instante de tiempo cada canal estará asignado a un dispositivo terminal específico.
- **Tráfico Entrante en Canal D:** el canal D está disponible para ser usado por todos los dispositivos, tanto para señalización como para datos, por lo que existe un riesgo potencial de contienda. El esquema

de direccionamiento de LAPD que estudiaremos más adelante es suficiente para resolver la contienda del tráfico entrante, pues cada trama incluirá de manera explícita un campo de dirección destino que identifica al equipo terminal específico al que va dirigida la trama, denominado *Terminal Equipment Identifier, TEI*. Así, todos los dispositivos conectados al bus leerán la trama y posteriormente determinarán si la trama era destinada para ellos.

- **Tráfico Saliente en Canal D:** el acceso en escritura al canal D debe ser regulado de manera que únicamente un dispositivo terminal pueda hacer uso del canal D en un instante de tiempo determinado. Los mecanismos de resolución de contienda se aplican por tanto a este tráfico de datos específico.

El algoritmo de resolución de contienda regula la transmisión sobre el canal D, de manera que la información de señalización tiene prioridad (prioridad clase 1) sobre otros tipos de información (prioridad clase 2). El algoritmo de resolución de contienda de acceso al canal D utiliza los siguientes elementos:

1. Cuando un dispositivo no tiene tramas LAPD que transmitir, transmite un conjunto de unos binarios al canal D. Usando el sistema de codificación pseudoternaria, se corresponde con ausencia de señal en la línea.

2. El NT como respuesta al bit de canal D, refleja de vuelta el valor binario recibido en el canal D en el canal de Eco o bit de Eco del entramado de nivel físico, como representa la figura 2.20.

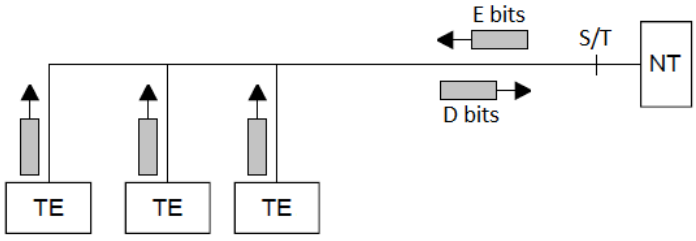

Figura 2.20: Resolución de contienda: Bit de Eco

3. Cuando un terminal está preparado para transmitir una trama LAPD, escucha previamente el flujo de los bits de eco del canal D. Si detecta una secuencia de unos binarios de longitud igual a un cierto valor límite X_i, donde i es el indicador de clase de prioridad para la trama LAPD a transmitir, entonces la transmite. En caso contrario el terminal debe asumir que algún otro terminal está utilizando el canal D y debe esperar.

4. Puedo ocurrir que varios terminales estén monitorizando simultáneamente el canal D y ambos detecten a la vez el valor límite de unos binarios y comiencen a transmitir a la vez causando una colisión. Para recuperarse de esta situación, mientras se transmite se escucha a la vez el canal de eco, y al encontrarse discordancia el terminal cesará la tranmisión de su trama y volverá al estado de escucha.

El uso de una codificación de línea pseudoternaria asegura que un equipo transmitiendo un cero (voltaje positivo o negativo) se impondrá a cualquier dispositivo transmitiendo un uno (voltaje nulo), lo que asegura que al menos uno de los dos dispositivos logrará una transmisión satisfactoria de su trama.

El mecanismo de prioridad se basa en el valor límite X_i, donde la información de señalización tiene prioridad sobre el resto. Así, todas las estaciones comienzan con un nivel de prioridad normal que se reduce tras una transmisión. La estación permanece en la prioridad menor hasta que el resto de terminales hayan tenido oportunidad de transmitir. Ejemplos de valores límite son:

- *Información de Señalización*
  - Prioridad Normal: $X_1 = 8$
  - Prioridad Baja: $X_1 = 9$
- *Información no asociada a señalización*
  - Prioridad Normal: $X_2 = 10$
  - Prioridad Baja: $X_2 = 11$

Por tanto, cada equipo terminal mantiene dos niveles de prioridad X_1 y X_2 correspondientes a la información de señalización y al resto de información a ser transmitida en el canal D. Cada uno de estos valores se inicializa a su prioridad normal. Cuando el TE tiene información de clase i a transmitir, debe esperar a escuchar en el canal de eco una cadena de unos binarios consecutivos de longitud X_i y sólo entonces transmite su trama, disminuyendo a su vez el valor de la prioridad correspondiente.

Para volver al valor de prioridad normal, el TE escucha nuevamente el canal de eco. Cuando observa una cadena de unos binarios igual al valor de prioridad más baja (el valor más alto), vuelve a cambiar el valor del nivel de prioridad a su valor normal de prioridad.

2.4.5. Interfaz U

La Recomendación I.411 no define un punto de referencia para la línea de transmisión existente entre la instalación del abonado y la central local,

esto es, el bucle de abonado.

No obstante, la UIT-T ha publicado la Recomendación G.961, en la cual se identifica la interfaz entre el equipamiento terminador de red, NT y el bucle de abonado para el acceso básico. Esta interfaz, o punto de referencia, normalmente denominado punto de referencia U.

G.961 es una especificación parcial. En ella se especifica el uso de canceladores de eco o técnicas de multiplexación por compresión en el tiempo sobre un único par trenzado.

La estructura del acceso básico consiste en dos canales B de 64 Kb/s y un canal D de 16 Kb/s. Estos canales, que generan un tráfico de 144 Kb/s, son multiplexados sobre una interfaz a 160 Kb/s en el punto de referencia U. La diferencia de capacidad se debe, como no, a necesidades de entramado y sincronización.

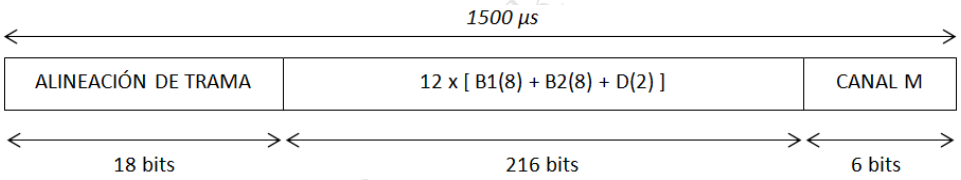

Figura 2.21: Trama Interfaz U

Como vemos el Canal M, que tiene una tasa de 4 Kb/s se utiliza para mantenimiento y otros aspectos. Podemos observar también que el entrelazado para los canales B y D es distinto del utilizado en el punto de referencia S/T. Al ser el entramado distinto pero mantener las tasas binarias se resuelve la situación mediante el empleo de pequeños buffers en transmisión. Es el NT1 el responsable de la conversión entre ambos formatos de trama.

La estructura básica de trama se organiza en **supertramas**, formadas cada una por 8 tramas. En cada supertrama tenemos por tanto 48 bits M que se usan para distintas funcionalidades, aunque la más habitual es formar un CRC de 12 bits para el control de errores.

2.4.6. Acceso Primario

El acceso primario, al igual que el básico, multiplexa múltiples canales a través de un único medio de transmisión. En el caso del acceso primario encontramos la restricción de que **únicamente se permite la configuración punto a punto.** Normalmente esta interfaz se encuentra en el punto de referencia T, junto con una centralita digital o algún otro dispositivo

concentrador, que controle múltiples equipos terminales y que provea un sistema TDM síncrono para acceder de manera conjunta a la RDSI.

Se definen dos tasas de transmisión para el acceso primario:

- **1.544 Mb/s.** Basada en la estructura de transmisión norteamericana DS1 (T1). Trama formada por 193 bits, formados por 24 intervalos de tiempo (IT) de 8 bits cada 125 μs,a los que se añade un bit de entramado. Evidentemente, cada canal tiene una capacidad de 64 Kb/s.

  Esta estructura de transmisión se utiliza habitualmente para soportar a 23 canales B y un canal D, tal y como comentamos anteriormente.

  El bit de entramado se utiliza para sincronización y otros aspectos relacionados con la gestión. La codificación utilizada para la interfaz 1.544 Mb/s es AMI[8], usando un código de línea B8ZS (Bipolar 8-Zero Substitution).

- **2.048 Mb/s.** La interfaz RDSI a 2.048 Mb/s se basa en la Estructura de Transmisión E1 de Europa (G.704), de la misma capacidad. El formato de trama se recoge en la figura 2.22.

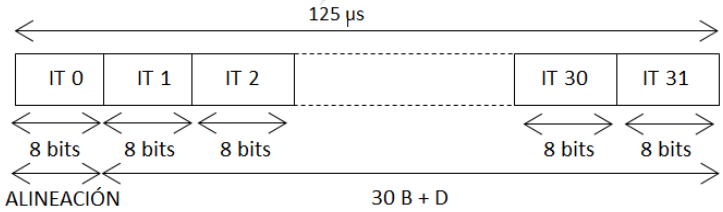

Figura 2.22: Acceso Primario 2.048 Mbps

El flujo binario se estructura en tramas repetitivas de 256 bits, donde cada trama se compone de 32 intervalos de tiempo de 8 bits. El primer intervalo de tiempo (IT0) se utiliza para labores de entramado y sincronización, mientras que los restantes 31 canales son canales de usuario.

A una tasa de 2.048 Mb/s, las tramas se repiten cada 125 μs, es decir, 8000 tramas/s. Y nuevamente, cada canal soporta por tanto 64 Kb/s. Típicamente se transportan 30 canales B y un canal D, que, de existir,

[8]AMI (Alternate Mark Inversion): Tipo de codificación que representa los '1's con impulsos de polaridad alternativa, y los '0's mediante ausencia de pulsos.

va siempre en el intervalo de tiempo 16 (IT16), aunque se permiten otras configuraciones.

El alineamiento de trama ocupa las posiciones 2 a 8 en el intervalo de tiempo 0 (IT0) de las tramas impares. Cuando se requiere una capacidad de monitorización de errores mejorada, se forma una multitrama que implementa un CRC de 4 bits.

El código de línea es AMI HDB3 (High Density Bipolar 3).

2.5. Nivel de Enlace

Por encima de la capa física, es necesario un protocolo de nivel de enlace para establecer las comunicaciones. La UIT-T ha hecho un especial énfasis en la definición del protocolo de nivel de enlace para el Canal D. Este protocolo, llamado LAPD , se usa para comunicaciones en la interfaz entre el abonado y la propia red. Todo el tráfico de canal D emplea el protocolo LAPD.

Para el Canal B, la situación es diferente, utilizándose distintos protocolos según la situación.

- Para conexiones por conmutación de paquetes, se utiliza LAPB.
- Para conmutación de circuitos, existe un enlace punto a punto entre los abonados, con lo cual, se puede utilizar el protocolo que sea necesario. No obstante, la UIT-T define un protocolo para datos en sus recomendaciones I.465/V.120, similar a LAPD.
- Para reenvío de tramas (Frame Relay) se ha desarrollado el protocolo LAPF.

Nosotros nos centraremos únicamente en el estudio del nivel de enlace para señalización en el canal D, es decir, LAPD.

2.5.1. LAPD

Todo el tráfico sobre el canal D emplea un protocolo de nivel de enlace conocido como LAPD (Link Access Protocol - D Channel), definido en Q.921.

El objetivo principal de LAPD es permitir el transporte de información entre las entidades de capa 3 usando el canal D. Requiere para su funcionamiento un canal D dúplex transparente, que en RDSI es ofrecido por el nivel físico I.430 o I.431. LAPD soporta:

- Múltiples terminales en el interfaz de usuario-red, como las vistas en las figuras 2.15 a 2.17.
- Múltiples entidades de capa 3 (como nivel 3 de X.25 o Q.931).

Características Básicas

El protocolo LAPD se modela basándose en los protocolos LAPB usado en X.25 y HDLC. Tanto la información de usuario como información de control y parámetros se transmiten en tramas, siendo LAPD un protocolo balanceado[9], es decir, ambas entidades (NT y TE) son equivalentes. Encontramos dos *tipos de operación* en LAPD:

- **Sin asentimiento:** la información de capa 3 se transmite en tramas sin numerar. La detección de errores se usa para descartar tramas erróneas, pero no existe control de errores ni control de flujo.
- **Con asentimiento (o multitrama):** la información de capa 3 se transmite en tramas que incluyen números de secuencia y que deben ser asentidas, incluyendo así métodos de control de errores y de flujo en el protocolo.

Ambos tipos de operación pueden coexistir en un mismo canal D. Además, gracias al asentimiento, es posible soportar múltiples conexiones lógicas LAPD simultáneas.

Estos tipos de operación se corresponden con los *servicios* que ofrece LAPD a los usuarios del nivel de red (capa superior).

Servicios a Usuarios de Nivel de Red

El Servicio de **Transferencia de Información Sin Asentimiento** se encarga simplemente de la transferencia de tramas que contienen datos de usuario[10] sin asentimiento, por tanto en tramas no numeradas. Este servicio no garantiza la entrega de información al otro usuario ni informa al emisor de errores en la transmisión. No existe control de flujo ni control de errores. El servicio sí soporta tanto conexiones punto a punto (envíos a un único usuario) como de difusión (envío a múltiples usuarios). Este servicio está orientado a la transferencia de datos de forma rápida y es útil para realizar procedimientos de gestión como mensajes de alarma o de difusión.

Por otro lado, LAPD implementa un servicio de **Transferencia de Información con Asentimiento**, que además es el más común y es parecido

[9] No balanceado seria un protocolo que siguiera el modelo Maestro-Esclavo.

[10] Cuidado con la notación. Usuario en este apartado es el Nivel Superior de Red RDSI, Q.931 que estudiaremos al final del tema.

al servicio ofrecido por LAPB y HDLC. Con este servicio, se establece una conexión lógica entre dos usuarios LAPD. La conexión se realiza en tres pasos: *establecimiento de la conexión, transferencia de datos y liberación de la conexión.*

En esencia, la existencia de la conexión lógica significa que LAPD en cada extremo de la conexión realizará asentimiento de tramas recibidas, permitiendo así el control de flujo y el control de errores, garantizando por tanto la entrega en el otros extremo de todas las tramas y en el mismo orden en que fueron enviadas.

Estructura de la Trama LAPD

La estructura de las tramas LAPD se recoge en la figura 2.23. Estudiaremos a continuación cada uno de los campos que la componen:

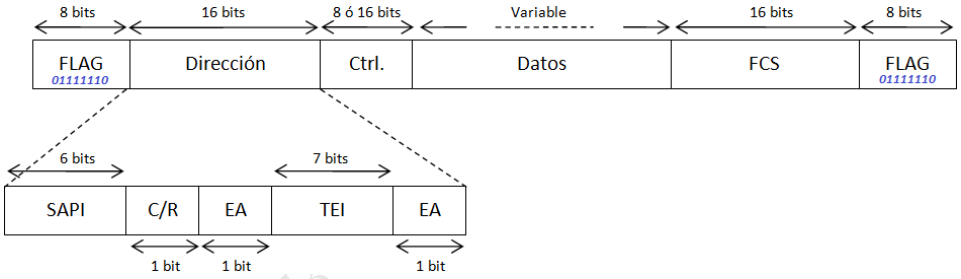

Figura 2.23: Estructura Trama LAPD

- **Flag.** Los campos bandera delimitan los extremos de la trama mediante un patrón único de 8 bits: '01111110'. Una única bandera puede ser simultáneamente delimitador de fin de trama e inicio de la siguiente. En ambos extremos de la interfaz, los receptores están continuamente inspeccionando el tráfico para capturar una bandera y sincronizarse con el inicio de la trama recibida. Este proceso de captura de bandera continua incluso durante la recepción de la trama completa para poder encontrar el final de la misma.

  El protocolo no impone restricciones en ningún caso en el contenido de la trama, por lo que, de forma aleatoria podría aparecer una secuencia de bits que coincida con el campo bandera, estropeando el alineamiento y sincronización de trama. Para evitar esta situación se utiliza una técnica de relleno de bits, conocida como *bit stuffing.*

  Entre la transmisión de las banderas de inicio y fin de trama, el transmisor siempre insertará un bit extra con valor '0' cada vez que trans-

mita cinco '1's seguidos. Así, cuando el receptor monitoriza el flujo binario (tras recibir una bandera de inicio), al recibir cinco bits a '1', examina el sexto bit. Si este bit es un '0', directamente lo elimina, pues es un bit de relleno. Si el sexto bit, es por el contrario un '1' y el séptimo bit es un '0', se acepta la condición como bandera. Si tanto el sexto como el séptimo bit están a '1', el emisor está indicando una condición de cancelación.

- **Dirección.** LAPD debe lidiar con dos niveles de multiplexación. El primero, en el lado del abonado, donde podemos encontrar múltiples dispositivos compartiendo la misma interfaz física. El segundo, dentro de cada dispositivo, donde podemos encontrar distintos tipos de tráfico, específicamente tráfico de datos (por conmutación de paquetes) y tráfico de señalización. Para acomodar estos niveles de multiplexación, LAPD emplea un tipo de dirección que consta de dos partes: un Identificador de Punto de Acceso al Servicio (SAPI) y un Identificador de Extremo Terminal (TEI).

  - *Service Access Point Identifier, SAPI.* El SAPI identifica al usuario de capa 3 y por tanto, se corresponde con una entidad de capa 3 dentro del dispositivo de usuario. Se han asignado cuatro valores, recogidos en la tabla 2.2.

SAPI	**Uso**
0	Señalización
16	Datos
32-61	Frame Relay
63	Gestión
Resto	Future Purposes

Tabla 2.2: Valores SAPI

Un valor de SAPI 0 se usa para indicar procedimientos de control de llamada para la gestión de circuitos de canal B. El valor 16 está reservado para indicar tráfico de datos e modo paquete en el canal D, usando el nivel 3 de X.25. El valor 63 se reserva para el intercambio de información de gestión de nivel 2[11]. Los valores 32 a 61 están reservados para soportar conexiones mediante Frame Relay.

  - *Terminal Endpoint Identifier, TEI.* Identificador entero codificado con 7 bits, tal que cada dispositivo conectado a bus S/T tiene asignado un único TEI. Aunque, en realidad es posible para un

[11] Un TE para solicitar un TEI enviará un mensaje al SAPI 63 con TEI 127 (difusión).

mismo dispositivo tener asignados más de un TEI, como puede ser el caso de un concentrador. La asignación de TEIs a dispositivos se produce de manera automática cuando el equipo se conecta por primera vez al interfaz, aunque puede ser asignado también manualmente por el usuario. En este último caso, el usuario es responsable de no asignar el mismo TEI a distintos dispositivos. La tabla 2.3 muestra los valores de asignación de TEIs.

TEI	**Tipo de Usuario**
0 - 63	TEs sin Asignación automática de TEI
64 - 126	TEs con Asignación automática de TEI
127	Conexión de enlace de Difusión

Tabla 2.3: Asignación de TEIs

La ventaja que ofrece este mecanismo automático es liberar a la gestión de la red del mantenimiento de una base de datos donde se relacionen los distintos equipos terminales de cada usuario.

- *Command/Response, C/R.* Todos los mensajes LAPD se categorizan como *comandos* o *respuestas*. Este bit se utiliza para indicar que tipo de mensaje contiene la trama. Si es un comando, irá a '0' si el origen es el usuario, y a '1' si el origen es la red. Para una respuesta irá a '1' si el origen es el usuario y a '0' si es la red. Una trama comando (C) será respondida inmediatamente con una trama respuesta (R).
- *Bit EA.* Bit de extensión de dirección. Es el bit menos significativo de cada octeto del campo de dirección e indica si estamos ante el último octeto del campo de dirección. Si vale '0' indica que la dirección sigue en nuevo octeto del campo de dirección, mientras que si vale '1' ese sería el último octeto. Como en LAPD siempre habrá 2 octetos para la dirección por lo que el primer bit EA será '0', y el segundo EA será '1'.

Comentar finalmente, que los valores de SAPI son únicos dentro de un TEI, es decir, para un TEI dado, existe una única entidad de capa 3 para un SAPI determinado. Por lo tanto, el TEI y el SAPI conjuntos, identifican de manera unívoca una conexión lógica. En este contexto, la combinación de SAPI + TEI se conoce como Identificador de Conexión de Enlace de Datos (Data Link Connection Identifier, DLCI).

- **Control.** LAPD define tres tipos de tramas, cada una de ellas con un formato de campo de control diferente.
  - *Tramas I (Information Transfer Frames).* únicamente portan los datos a ser transmitidos por el usuario. Adicionalmente pueden

transportar datos de control de error y flujo, usando el mecanismo Go-Back-N ARQ.

- *Tramas S (Supervisory Frames).* Para el mecanismo Automatic Repeat Request, ARQ.
- *Tramas U (Unnumbered Frames).* Se utilizan para dotar funciones de control del enlace adicionales, así como para soportar operaciones que no necesiten de asentimiento.

El primer o los dos primeros bits del campo de control sirven para identificar el tipo de trama, como recoge la tabla 2.4.

1 2	**TRAMA**	**LONG.**
0 X	I	16
1 0	S	16
1 1	U	8

Tabla 2.4: Tipos de Tramas LAPD

- **Información.** El campo de información se encuentra presente únicamente en las Tramas I y en algunas tramas no numeradas. Este campo puede contener cualquier secuencia de bits, pero debe estar formado por un número entero de octetos. La longitud del capo de información es variable, hasta un máximo definido en el sistema, de 260 octetos definido en Q.921. En este campo serán transportados los datos de usuario de LAPD, que en nuestro contexto serán los mensajes Q.931 generados por el nivel superior del plano de control.
- **Frame Check Sequence, FCS.** Es un código detector de errores, de longitud 16 bits, calculado usando el resto de bits de la trama, sin incluir las banderas. El código utilizado es el CRC-CCITT.

2.6. Nivel de Red

Para RDSI se desarrolló un nuevo protocolo de nivel de red, Q.931, que proporciona control de llamadas para los canales B y H. Este protocolo, que hace uso del canal D, trabaja al nivel de red de modelo OSI y se utiliza en comunicaciones tanto en modo circuito como en modo paquete.

Provee además de funcionalidad adicional para el control de servicios suplementarios.

Las especificaciones RDSI para el control de llamadas está recogido en seis recomendaciones:

- Q.930. Aspectos generales usuario-red de capa 3. Describe aspectos generales de las funciones y protocolos de nivel 3 del canal D empleados en las interfaces usuario-red en RDSI.

- Q.931. Control de llamadas básico. Especifica los procedimientos para el establecimiento, mantenimiento y liberación de conexiones de red en la interfaz usuario-red en RDSI.

- Q.932. Control de los servicios suplementarios. Define los procedimientos genéricos para la invocación y funcionamiento de los servicios suplementarios en asociación junto con una llamada en curso o sin llamada en curso.

- Q.933. Control de llamadas básico en modo trama. Especifica procedimientos para el establecimiento, mantenimiento y liberación de conexiones en modo trama en la interfaz usuario-red en RDSI.

- Q.939. Códigos DSS1 de identificación de servicios de telecomunicación. Provee códigos específicos para servicios de telecomunicaciones.

- Q.950. Estructura y protocolos de servicios suplementarios. Provee procedimientos detallados aplicables a servicios suplementarios individuales.

El conjunto de capacidades para proveer señalización para el control de llamada sobre el canal D se conoce como Sistema de Señalización del Abonado Digital Número 1 (Digital Subscriber Signaling System Number 1, DSS1). Su arquitectura general se muestra en la figura 2.24.

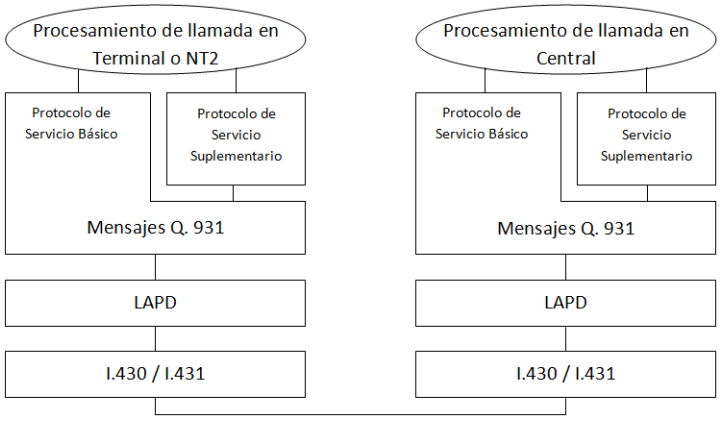

Figura 2.24: Modelado de Servicios Básicos y Suplementarios

2.6.1. Control Básico de Llamada

Q.931 especifica los procedimientos para el establecimiento de conexiones en los B y H que comparten la misma interfaz con el canal D hasta RDSI. Provee asimismo señalización de control usuario-usuario sobre el canal D. En términos OSI, Q.931 es un protocolo de nivel 3, de nivel de red.

Como indica la figura 2.25 este protocolo se basa en LAPD para transmitir mensajes en el canal D. Cada mensaje Q.931 se encapsula en una trama de nivel de enlace. La trama de nivel de enlace se transmite sobre en el canal D, que es multiplexado en la capa física junto al resto de canales, acorde a I.430 o I.431, según el tipo de acceso.

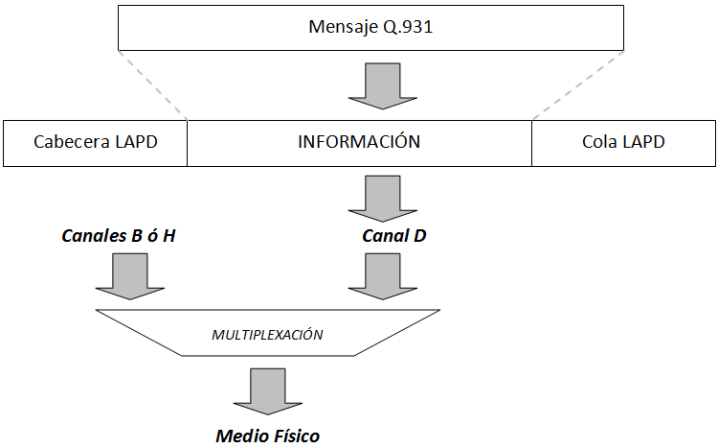

Figura 2.25: Empaquetado de Mensaje Q.931

La UIT-T especifica las siguientes funciones básicas a realizar en la capa de red para el control de llamadas:

- Interactuar con la capa de enlace (LAPD) para transmitir y recibir mensajes.
- Generación e interpretación de mensajes de capa 3.
- Administración de tiempos y entidades lógicas usadas en los procedimientos de control de llamadas.
- Administración de los canales B.
- Asegurar la consistencia entre los servicios ofrecidos a los usuarios y los requerimientos de los mismos.

Además de estas funciones básicas, otras funciones pueden ser necesarias en algunas configuraciones de red para soportar ciertos servicios. La UIT-T cita entre otros:

- *Encaminamiento y reenvío.* Para sistemas finales conectados a diferentes subredes, el encaminamiento y reenvío son imprescindibles para establecer conexiones extremo a extremo.
- *Control de Conexiones de Red.* Incluye mecanismos para proveer conexiones de red haciendo uso de conexiones de enlace de datos.
- *Transmisión de información usuario-red y red-usuario.* Esta función puede llevarse a cabo con o sin el establecimiento de una conexión por conmutación de circuitos.
- *Multiplexación de conexiones de red.* La capa 3 multiplexa información de control de múltiples llamadas sobre una sola conexión de enlace de datos.
- *Segmentación y ensamblado.* Puede ser necesario segmentar mensajes Q.931 en transmisión para luego reensamblar dichos mensajes en recepción, para poder atravesar interfaces particulares locales usuario-red.
- *Detección y recuperación de errores.* Estas labores se realizan en la capa 3.
- *Secuenciación.* Esta función proporciona mecanismos para la entrega secuenciada (en orden) de información de capa 3 cuando sea necesario.
- *Control de congestión y de flujo de datos de usuario.* El control de congestión puede decretar denegaciones temporales a peticiones de establecimiento de conexiones. El control de flujo para señalización usuario-usuario se puede ofrecer en esta capa.
- *Reinicio.* Esta función se utiliza para retornar canales e interfaces a un estado ocioso inicial, para recuperarse de situaciones de funcionamiento anormales.

Tipos de Terminales

RDSI soporta dos tipos básicos de terminales: funcionales y estímulos. Los **terminales funcionales** son considerados los dispositivos inteligentes, y pueden emplear el rango completo de mensajes Q.931, junto con sus parámetros de control. Toda la información de señalización se envía en único mensaje de control.

Los **terminales estímulos** son dispositivos con una capacidad de señalización muy básica. Los mensajes que un terminal estimulo envía a la red son normalmente generados como resultado directo de acciones realizadas por el usuario del terminal, como por ejemplo la pulsación de una tecla, y en

general, realizan poco más que notificar del evento que ha ocurrido en ellos. Por lo tanto, los terminales estímulo transmiten únicamente información de señalización de un evento o dígito en cada mensaje de señalización (envío superpuesto). Los mensajes de señalización que la red envía a los terminales estímulo contienen las instrucciones precisas relacionadas con la operación a realizar por el terminal, como por ejemplo conectar canal B o comenzar alerting. Para los terminales estímulo, las funciones de control están localizadas en la central y cualquier cambio o expansión funcional debe realizarse realizando cambios en la central.

Formato Mensajes Q.931

El proceso de establecimiento, control y terminación de una llamada, así como el proceso de selección de algún servicio suplementario, ocurre como resultado del intercambio de mensajes de señalización de control entre el usuario y la red sobre el canal D.

El formato común utilizado para todos estos mensajes definido en Q.931 se muestra en la figura 2.26.

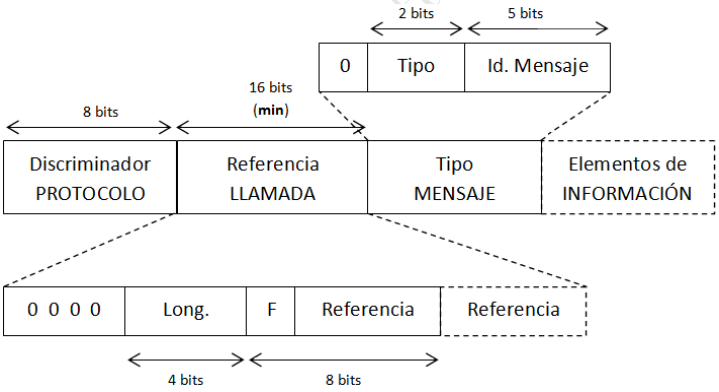

Figura 2.26: Formato mensaje Q.931

Los tres primeros campos son comunes a todos los mensajes:

- **Discriminador de Protocolo.** Se utiliza para distinguir mensajes para el control de llamada usuario-red de otros tipos de mensaje, pues como vemos según los valores que puede tomar, recogidos en la tabla 2.5, otros protocolos pueden estar compartiendo el canal D.

- **Referencia de Llamada.** Identifica la llamada sobre canal B o H a la que se refiere el mensaje, teniendo por tanto *significado local a la*

DISCRIMINADOR	PROTOCOLO
00000000 - 00000111	No utilizables
00001000	**Q.931**
00010000 - 00111111	Otros protocolos capa 3 (X.25)
01010000 - 11111110	Otros protocolos capa 3 (X.25)
01000000 - 01001111	Uso Nacional

Tabla 2.5: Valores discriminador de protocolo

interfaz en la que transcurre la llamada. Está dividido en 3 subcampos. El campo *longitud* especifica la longitud del resto del campo en número de octetos. Esta longitud es de un octeto para un acceso básico y de dos octetos para un acceso primario.

El valor de *referencia de llamada* es el número asignado a esta llamada. Identifica una conexión de manera unívoca y será el valor utilizado por los futuros mensajes (por ejemplo para un mensaje de DISCONNECT) para especificar dicha conexión. Este valor es asignado normalmente por el TE si estamos en una solicitud de conexión o bien será asignado por el NT2 o por la red directamente, si estamos anunciando una llamada entrante.

El campo bandera indica qué extremo de la conexión lógica LAPD inició la llamada: el valor '0' se utiliza si el mensaje procede del lado que originó la referencia de llamada y '1' en el caso del lado destino de la llamada. El campo bandera es necesario para evitar ambigüedades en el caso que ambos, TE y NT seleccionen simultáneamente un mismo valor de referencia de llamada.

Es posible incluso que en una misma interfaz dos terminales utilicen el mismo valor de referencia de llamada, ya que sera posible distinguirlas utilizando el TEI de cada uno de ellos.

Encontramos por último, dos valores especiales de referencia de llamada a destacar. Un valor de referencia de llamada *mudo*, cuyo campo de longitud tiene valor cero y por tanto, la referencia de llamada es un único octeto de longitud todo ceros.

El segundo caso es un valor de referencia cero, es decir, un campo de longitud con valor 1, indicando la presencia de un segundo octeto en el campo de referencia de llamada, y el valor numérico de dicha referen-

cia que es cero. Este caso es una *llamada de referencia global*, utilizada para procedimientos de reinicio del enlace de datos.

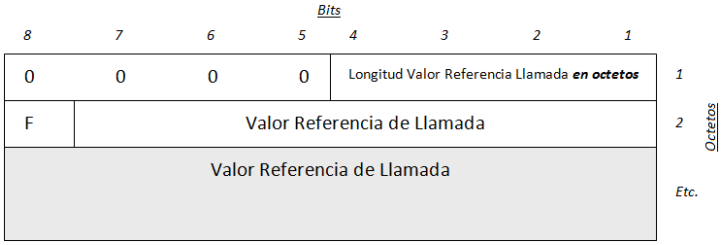

Figura 2.27: Referencia de Llamada

- **Tipo de Mensaje.** Identifica qué mensaje Q.931 o Q.932 está siendo enviado. El contenido del resto del mensaje dependerá del tipo de mensaje.

Tras estos tres campos comunes, el resto del mensaje consiste en una secuencia de cero o más **elementos de información o parámetros**. Estos parámetros contienen información adicional a ser transmitida con el mensaje.

Por tanto, el tipo de mensaje especifica si es un comando o respuesta y loa información adicional necesaria irá en los elementos de información. Algunos de estos elementos de información siempre serán incluidos en el mensaje, elementos obligatorios, mientras que otros serán opcionales.

A continuación profundizaremos en los tipos de mensajes y elementos de información que encontramos en Q.931.

Tipos de Mensaje

Los mensajes Q.931 se pueden clasificar según dos criterios independientes, uno por las aplicaciones que soportan y el otro en función de las acciones que realizan. Nosotros nos ceñiremos al segundo criterio, encontrando cuatro tipos de mensajes según la función que realizan:

- **Establecimiento de Llamada.** mensaje utilizado para establecer inicialmente una llamada. Este grupo incluye mensajes entre el terminal llamante y la red así como entre la red y el terminal llamado. Estos mensajes soportan los siguientes servicios: establecer una llamada en canal B en respuesta a petición del usuario; proveer de facilidades de red para dicha llamada e informar al usuario llamante de progreso del establecimiento de la llamada.

- **Información de Llamada.** Enviados entre el usuario y la red una vez que la llamada ya ha sido establecida, pero antes de la fase de terminación. Uno de los mensajes en este grupo permite a la red el reenvío, sin modificación, de información entre los dos usuarios de la llamada.

- **Liberación de Llamada.** Enviado entre el usuario y la red para finalizar una llamada.

- **Varios.** Pueden ser enviados entre el usuario y la red en varias etapas de la llamada. algunos pueden ser enviados durante el establecimiento y otros incluso cuando no existe llamada en curso. La función principal de estos mensajes es negociar características de la red, es decir, se usan para establecer servicios suplementarios.

La tabla 2.6 recoge los Tipos de Mensaje para Control de Conexión en Modo Circuito, los únicos que estudiaremos.

Como vemos, cada entrada incluye una indicación de la dirección del mensaje, con tres posibles opciones:

- Sólo Usuario a Red: u $\rightarrow$ r.

- Sólo Red a Usuario: r $\rightarrow$ u.

- Ambos.

Cada entrada especifica también donde tiene sentido el mensaje, es decir su significación, representada en la figura 2.28.

- *Significación Local:* el mensaje únicamente tiene sentido en alguno de los accesos (origen o destino) del usuario a la red.

- *Significación de Acceso:* relevancia en los accesos origen y destino pero no en la red, es decir, en ambas interfaces simultáneamente.

- *Significación Global:* relevancia en los acceso origen y destino así como en la red.

- *Significación Dual:* importa dentro de la red y en alguna de las interfaces (no hay ningún mensaje así definido por la ITU).

MENSAJE	SIGN.	DIR.	FUNCIÓN
			Establecimiento de Llamada
ALERTING	global	ambos	Indica que la alerta de usuario ha comenzado
CALL PROCEEDING	local	ambos	Indica que el establecimiento de llamada ha comenzado
CONNECT	global	ambos	Indica el aceptamiento de llamada por el TE llamado
CONNECT ACK	local	ambos	Indica que el usuario ha recibido la llamada
PROGRESS	global	ambos	Informa del progeso de una llamada
SETUP	global	ambos	Indica establecimiento de llamada
SETUP ACK	local	ambos	Indica que el establecimiento de llamada ha sido iniciado pero requiere de más información
			Información de Llamada
RESUME	local	u → r	Solicita reanudación de llamada previamente suspendida
RESUME ACK	local	r → u	Indica que la llamada requerida ha sido reestablecida
RESUME EJECT	local	r → u	Indica fallo en la reanudación de llamada suspendida
SUSPEND	local	u → r	Solicita suspensión de llamada
SUSPEND ACK	local	r → u	Indica que la llamada ha sido suspendida
SUSPEND REJECT	local	r → u	Indica error o suspensión de llamada requerida
			Liberación de Llamada
DISCONNECT	global	ambos	Enviado por el usuario para solicitar liberación de conexión.Enviado por la red para indicar liberación de conexión
RELEASE	local	ambos	Indica intento de liberación de canal y referencia de llamada
RELASE COMPLETE	local	ambos	Indica liberación de canal y referencia de llamada
			Varios
INFORMATION	local	ambos	Provee información adicional
NOTIFY	access	ambos	Indica información correspondiente a una llamada
STATUS	local	ambos	Enviado en respuesta a STATUS INQUIRY o en cualquier momento para informar de un error
STATUS INQUIRY	local	ambos	Solicita mensaje STATUS

Tabla 2.6: Mensajes Q.931 para Conexión en Modo Circuito

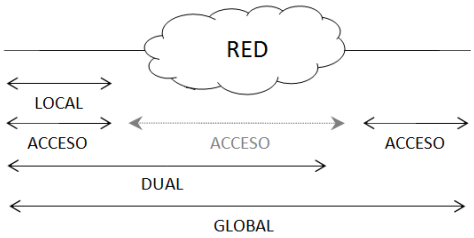

Figura 2.28: Significación mensajes Q.931

ELEMENTOS DE INFORMACIÓN		
Cambio	Indicador notificación	Número llamante
Más datos	Visualización	Subdirección llamante
Envío completo	Fecha/Hora	Número llamado
Nivel de Congestión	Facilidad Teclado	Subdirección llamada
Indicador repetición	Señal	Número redireccionamiento
Mensaje segmentado	Velocidad Información	Selección red tránsito
Capacidad portadora	Retardo extremo a extremo	Indicador de rearranque
Causa	Selec. e ind. retardo tránsito	Compatibilidad capa baja
Identidad de la llamada	Parámetros binarios N3	Compatibilidad capa alta
Estado llamada	Tamaño ventana N3	Usuario a usuario
Identificación de canal	Tamaño paquete	Escape para Ampliación
Indicador de progreso	Grupo cerrado usuarios	
Facil. específicas red	Indicación cobro revertido	

Tabla 2.7: Elementos de Información Mensajes Q.931 para Conexión en Modo Circuito

Elementos de Información

Ya sólo nos resta estudiar los elementos de información o parámetros que forman el último campo de un mensaje Q.931. A continuación recogemos en la tabla 2.7 todos los elementos de información existentes.

De todos ellos, tan sólo estudiaremos a fondo uno de ellos y definiremos los más importantes:

- *Identidad de la llamada.* Identifica una llamada suspendida. Se asigna al principio de la suspensión de la llamada.
- *Estado de la llamada.* Describe el estado actual de una llamada, como activa, separada o desconectada.
- *Número llamado/llamante.* Identifica la dirección de subred de la parta llamada o llamante.
- *Subdirección llamada/llamante.* Identifica la subdirección de la parte llamada o llamante.
- *Causa.* Describe la razón para la generación de ciertos mensajes, para proveer información de diagnóstico en el caso de errores de operación, y para indicar la localización del originador de la causa. La localización se especifica en términos de que red originó la causa.
- *Identificación de canal.* Identifica el canal/subcanal dentro de la interfaz (por ejemplo qué canal B) que es controlado por los mensajes de señalización.
- *Fecha/Hora.* Indica cuando se generó el mensaje por la red.
- *Display.* Proporciona información adicional codificada en caracteres IA5 (International Alphabet 5, qué es el mismo que ASCII). Pensado para ser mostrado en el dispositivo terminal de usuario.
- *Compatibilidad de capa alta.* Especifica el tipo de terminal o aplicación que se encuentra en la del usuario, en la interfaz S/T (por ejemplo, telefonía, teletex, sistema de manejo de mensajes X.400). La red transporta esta información de manera transparente extremo a a extremo para habilitar al usuario remoto a realizar chequeos de compatibilidad.
- *Compatibilidad de capa baja.* Usado para chequeo de compatibilidad extremo a extremo. Incluye capacidad de transferencia de información, tasa de transferencia de información e identificación de protocolos de las capas 1 a 3.

- *Facilidad de teclado.* Transporta caracteres IA5 introducidos por medio de la entrada del terminal.
- *Facilidades específicas de red.* Especifica facilidades características de una red particular.
- *Indicador de notificación.* Provee información pertinente a una llamada. Los valores actualmente definidos son: usuario suspendido, usuario reanudado y carga del servicio portador.
- *Indicador de progreso.* Describe un evento que se ha producido durante la llamada.
- *Indicador de repetición.* Indica que una posibilidad debe ser elegida entre varios elementos de información repetidos.
- *Envío completo.* Indica que el número de la parte llamada ha sido completado.
- *Señal.* Transporta información provocando a un terminal estímulo a generar tonos y señales de alerta. Algunos ejemplos son activación tono de invitación a marcar, activación tono de llamada, y tonos desactivados.
- *Selección de red de tránsito.* Identifica la red que la conexión debe usar para llegar al destino final. Este elemento de información puede ser repetido dentro de un mensaje para seleccionar una secuencia de redes a través de las cuales una llamada debe pasar.

únicamente nos resta estudiar el único elemento de información que necesita una descripción algo más detallada, que es el elemento de información **Capacidad del Servicio Portador**. Este parámetro se utiliza en los mensajes de SETUP para solicitar un servicio portador, como se especifica en I.231. A diferencia de otros elementos de información que viajan entre la fuente y el destino, este elemento es utilizado por la red en el establecimiento de la conexión. Es el único elemento de información obligatorio en el mensaje de SETUP ya que indica los recursos de red que serán necesarios para atender la llamada, por ejemplo el número llamado puede enviarse más adelante.

La estructura del elemento de información capacidad del servicio portador se muestra en la figura 2.29.

Lleva dos tipos de información:

- La selección del servicio portador, elegido entre los distintos servicios ofrecidos por la red a la que el usuario está conectado. Un ejemplo es

		8	7	6	5	4	3	2	1
Octeto	1	0	Identificador del elemento de información "Capacidad del servicio portador" (0000100)						
Octeto	2	Longitud							
Octeto	3	1	Código		Capacidad de transferencia de información				
Octeto	4	0/1	Modo de transferencia		Velocidad de transferencia de información				
Octeto	4a*	1	Multiplicador de velocidad						
Octeto	5*	0/1	Identidad de capa 1		Protocolo de capa 1 de información de usuario				
Octeto	5a*	0/1	Sínc/Asínc	Negociación	Velocidad de Usuario				
Octeto	5b*	0/1	Velocidad intermedia		NIC Tx	NIC Rx	C. flujo Tx	C. flujo Rx	Reserva (0)
Octeto	5c*	0/1	Encabez.	Multitrama	Modo	Negoc. LLI	As.(or/ado)	Neg. D/F B.	Reserva (0)
Octeto	5d*	0/1	Bits de parada		Bits de datos		Paridad		
Octeto	5e*	1	M. dúplex	Tipo de módem					
Octeto	6*	1	Identidad de Nivel 2		Protocolo de nivel 2 de información de usuario				
Octeto	7*	1	Identidad de Nivel 3		Protocolo de nivel 3 de información de usuario				

Figura 2.29: Capacidad del Servicio Portador

información digital sin restricciones. Esta información s codificada en los octetos 3 y 4 para el modo circuito y en los octetos 3, 4, (incluyendo 4a y 4b si es necesario), 6 y 7 para el modo paquete.

- Información acerca del terminal o de la llamada pretendida, que se utiliza para decidir la compatibilidad del terminal destino y posiblemente para facilitar el interfuncionamiento con otras redes RDSI o no RDSI. Un ejemplo es Codificación por Ley A. Esta información se codifica en el octeto 5 del elemento de información capacidad del servicio portador.

El octeto 3 incluye un indicador para discernir si la capacidad portadora es o no un estándar UIT-T. En caso afirmativo, el campo capacidad de transferencia de información especificará uno de los siguientes estándares: *Conversación, Información digital sin restricciones, Información digital con restricciones, Audio 3,1 KHz, Audio 7 KHz, Video.*

El octeto 4 indica si el modo de operación, modo circuito o modo paquete, así como la tasa de transferencia del canal de usuario: *64 Kb/s, 2x64 Kb/s, 384 Kbp/, 1,536 Mb/s, 1,92 Mb/s.*

En el octeto 4a, el campo estructura provee información de sincronización: *Integridad 8 KHz, Integridad Unidad Servicio de Datos, Sin estructurar.*

Actualmente, el resto de los octetos 4a y 4b únicamente soporta configuraciones extremo a extremo, demanda de establecimiento de conexión, y transferencia simétrica bidireccional. Dado que el tráfico es simétrico, la tasa de transferencia de información debe ser la misma en ambas direcciones de la conexión.

El octeto 5 se utiliza para indicar la norma de codificación seguida para la capacidad de transferencia de información, por ejemplo: tasa de adaptación V.110 o V.120, X.31 bandera de relleno, Ley A, Ley μ.

El octeto 5a incluye una indicación para indicar transferencia síncrona o asíncrona y un indicador de la negociación utilizado con V.110. La tasa de usuario muestra la tasa base con la que se produce la adaptación. El octeto 5b trata con los detalles de la técnica de adaptación de tasa elegida y toma dos formas, una con V.110 y otra con V.120.

Los octetos 5c y 5d contienen características adicionales de la capa física. El octeto 6 información sobre el uso de la capa 2 (I.441/Q.921 o capa 2 de X.25). El octeto 7 la tiene sobre la capa 3 (Q.931 o capa 3 de X.25).

2.7. Control de Conexión en Modo Circuito

En la tablas 2.8 a 2.17, quedan recogidos los elementos de información correspondientes a mensajes Q.931 para el funcionamiento en modo circuito,que son los únicos que estudiaremos. Es importante observar si son Obligatorios u Opcionales y también distinguir el sentido de los mismos.

CONNECT			
E. Información	Dirección	Tipo	Significación
Capacidad Portadora	$\Longleftrightarrow$	Optativo	Global
Identificación de canal	$\Longleftrightarrow$	Optativo	Global
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Global
Visualización	$\Longrightarrow$	Optativo	Global
Fecha/Hora	$\Longrightarrow$	Optativo	Global
Señal	$\Longrightarrow$	Optativo	Global
Compatibilidad capas bajas	$\Longleftrightarrow$	Optativo	Global
Compatibilidad capas altas	$\Longleftrightarrow$	Optativo	Global

Tabla 2.8: Elementos de Información Mensaje CONNECT en Modo Circuito

CONNECT ACKNOWLEDGE			
E. Información	Dirección	Tipo	Significación
Visualización	$\Longrightarrow$	Optativo	Local
Señal	$\Longrightarrow$	Optativo	Local

Tabla 2.9: Elementos de Información Mensaje CONNECT ACKNOWLEDGE en Modo Circuito

CALL PROCEEDING			
E. Información	Dirección	Tipo	Significación
Capacidad Portadora	$\Longleftrightarrow$	Optativo	Local
Identificación de canal	$\Longleftrightarrow$	Optativo	Local
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Local
Visualización	$\Longrightarrow$	Optativo	Local
Compatibilidad capas altas	$\Longleftrightarrow$	Optativo	Local

Tabla 2.10: Elementos de Información Mensaje CALL PROCEEDING en Modo Circuito

ALERTING			
E. Información	Dirección	Tipo	Significación
Capacidad Portadora	$\Longleftrightarrow$	Optativo	Global
Identificación de canal	$\Longleftrightarrow$	Optativo	Global
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Global
Visualización	$\Longrightarrow$	Optativo	Global
Señal	$\Longrightarrow$	Optativo	Global
Compatibilidad capas altas	$\Longleftrightarrow$	Optativo	Global

Tabla 2.11: Elementos de Información Mensaje ALERTING en Modo Circuito

PROGRESS			
E. Información	Dirección	Tipo	Significación
Capacidad Portadora	$\Longleftrightarrow$	Optativo	Global
Causa	$\Longleftrightarrow$	Optativo	Global
Indicador de Progreso	$\Longleftrightarrow$	*Obligatorio*	*Global*
Visualización	$\Longrightarrow$	Optativo	Global
Compatibilidad capas altas	$\Longleftrightarrow$	Optativo	Global

Tabla 2.12: Elementos de Información Mensaje PROGRESS en Modo Circuito

SETUP			
E. Información	Dirección	Tipo	Significación
Envío completo	$\Longleftrightarrow$	Optativo	Global
indicador de repetición	$\Longleftrightarrow$	Optativo	Global
Capacidad Portadora	$\Longleftrightarrow$	**Obligatorio**	**Global**
Identificación de canal	$\Longleftrightarrow$	Optativo	Global
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Global
Facilidad de red especifica	$\Longleftrightarrow$	Optativo	Global
Display	$\Longrightarrow$	Optativo	Global
Facilidades de Teclado	$\Longleftarrow$	Optativo	Global
Señal	$\Longrightarrow$	Optativo	Global
Número llamante	$\Longleftrightarrow$	Optativo	Global
Subdirección llamante	$\Longleftrightarrow$	Optativo	Global
Número llamado	$\Longleftrightarrow$	Optativo	Global
Subdirección llamado	$\Longleftrightarrow$	Optativo	Global
Selección red de tránsito	$\Longleftarrow$	Optativo	Global
Indicador de repetición	$\Longleftrightarrow$	Optativo	Global
Compatibilidad capas bajas	$\Longleftrightarrow$	Optativo	Global
Compatibilidad capas altas	$\Longleftrightarrow$	Optativo	Global

Tabla 2.13: Elementos de Información Mensaje SETUP en Modo Circuito

SETUP ACKNOWLEDGE			
E. Información	Dirección	Tipo	Significación
Identificación de canal	$\Longleftrightarrow$	Optativo	Local
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Local
Display	$\Longrightarrow$	Optativo	Local
Señal	$\Longrightarrow$	Optativo	Local

Tabla 2.14: Elementos de Información Mensaje SETUP ACKNOWLEDGE en Modo Circuito

DISCONNECT			
E. Información	Dirección	Tipo	Significación
Causa	$\Longleftrightarrow$	*Obligatorio*	*Global*
Indicador de Progreso	$\Longleftrightarrow$	Optativo	Global
Display	$\Longrightarrow$	Optativo	Global
Señal	$\Longrightarrow$	Optativo	Global

Tabla 2.15: Elementos de Información Mensaje DISCONNECT en Modo Circuito

RELEASE			
E. Información	Dirección	Tipo	Significación
Causa	$\Longleftrightarrow$	*Obligatorio*	*Local*
Visualización	$\Longrightarrow$	Optativo	Local
Señal	$\Longrightarrow$	Optativo	Local

Tabla 2.16: Elementos de Información Mensaje RELEASE en Modo Circuito

RELEASE COMPLETE			
E. Información	Dirección	Tipo	Significación
Causa	$\Longleftrightarrow$	*Obligatorio*	*Local*
Visualización	$\Longrightarrow$	Optativo	Local
Señal	$\Longrightarrow$	Optativo	Local

Tabla 2.17: Elementos de Información Mensaje RELEASE COMPLETE en Modo Circuito

2.7.1. Conexión en Modo Circuito en Bloque

La figura 2.30 es un ejemplo de uso del protocolo para configurar una llamada telefónica en canal B en modo circuito. Explicaremos este ejemplo paso a paso para dar una idea del uso de Q.931. El ejemplo es para el establecimiento de una llamada telefónica, pero la secuencia sería similar para una llamada entre ordenadores u otra de otro tipo.

El proceso comienza cuando en la línea llamante, el usuario descuelga el terminal. El teléfono RDSI asegura que el canal D está activo antes de generar el tono de invitación a marcar. Cuando el abonado marca el número llamado, el terminal acumula los dígitos y una vez los tiene todos, envía el mensaje de SETUP sobre el canal D a la central. El mensaje de SETUP incluye el número destino, identificador de canal, que especifica el canal B a usar y cualquier otra facilidad o servicio de red, como por ejemplo, cobro revertido.

El mensaje de SETUP dispara dos actividades en la central local. En primer lugar, la central envía mensajes de señalización a través de la red, hasta la central destino, reservando los recursos necesarios para el establecimiento del circuito para la llamada. Estos mensajes, pertenecientes al protocolo de señalización SS7, se estudiarán en el próximo tema, pero podemos aprovechar aquí para introducirlos y al menos tener constancia de su uso:

- *IAM (Initial Address Message).* Es un mensaje de establecimiento de

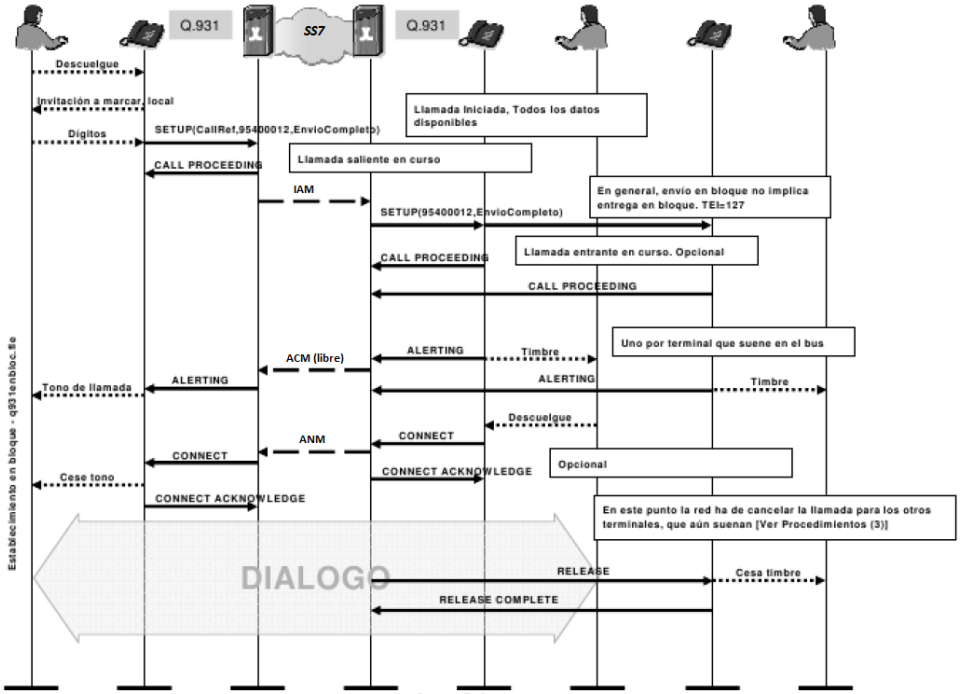

Figura 2.30: Conexión en Modo Circuito en Bloque

llamada con el número completo.

- *ACM (Address Complete Message).* Avisa al llamante de que se dispone de toda la información para cursar la llamada hacia el llamante.
- *ANM (Answer Message).* Informa al lado llamante que el lado llamado ha descolgado.

En segundo lugar, la central contesta al usuario con un mensaje de CALL PROCEEDING, indicando que el establecimiento de la llamada está en curso. La central podría también requerir más información al usuario llamante, enviándole para ello mensajes de SETUP ACKNOWLEDGE o de INFO, como ocurren en el envío solapado.

Cuando el mensaje de señalización entre centrales IAM llega a la central local del abonado llamado, ésta envía un mensaje de SETUP al teléfono llamado. Importante destacar que este mensaje de SETUP es distinto al mensaje de SETUP que se generó en el lado llamante. Es decir, **los mensajes Q.931 no viajan a través de la red**, sino que son generados y consumidos en los extremos con entidades Q.931, (TEs, NT2 y central local), disparando las acciones necesarias según el caso (generar un nuevo SETUP, un mensaje SS7, otros procedimientos, ...).

El teléfono llamado acepta la llamada, contestando a su central con un mensaje de ALERTING y opcionalmente con CALL PROCEEDING, generando el timbre de alerta para el usuario. El mensaje de ALERTING es retransmitido de vuelta atravesando todo el camino hasta el terminal llamante, que genera al recibirlo el tono de llamada, avisando así al usuario llamante, que se esta esperando la respuesta del usuario en el teléfono llamado.

Cuando el usuario llamado descuelga su terminal, éste envía un mensaje CONNECT a la red y su central le responde con un CONNECT ACKNOWLEDG a la vez que envía un mensaje ANM a la parte llamante, transportando así el CONNECT del llamado que llegará al terminal llamante. Al recibirlo, contestará a la red con un CONNECT ACKNOWLEDGE, cesando el tono de llamada y quedando así totalmente establecido el circuito sobre el canal B reservado, permitiendo el diálogo entre los usuarios.

Con el circuito establecido, flujos de datos full duplex de 64 Kb/s son intercambiados entre los usuarios por el canal B. Durante esta fase, se pueden enviar mensajes de señalización adicionales, como por ejemplo, mensajes de información de la llamada.

Dado que todo el proceso de establecimiento de llamada hace uso de señalización por canal común los otros canales no se ven afectados y el hecho de que todos los canales B estén ocupados, no impide que se produzca diálogo por el canal D. Por ejemplo, si todos los canales B estuvieran asignados a circuitos, una petición de llamada entrante sería presentada al usuario por el canal D. Así, el usuario podría si quisiera poner una llamada en curso en espera, liberando así el canal B ocupado para atender la nueva llamada entrante.

2.7.2. Conexión en Modo Circuito Solapada

En este modo, el número llamado no va en el mensaje de SETUP inicial, sino que los dígitos se van enviando en posteriores mensajes de INFORMATION. Una vez que el número llamado ha sido completamente enviado a la red, se procede enviando al usuario llamante el mensaje CONNECT ACKNOWLEDGE, y procediendo a continuación exactamente igual que en el modo en bloque, tal y como recoge el diálogo entre entidades mostrado en la figura 2.31.

En este escenario se utiliza un nuevo mensaje SS7, denominado *CPG (Call Progress)*, mensaje que indica la ocurrencia de un evento durante el establecimiento de la llamada que debería hacerse llegar a la parte llamante o la parte llamada.

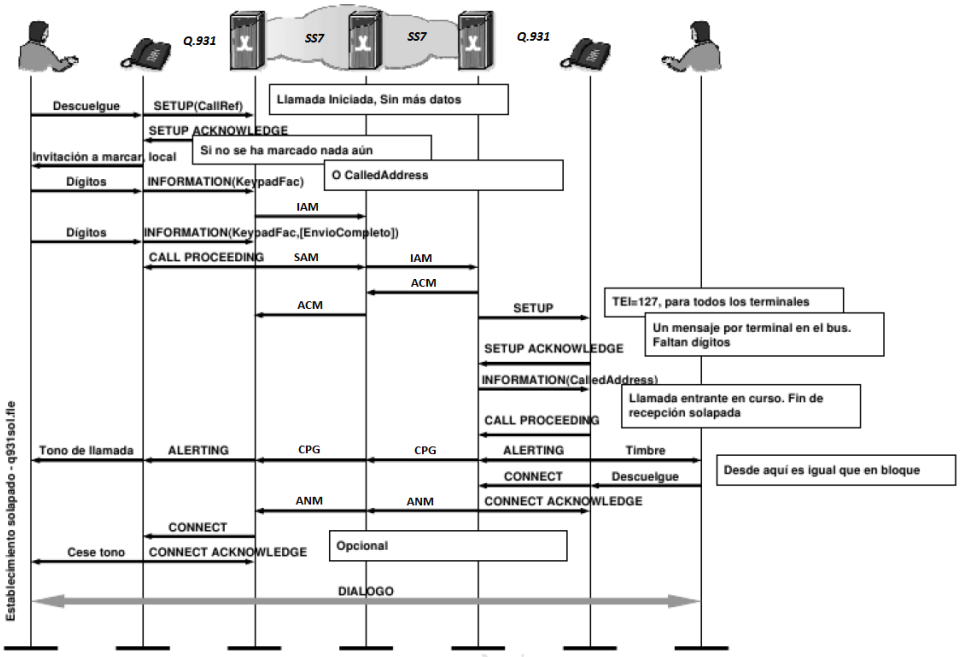

Figura 2.31: Conexión en Modo Circuito Solapada

En este ejemplo, se muestra una diferencia adicional con el caso anterior, y que consiste en que tras el SETUP ACK en la parte llamada, suponemos que faltan datos y los pedimos a la central destino, que los devuelve en una trama INFORMATION. Es importante destacar que no existe relación alguna entre realizar el SETUP en bloque o de manera solapada entre parte llamante y llamada y viceversa, es decir, el SETUP en cada extremo se puede realizar de cualquier manera.

2.7.3. Desconexión en Modo Circuito

La terminación de llamada comienza cuando uno de los usuarios cuelga su terminal. Este evento provoca el envío del mensaje DISCONNECT del terminal a la central. La central responde con un un mensaje de RELEASE, que el terminal confirma a la central con un RELEASE COMPLETE, quedando así liberado el canal B.

En la otra interfaz red terminal, ocurre una acción análoga, siendo en este caso la central la que envía el mensaje de DISCONNECT inicial al terminal.

En este escenario es necesario el uso de un mensaje SS7 denominado *REL (Release)*, que es utilizado para indicar que el circuito se libera.

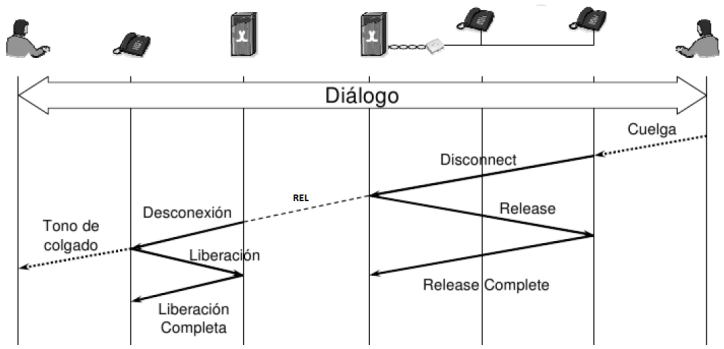

Figura 2.32: Desconexión en Modo Circuito

Capítulo 3

Sistema de Señalización por Canal Común N^{o}7 [1]

3.1. Introducción

LA UIT-T define la señalización como *el intercambio de información no vocal, específicamente dedicada al establecimiento, liberación y otros controles de las llamadas así como a la realización de labores de gestión de red.*

Es decir la señalización realiza tareas que pertenecen o podríamos englobar en los planos de control y de gestión.

La señalización se realiza entre distintas entidades, que son:

- Abonado y central.
- Central y central.
- Central y centros de gestión de red.

Podría entenderse que su función es controlar el camino (circuito) dedicado en exclusiva entre los extremos de la conexión.

Las funciones asociadas a la señalización en una red pueden catalogarse en diferentes categorías:

- *Señales de supervisión:* disponibilidad de recursos (enlaces, ...).
- *Señales de dirección:* identificación de abonados, encaminamiento de llamada, localización de abonados.
- *Señales de información de llamada:* estado de la llamada (tonos audibles).

[1] Este capítulo está basado en los trabajos [6] y [14].

- *Señales de gestión de red:* mantenimiento y operación de la red (tabla de encaminamiento, ...).

Para realizar todas éstas y otras funciones, encontramos dos técnicas o modos principales de señalización:

- **Asociada al canal (CAS).** La característica clave que distingue la señalización asociada al canal (CAS) de la señalización por canal común (CCS) es la relación determinista existente entre las señales de control de llamada y las señales portadoras (circuitos) que controlan en los sistemas CAS. En otras palabras, para cada enlace se asigna una capacidad de señalización fija y predeterminada.

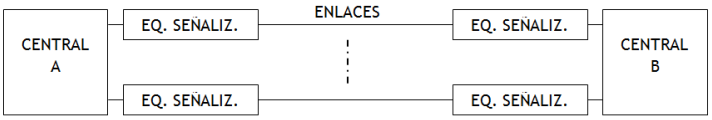

Figura 3.1: Señalización Asociada al Canal

La señalización asociada al canal, ya sea analógica o digital, presenta una serie de desventajas características:

  - *Más susceptible al fraude:* al usar señales de supervisión en banda audible, los sistemas CAS son extremadamente sensibles al fraude porque el usuario puede generar estas señales usando simplemente un generador de tonos en lugar del micrófono de su terminal telefónico. Este tipo de dispositivos se conoce como Blue Box[2]. Al principio de los años 70 podía ser adquirido como un pequeño pad, evolucionando en los años 80, incorporándose en PCs mediante software.
  - *Repertorio limitado de señales:* la capacidad de señalización de los sistemas CAS es limitada ya que la cantidad de información que puede ser transmitida en banda vocal es limitada. Dado que únicamente se usa una pequeña porción de la banda vocal, los sistemas CAS no pueden alcanzar los requerimientos de las redes actuales, que requieren de una mayor ancho de banda para su correcta señalización.
  - *Desperdicio de recursos:* los sistemas CAS son ineficientes ya que requieren señalización de forma continua o, en el caso de sistemas digitales, a intervalos regulares.

- **Canal Común (CCS).** Se refiere a la situación en que la capacidad de señalización se provee en un único canal de manera conjunta, donde

[2] `http://en.wikipedia.org/wiki/Blue_box`

la capacidad es utilizada como y cuando es necesaria. El canal de señalización puede portar información de señalización para miles de canales de tráfico.

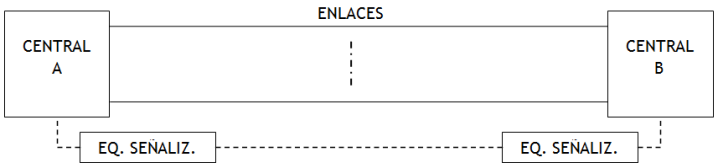

Figura 3.2: Señalización por Canal Común

Además de su naturaleza, únicamente digital, podemos destacar las siguientes ventajas que los sistemas CCS presentan sobre los CAS:

- Inaccesible al usuario.
- Repertorio amplio y extensible de señales.
- Asignación flexible de recursos.

El **modo de señalización** se refiere a la relación existente entre el tráfico y el camino que sigue la señalización. Dado que los sistemas CCS no definen una relación determinista y fija entre el tráfico y el camino de la señalización, encontramos por tanto un amplio abanico de posibilidades de configuración, o modos de señalización. Únicamente estudiaremos dos, que son los modos en los que puede operar SS7.

- **Modo Asociado:** tanto la información de usuario como la de señalización recorren la misma ruta a través de la red. Las redes que operan en modo asociado son más fáciles de diseñar y mantener a cambio de resultar menos económicas, a excepción de redes de tamaño pequeño. Toda central requiere de un enlace de señalización a cualquier otra central a la que tenga un enlace de datos, tal y como refleja la figura 3.3.

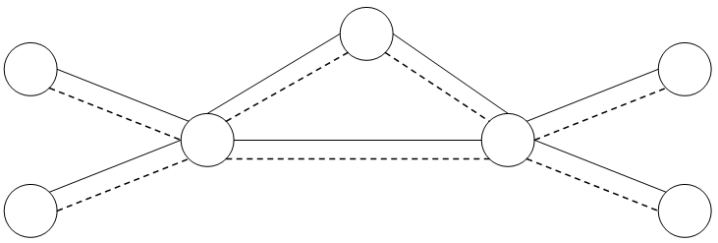

Figura 3.3: CCS Modo Asociado

- **Modo No Asociado:** la señalización sigue una ruta diferente que el tráfico conmutado al que va asociada, requiriendo que la

señalización atraviese al menos un nodo intermedio, lo que en este caso además implica la existencia de dos tipos de nodos, como muestra la figura 3.4. Las redes no asociadas suelen hacer un menor uso de los recursos de señalización aunque tienden a crear redes más complejas de mantener, donde los los fallos tienen un mayor potencial para ser catastróficos.

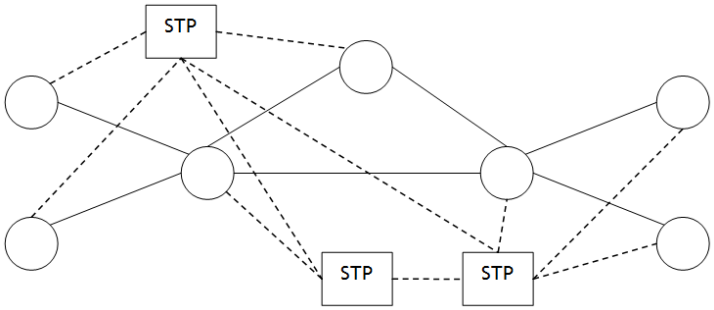

Figura 3.4: CCS Modo No Asociado

Para cerrar este apartado de repaso a los conceptos básicos de señalización, vamos a centrarnos en los diferentes **contextos de señalización**, es decir, en qué lugar de la red tiene lugar la señalización. Como se puede entender o intuir, ésto no es algo trivial y tiene importantes consecuencias.

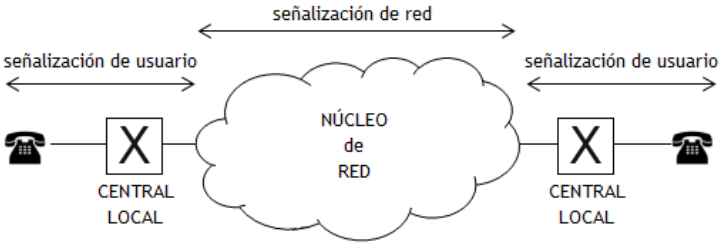

Figura 3.5: Señalización de Red y de Usuario

- **Señalización de Abonado:** tiene lugar entre el abonado y la red (asimétrica: entidades de distinto nivel jerárquico). También se conoce como señalización de acceso. Utiliza funciones de señalización sencillas, determinadas por las necesidades del dispositivo de abonado y de usuario. Encontramos varias posibilidades:

  - *Digital:* por canal común CCS, como la estudiada Q.931 en RDSI.
  - *Analógica:* asociada al canal. Se implementan señales de dirección (decádica/multifrecuencia DTMF), de supervisión (apertu-

ra/cierre de bucle) y de información (timbre, tonos audibles de progresión de llamada).

- **Señalización de Red:** es la que tiene lugar dentro de la red (simétrica: entre entidades de nivel jerárquico equivalente). Se emplean unas señales y funciones más complejas, implementadas entre equipos con inteligencia, que se encargan tanto de la gestión de las llamadas de abonados como de la gestión de red. Distinguimos:

  - *Asociada al Canal:* Analógica como el sistema C5, recogido en las normas Q.140 a Q.180, donde se implementan señales de dirección (multifrecuencia: tonos distintos de DTMF) y de supervisión (monofrecuencia).
  - *Canal Común:* sistemas de señalización digital como SS6 (recomendaciones Q.251 a Q.300) y SS7 (recomendaciones Q.700 a Q.788), utilizado en RDI y en redes móviles.

3.2. Sistema de Señalización N^{o}7 (CSS7 o SS7)

3.2.1. Generalidades

SS7 es un sistema de señalización de red por canal común de propósito general, recogido en las recomendaciones Q.700 a Q.787 de la UIT-T.

SS7 está formado por un conjunto de protocolos, empleados globalmente a través de redes de telecomunicación en todo el mundo, para dotar a las mismas de capacidad de señalización. Se puede visualizar como una red privada de conmutación de paquetes en sí misma, utilizada para realizar labores de señalización en otras redes. Al ser un conjunto de protocolos de señalización, SS7 provee de mecanismos que permiten a los elementos de las redes de telecomunicación intercambiar información de control.

AT&T desarrolló SS7 en 1975, siendo finalmente adoptado por el CCITT como un estándar mundial. En el último cuarto de siglo pasado, SS7 ha sufrido una serie de revisiones que lo han mantenido y mejorado para soportar nuevos servicios, que hoy en día prácticamente se dan por habituales.

SS7 es susceptible de ser utilizado por una gran variedad de redes digitales de conmutación de circuitos, como por ejemplo en redes de telefonía (RTC y RDSI), redes inteligentes (IN) y redes móviles. Por ejemplo, cada vez que un teléfono móvil es encendido, una serie de transacciones basadas en SS7 se encargan de identificar, autenticar y registrar al usuario en la red, como veremos más adelante.

Objetivos

El objetivo final de SS7 es lograr un sistema de señalización general para redes de telecomunicaciones digitales, que permita realizar labores de:

- Control de Llamadas.
- Control a distancia.
- Gestión.
- Mantenimiento.

SS7 es un medio seguro de transferencia de información, en secuencia, sin pérdidas ni duplicados.

SS7 está optimizado para canales digitales a 64 Kb/s, aunque puede funcionar sobre otros soportes, como por ejemplo enlaces de menor velocidad binaria, canales analógicos o enlaces punto a punto terrestres o por satélite.

Conceptos Básicos

Los nodos de la red SS7 se denominan **Puntos de Señalización (Signaling Points, SP)**. Cada punto de señalización es direccionado (identificado) por un número entero denominado **Código de Punto (Point Code, PC)**, que siguen un plan propio de numeración mundial, asignados de forma jerárquica y geográfica por la UIT. Se han definido tres tipos diferentes de SPs, es decir, de nodos SS7:

- **Punto de Transferencia de Señalización (Signaling Transfer Point, STP).** Son los responsables de la transferencia de los mensajes SS7 entre los otros nodos SS7. Su comportamiento puede ser comparado en cierto modo al de un router en una red IP.

  Los STP no suelen ser el origen ni el destino de la mayoría de los mensajes de señalización, sino que simplemente reciben un mensaje de señalización por un enlace y lo envían por otro. Los únicos mensajes que no se tratan así en un STP son los relacionados con la gestión de red y los de traducción de Títulos Globales, conceptos que estudiaremos más adelante.

  Los STPs enrutan cada mensaje entrante hacia un enlace de salida, basándose en la información de enrutado contenida en el mensaje SS7, específicamente la información encontrada en la etiqueta de enrutado MTP3, que estudiaremos más adelante.

Un STP puede encontrarse en una de estas dos formas:

- *STP individual:* se suelen desplegar en pares acoplados por motivos de redundancia y en condiciones normales de funcionamiento balancean la carga. Si falla uno de los STPs, el otro realiza todo el trabajo hasta que se resuelve el problema.
- *STP integrado (SSP+STP):* combinan la funcionalidad de un SSP y de un STP. Ambos son origen y destino de tráfico de usuario MTP. Pueden también simplemente transferir mensajes entrantes hacia otros nodos.

- **Punto de Conmutación de Servicio (Service Switching Point, SSP).** Es un conmutador de voz que incorpora funcionalidades de SS7. Procesa tráfico en banda vocal (voz, fax, modem, ...) y realiza señalización SS7. Un SSP puede ser origen y/o destino de mensajes de señalización pero no puede transferirlos. Si un SSP recibe un mensaje con un código de punto destino distinto al suyo propio, simplemente descarta el mensaje.

- **Punto de Control de Service (Service Control Point, SCP).** Actúan como interfaces entre bases de datos (específicas de telecomunicaciones) y la red SS7. Las compañías telefónicas y otros proveedores de servicios emplean numerosas bases de datos que pueden o necesitan ser consultadas para poder proveer de ciertos servicios, por ejemplo, los SCPs son el medio que provee las redes móviles de su funcionalidad básica de movilidad del abonado, como veremos al finalizar el tema.

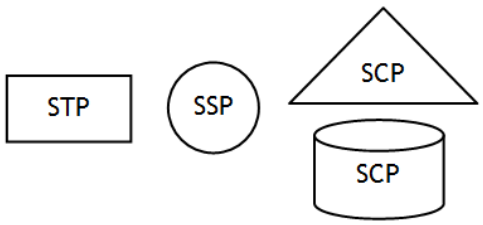

Figura 3.6: Tipos de nodos SS7.

Hemos presentado tres tipos de nodos en la red SS7, STP, SSP y SCP. Sin embargo, en el contexto de la asignatura es una práctica habitual hacer un pequeño abuso de notación y normalmente nombraremos los SSPs como SPs directamente. Consideraremos el SP como un nodo con unas capacidades más básicas en SS7 y el SSP otro nodo con unas capacidades algo más avanzadas. Más adelante incidiremos en estas diferencias.

Los SPs y STPs están conectados entre sí mediante **enlaces de señalización**, cuyo ancho de banda común es de 64 Kb/s. Para proveer de mayor capacidad o por redundancia, se pueden utilizar hasta 16 enlaces entre dos nodos. Dichos enlaces se agrupan de manera lógica por motivos administrativos y de carga compartida. Un grupo lógico de enlaces entre dos nodos se denominan simplemente *Conjunto de enlaces de Señalización (linkset).*

Un grupo de enlaces dentro de un linkset, que tengan las mismas características (capacidad de datos, terrestre/satélite, ...) se denominan *Grupo de Enlaces.* Normalmente, los enlaces en un linkset suelen tener las mismas características, con lo que, en la práctica, un grupo de enlaces suele ser sinónimo de conjunto de enlaces (linkset).

De forma parecida a los enlaces individuales, se define el Conjunto de Rutas (de una relación de señalización) como el conjunto formado por todas las rutas que puede utilizar un mensaje entre origen y destino.

Las relaciones de señalización que existen entre dos nodos SS7 se denominan modos de señalización. Los dos modos de señalización son la señalización asociada y la cuasi asociada, como ya hemos comentado. Cuando en destino de un mensaje SS7 está directamente conectado por un linkset, se utiliza el modo de asociado. Cuando el mensaje debe pasar por 2 o más linksets y a través de nodos intermedios, se utiliza la señalización cuasi asociada.

Nosotros estudiaremos SS7 utilizando un modo de señalización especial, denominado **Modo Cuasi Asociado**, que se puede clasificar como un caso particular de señalización No Asociada.

En el modo cuasi asociado, las rutas SS7 son almacenadas estáticamente[3] en cada SP, no existiendo mecanismos de descubrimiento de rutas, salvo en el caso en que se detecten errores en los enlaces. Una ruta se define como un camino preestablecido entre un origen y un destino para una relación particular. Es decir, está compuesta por un conjunto de SPs y enlaces de señalización entre el punto de origen y el de destino.

Por lo tanto, el trayecto que siguen los mensajes de señalización está predeterminado y es fijo en un momento dado, por lo que *todos los mensajes de señalización correspondientes a la misma conexión de circuito siguen la misma ruta,* así se garantiza la correcta secuenciación de los mensajes.

[3]En el proceso de inicialización de los SP y STP existe un procedimiento que se encarga de cargar las tablas de señalización que luego se utilizarán en operación.

Es fácil entender el modo de señalización si se examina la relación entre los códigos de punto entre origen y destino. Cuando se usa el modo asociado, el código de punto destino (DPC) de un mensaje enviado coincide con el código del punto del nodo al extremo final del enlace, lo que no ocurre en el modo cuasi asociado. Es evidente, que el modo cuasi asociado requiere del uso de STPs, pues como hemos comentado, los SPs, en principio no pueden reenviar mensajes de señalización.

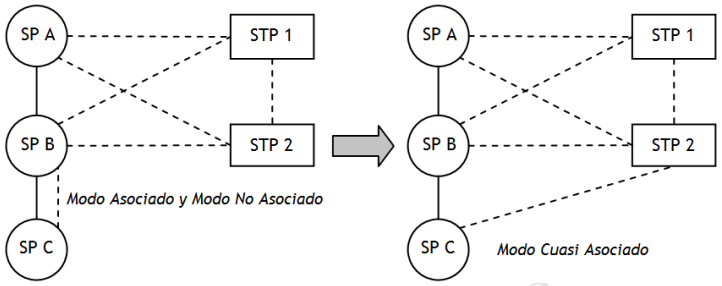

Figura 3.7: Ejemplo modos de señalización

En la parte izquierda de la figura 3.7 los modos de señalización usados son:

- SP A - SP B utiliza señalización no asociada.
- SP B - SP C utiliza señalización asociada.
- STP 1 y STP 2 utilizan señalización asociada (entre ellos y entre SP A y SP B).

Sin embargo nosotros nos centraremos únicamente en el modelo de la derecha de la figura 3.7, donde se utiliza exclusivamente el modo cuasi asociado.

3.2.2. Arquitectura de SS7

La torre de protocolos de SS7, recogida en la figura 3.8, podemos subdividirla en dos niveles:

- **Parte común** que es el sistema que ofrece al usuario transferencia fiable de mensajes de señalización, formado por la torre de protocolos *Message Transfer Part, MTP*. En principio incluye *SCCP*. A este conjunto de protocolos se le suele denominar también *Network Service Part, NSP*.
- **Parte de usuario** que es quien hace uso de los servicios de la parte común (quien decide los mensajes que se envían). Inicialmente sólo se

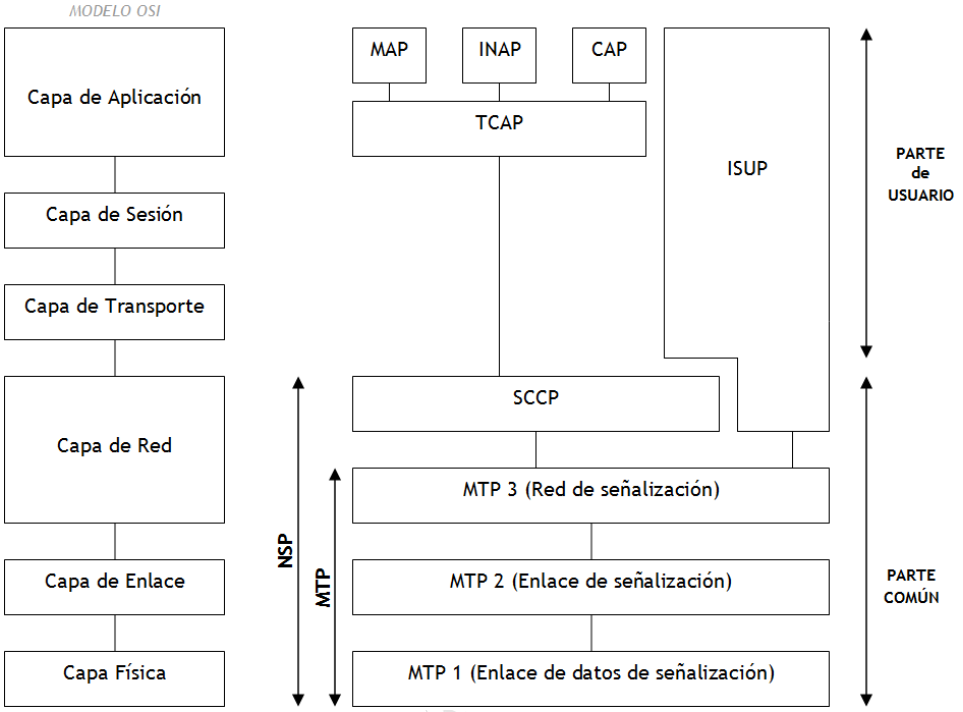

Figura 3.8: Arquitectura de SS7

usaba para el control de telefonía por conmutación de circuitos (ISUP y TUP). Con el tiempo se han ido adaptando ciertos elementos de la torre OSI al modelo de SS7 como por ejemplo la opción de protocolos orientados a conexión y otros no orientados a conexión.

Introducimos ahora los distintos niveles de la torre SS7.

- **MTP (Message Transfer Part).** Los niveles MTP 1 a 3 son nombrados colectivamente como MTP. MTP comprende las funciones para transportar información de un SP a otro. MTP se encarga de transferir el mensaje de señalización, en el orden correcto sin pérdidas ni duplicados, entre los distintos SPs que componen la red SS7. MTP proporciona transferencia fiable de los mensajes de señalización. Inicialmente, MTP fue diseñado para transmitir señalización de conmutación de circuitos, dado que no se había definido ningún otro protocolo que no fuera de conmutación de circuitos.

  - **MTP 1. Enlace de datos de señalización**. Se definen las características físicas, eléctricas y funcionales del enlace de datos así como los medios para acceder al mismo.
  - **MTP 2. Enlace de señalización.** Proporciona transferencia fiable de mensajes de señalización entre dos puntos por el enlace

de datos de señalización. MTP2 encapsula mensajes de señalización en paquetes SS7 de longitud variable. Estos paquetes SS7 se denominan unidades de señalización (SUs). MTP2 proporciona delimitación de SUs, alineamiento de SUs, monitorización de errores en el enlace de señalización, corrección de errores por retransmisión y control de flujo. MTP2 es específico para enlaces de baja capacidad (56 ó 64 Kb/s).

- **MTP 3. Red de señalización.** MTP3 realiza dos funciones:
  - *Manejo de Mensajes de señalización:* entrega mensajes entrantes a su correspondiente parte de usuario y enruta mensajes salientes hacia sus destinos. MTP3 utiliza los códigos de punto para identificar el nodo correcto para la entrega del mensaje. Cada mensaje tendrá, como veremos, un Código de Punto Origen y un Código de Punto Destino.
  - *Gestión de la red de señalización:* monitoriza los enlaces y rutas, informando de su estado a los nodos de la red para que el tráfico pueda ser redirigido cuando sea necesario. También proporciona mecanismos para realizar las correspondientes acciones correctivas cuando se produzca un error, manteniendo así la red SS7 siempre en funcionamiento.

- **SCCP. Signaling Connection Control Part.** La combinación de MTP y SCCP se suele llamar NSP (Network Service Part) en las especificaciones. La adición de SCCP dota a la red de unos métodos de enrutado más flexibles (permite servicios orientados a conexión y no orientados a conexión) a la vez que provee de un medio para transmitir datos sobre la red SS7. Estas propiedades se utilizan para soportar señalización no asociada a circuitos, lo cual se usa en mayor medida para interactuar con bases de datos (SCPs). También se utiliza para conectar con los elementos relacionados con la interfaz radio de las redes móviles. Permite el control de conexiones de señalización en la red SS7 y además proporciona la capacidad de traducción de títulos globales a códigos de punto de señalización y número de subsistema, por ejemplo, para el encaminamiento de mensajes basado en los dígitos marcados.

- **ISUP. ISDN User Part.** ISUP y TUP (Telephone User Part, que no lo estudiaremos), se sitúan encima de MTP para proveer señalización asociada al circuito para el establecimiento, mantenimiento y finalización de llamadas. ISUP además provee de soporte para los servicios suplementarios en RDSI, tales como rellamado automático, identificación de línea llamante, etc.

- **TCAP. Transaction Capabilities Application Part.** TCAP permite a las aplicaciones (llamadas subsistemas) comunicarse entre ellas

(sobre la red SS7) usando unos elementos de datos acordados. Estos elementos de datos se denominan componentes. Los componentes pueden verse como una serie de instrucciones enviadas entre las distintas aplicaciones. Algunos de los subsistemas más comunes son:

- **MAP o Mobile Application Part:** utilizada para señalización en redes móviles, por ejemplo, cuando un abonado cambia su localización VLR en una red móvil GSM, su HLR se actualiza con la nueva localización del VLR, mediante el uso de un componente *UpdateLocation*.
- **INAP o Intelligent Network Application Part:** utilizada para labores de inteligencia de red, centrándonos en el contexto de la asignatura en consultas a bases de datos, principalmente para portabilidad o servicios como cobros revertidos, tarificación adicional, ...
- **CAP o CAMEL[4] Application Part:** que es una versión simplificada de INAP para redes móviles y que no estudiaremos.

De manera genérica consideraremos los SPs como nodos que únicamente implementan ISUP como parte de usuario y los SSPs como nodos algo más avanzados que implementan, aparte de ISUP, capacidades de inteligencia de red, ya sea INAP, CAP ó MAP.

Una vez introducida la arquitectura de protocolos de SS7, pasaremos a estudiar en detalle los distintos protocolos que la componen.

3.3. MTP

En esta sección describiremos en profundidad los 3 niveles de protocolos que componen la Parte de Transferencia de Mensajes (MTP), base de SS7.

3.3.1. MTP1

MTP1, o Enlace de Datos de Señalización (Signaling Data Link, SDL), proporciona el soporte para un enlace de señalización. Recogido en la Recomendación Q.702, donde se definen las características físicas, eléctricas y funcionales del enlace, constituido por un trayecto bidireccional de datos de la misma velocidad. Los canales pueden tener naturaleza:

- *Digital*: formada por canales de transmisión digital extraídos de señales digitales. Se definen velocidades estructuradas de 2,048 Mb/s, 1,544 Mb/s y 8,448 Mb/s (Rec. G.704) y de 64 Kb/s en múltiplex digitales con estructura para circuitos de datos (Rec. X.50).

[4]CAMEL: Customised Applications for Mobile networks Enhanced Logic

- *Analógica*: formada por canales de transmisión analógicos a frecuencia vocal y modems. Hasta un mínimo de 4,8 Kb/s en control de llamadas telefónicas.

MTP1 se soporta con una velocidad binaria normalizada de 64 Kb/s en un soporte digital:

- IT 16 en señales de 2,048 Mb/s (normalizado) (si no están disponibles se puede usar cualquier otro).
- IT 67 a 70 en señales de 8,448 Mb/s (si no están disponibles se puede usar cualquier otro).

3.3.2. MTP2

En este apartado, describiremos el protocolo de capa 2, conocido como Parte de Transferencia de Mensajes (Message Transfer Part 2, MTP2), o Enlace de Señalización, que se corresponde como ya hemos indicado con la capa de 2 del Modelo OSI. MTP2 está descrito en la recomendación Q.703.

MTP2 proporciona un enlace de señalización para la transferencia fiable de mensajes de señalización entre dos puntos de señalización (SPs) directamente conectados, asegurando que la información de señalización es entregada en secuencia y sin errores, es decir, convierte un enlace físico no fiable en un enlace de datos fiable.

MTP2 realiza las siguientes funciones:

- Delimitación de las unidades de señalización.
- Alineación de las unidades de señalización.
- Transparencia.
- Detección de errores del enlace de señalización.
- Corrección de errores, mediante retransmisión (retransmisión cíclica preventiva o bien mediante «go-back-N ARQ»).
- Control de flujo.
- Alineación inicial o establecimiento de la conexión (inicialización del enlace o restablecimiento tras un fallo).
- Supervisión de errores en el enlace de señalización.

La información de señalización es transmite en unas tramas denominadas **Unidades de Señalización** (SU: Signal Unit). Las SUs son de longitud variable, por lo que requieren de unas banderas al inicio y al final de las mismas paras su correcta delimitación dentro del flujo de datos. Esta tarea, como indicamos en la lista anterior es realizada por MTP2.

La corrección de errores se implementa retransmitiendo las SUs recibidas con error. El enlace, está continuamente monitorizado, para asegurar que las tasas de error están dentro de unos limites permitidos. Si la tasa de error supera un límite predefinido, MTP2 reporta la situación a la capa superior MTP3, la cual, ordena en consecuencia a MTP2 poner el enlace fuera de servicio.

Los procedimientos de control de flujo se utilizan para evitar situaciones de congestión en la capa 2. La congestión ocurre si MTP3 se queda atrás en el procesado de las SUs disponibles en el buffer MTP2.

Es importante comprender que MTP2 no trabaja extremo a extremo. Más bien opera en un modo enlace por enlace entre dos SPs. Por lo tanto, cada enlace de señalización tiene una entidad MTP2 en cada extremo del mismo.

Formato de la Unidad de Señalización

Las unidades de señalización transportan información, originada en las capas superiores (MTP3, ISUP, SCCP) en forma de mensajes, sobre el enlace de señalización. MTP2 es similar a otros protocolos de red orientados a bit, como HDLC, SDLC o LAPB. La principal diferencia con estos protocolos proviene de los requerimientos de rendimiento en términos de pérdidas, mensajes fuera de secuencia y retraso.

Encontramos tres tipos de unidades de señalización, cada uno con su propio formato, tal y como se recoge en la figura 3.9.

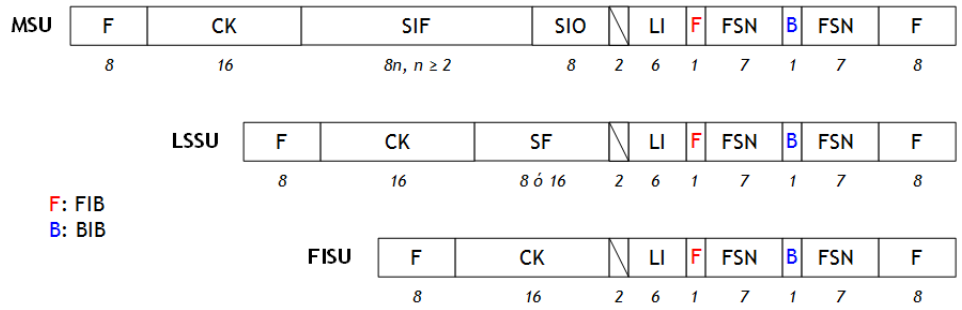

Figura 3.9: Formato Unidad de Señalización MTP2

Los tres tipos de unidad de señalización se distinguen como veremos por el campo indicador de longitud (LI).

- **FISU (Fill-In Signal Unit).** Unidad de señalización de relleno. Son las unidades de señalización más básicas y únicamente portan información correspondiente a MTP2. Se envían cuando no hay LSSUs o MSUs para enviar, evitando así que el enlace pase a estado a ocioso. El envío de FISUs garantiza que el enlace esté siempre ocupado al 100 %.

  Monitoriza errores para detectar fallos del enlace incluso cuando no hay tráfico, lo que permite conocer de manera continua el estado del enlace, permitiendo detectar rápidamente enlaces degradados y sacarlos del servicio para enviar el tráfico por otros enlaces alternativos, logrando así conseguir el requerimiento de alta disponibilidad, necesario en las redes SS7. Dado que MTP2 es un protocolo punto a punto, únicamente los niveles MTP2 de puntos de señalización adyacentes intercambian FISUs.

  Los siete campos que componen una FISU son comunes a las LSSUs y MSUs están recogidos en la tabla 3.2 y los explicaremos más adelante.

- **LSSU (Link Status Signal Unit).** Unidad de señalización de estado del enlace. Las LSSUs portan uno o dos octetos con información de estado del enlace (en el campo SF) entre los puntos de señalización en cada extremo de un enlace. El intercambio de LSSUs se utiliza para controlar el alineamiento del enlace e indicar el estado del enlace. La presencia de LSSUs en cualquier instante que no sea el alineamiento del enlace indica un fallo en el enlace, como una interrupción de procesador, congestión o una tasa de error excesivamente alta, que afecte a la estabilidad del enlace.

  Una vez que el fallo es subsanado, la transmisión de LSSUs cesa y el tráfico normal se reanuda. Como las FISUs, las LSSUs se intercambian entre MTP2 de puntos de señalización adyacentes. Los campos que componen la LSSUs son los mismos que la FISU, con el añadido de un campo adicional denominado Campo Estado (Status Field, SF). Aunque la norma especifica que pueden ser dos octetos, únicamente se utiliza uno de ellos.

  Del campo SF, únicamente tres bits están definidos, cuyo significado queda recogido en la tabla 3.1.

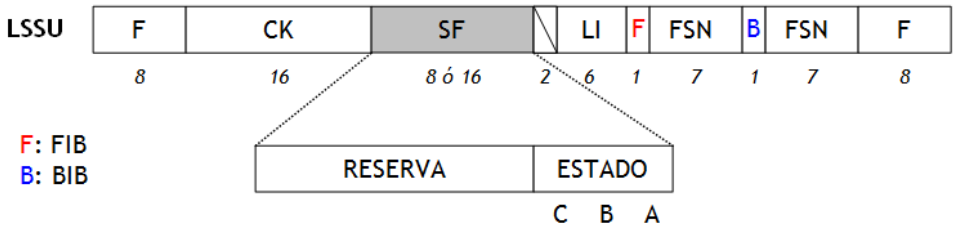

Figura 3.10: Formato Unidad de Señalización LSSU MTP2

C	B	A	ESTADO	ACR.	SIGNIFICADO
0	0	0	O: Out of Alignment	SIO	Sin alineamiento
0	0	1	N: Normal Alignment	SIN	Alineamiento normal
0	1	0	E: Emergency Alignment	SIE	Alineamiento emergencia
0	1	1	OS: Out of Service	SIOS	Fuera de Servicio
1	0	0	PO: Processor Outage	SIPO	Fallo procesador
1	0	1	B: Busy	SIB	Ocupado (congestión)

Tabla 3.1: LSSU: Valores en Campo SF

- **MSU (Message Signal Unit).** Unidad de señalización de mensaje. Las MSUs contienen los campos comunes de la FISU y dos campos adicionales: el SIF (Signalling Information Field) y el SIO (Service Information Octet). Las MSUs son las encargadas de transportar la información (o mensajes) de usuario, que en este caso son los niveles MTP3 y superiores. Los mensajes que transporta de capa superior, que pueden ser de control de llamada, consultas a bases de datos, de gestión de red, son todos mapeados dentro del SIF.

Como se indica en la tabla 3.2, un octeto bandera, codificado como 01111110 se utiliza para separar unidades de señalización consecutivas en un enlace. La bandera indica el comienzo o el final de una unidad de señalización o bien,ambos de manera simultánea.

Dado que el patrón bandera puede aparecer dentro de la propia unidad de señalización, el transmisor procesa la misma insertando un 0 detrás de cada secuencia de cinco 1's consecutivos. Este procedimiento, denominado *bit stuffing* soluciona el problema de la falsa bandera ya que evita que aparezca el patrón bandera dentro de la unidad de señalización. El receptor MTP2 realiza el proceso inverso, denominado *bit removal.* Tras la detección de la bandera, cada 0 que aparezca tras una serie de cinco 1's consecutivos es directamente borrado[5].

[5]Exactamente igual que en LAPD.

Campo	bits	Nombre	Descripción
Flag	8	Bandera	01111110 para delimitar el inicio y fin de la SU.
BSN	7	Backward Sequence Number	Indica la última MSU recibida correctamente.
BIB	1	Backward Indicator Bit	Se niega para indicar error en la SU recibida.
FSN	7	Forward Sequence Number	Identifica cada MSU transmitida.
FIB	1	Forward Indicator Bit	Se niega para indicar la retransmisión de un SU que fue recibida con error por el SP remoto.
LI	6	Length Indicator	Tipo de Trama: FISU(0), LSSU (1-2), MSU ($\geq$3).
SF	8 a 16	Status Field	Provee mensajes de estado en las LSSUs.
SIO	8	Service Information Octet	Especifica el usuario MTP3 que ha colocado un mensaje en el SIF
SIF	16 a 2176	Signaling Information Field	Contiene el contenido «real» de señalización. Relacionado con el control de llamada, gestión de red o consultas a bases de datos.
CK	16	Check Bits	Utiliza un CRC-16 para detectar errores en transmisión.

Tabla 3.2: Descripción Campos Unidades de Señalización MTP2

Los mecanismos de control de flujo y errores se basan en la numeración de las unidades de señalización. Así, las MSUs son las únicas SUs numeradas, con 7 bits en un rango de 0 a 127. Cuando hay una nueva MSU disponible para transmitir, se incrementa FSN en 1, teniendo un máximo de 127 MSUs disponibles para retransmisión. En el sentido contrario, el BSN indica el número de secuencia de la última MSU recibida correctamente, no de la siguiente que se espera.

Las LSSUs y FISUs utilizan FSN pero no se incrementan, es decir, utilizan el FSN de la última MSU enviada. Por tanto, ya que no se numeran ni asienten el envío de LSSUs y FISUs es continuo, para garantizar su correcto envío.

Se utilizan además el BIB que cambia de valor cuando solicitamos la retransmisión de una MSU, indicando en el BSN la última recibida correctamente, es decir, con un asentimiento negativo. El FIB varía su valor para indicar que estamos en una retranmisión. Su valor se mantiene hasta que se recibe un nuevo asentimiento negativo.

Respecto al campo LI, como vemos se utiliza para indicar el tipo de unidad de señalización, y lo hace indicando la longitud de la misma. Todas las SUs tienen 7 campos fijos, con un total de 7 octetos de longitud. Así el campo LI identifica el tipo de trama ya que indica el número de octetos que siguen al de LI, sin contar CK. Es decir:

- FISU = 7 octetos + LI(0) = 7 octetos.
- LSSU = 7 octetos + LI(1-2) = 8-9 octetos, donde SF = 1-2 octetos.
- MSU = 7 octetos + LI($\geq$3) = 10-... octetos, donde SIO = 1 octeto, SIF $\geq$2 octetos.

EL SIO indica la naturaleza de la MSU, es decir asocia la información de señalización con una parte de usuario mientras que el SIF es la zona destinada a la parte de usuario. Porta la información de MTP3 y tiene un tamaño entero de octetos (2 a 272 octetos). Se estudiarán más en detalle en el apartado dedicado a MTP3.

Respecto al CK o Check Bits, se utiliza un CRC de 16 bits sin contar las banderas. Como últimos aspectos a destacar, comentamos que se comienza por el bit menos significativo (LSB) en el orden de transmisión de los bits dentro de cada octeto, mientras que los bits de CK se van transmitiendo en el orden en que se generan.

La prioridad de envío de las unidades de señalización está regida como:

LSSU > MSU con ACK- > MSU Nueva > FISU > Bandera

Procedimientos

A continuación estudiaremos más en detalle los principales mecanismos y procedimientos que ocurren en el nivel MTP2 para el correcto mantenimiento del enlace: *Alineación del Enlace, Control de Flujo, Control de Errores y Supervisión de Errores.*

- **Alineamiento del Enlace**

  La finalidad del procedimiento de Alineamiento del Enlace de Señalización es establecer la sincronización y alineamiento de las unidades de señalización para que ambos extremos del enlace de señalización (puntos de señalización) sepan donde comienzan y terminan las SUs. De este modo, se realiza de manera automática un test de calidad del enlace antes de ponerlo en funcionamiento.

  Se puede entender como una fase de establecimiento de conexión para el enlace.

  El procedimiento de alineación del enlace de señalización, cuyo diagrama de flujo se recoge en la figura 3.11 asegura que ambos extremos del enlace son capaces de reconocer correctamente las banderas trasmitidas por el enlace.

  El alineamiento inicial se realiza por (encendido) para poner el enlace en servicio en su puesta en marcha o también para restaurar el servicio tras un error. El alineamiento se basa en el intercambio obligado de información de estado y un período de prueba que asegura que las SUs son detectadas correctamente.

  MTP3 solicita alineamiento inicial que es realizado por MTP2. Dado que MTP2 opera independientemente en cada enlace, el procedimiento de alineamiento se realiza en cada enlace sin envolver al resto.

  Existen dos procedimientos de alineamiento: el *procedimiento de emergencia* y el *procedimiento normal*. El procedimiento de emergencia se utiliza cuando el enlace que se va a alinear es el único enlace disponible para alguna de las rutas. En caso contrario, se utiliza el procedimiento normal.

El procedimiento de alineación se basa en el intercambio de LSSUs, donde se indica el estado del enlace según el estado que se transmite en el campo de estado (Status Field). En el procedimiento de alineación únicamente se utilizan los cuatro primeros valores recogidos en la tabla 3.1: SIE, SIN, SIO y SIOS.

El procedimiento de alineación pasa por una serie de estados durante el alineamiento inicial, tal y como se recoge la figura 3.11, y que pasamos a describir:

- *IDLE.* Cuando un SP es iniciado (encendido), los enlaces pasan automáticamente al estado ocioso (IDLE), que indica que el procedimiento está suspendido. Si el procedimiento falla en algún momento, se vuelve al estado inicial (IDLE).

- *NOT ALIGNED.* Cuando MTP2 recibe una orden para comenzar el alineamiento, el SP cambia el estado de las LSSUs transmitidas para indicar SIO (sin alineamiento) y comienza un contador T2. Si el contador T2 expira, el estado de las LSSUs vuelve a SIOS.

- *ALIGNED.* Durante T2 SIO, si se reciben SIN (alineamiento normal) o SIE (alineamiento de emergencia) del SP remoto, se paraliza el contador T2 y se cesan las transmisiones de SIOS. El SP transmite SIN o SIE, según lo que hubiera recibido previamente, y se inicia un tercer contador T3. El enlace está ahora inicializado, indicando que puede detectar banderas, y por lo tanto SUs sin error. Si el contador T3 expira, el procedimiento de alineación comienza de nuevo, transmitiendo LSSUs con un campo de estado SIOS.

- *PROVING.* El contador T4 gobierna el período de prueba, utilizando la Tasa Alignment Error Rate Monitor (AERM) durante este período. El período de prueba se utiliza para comprobar la integridad del enlace de señalización. Para ello se envían FISUs y se cuentan los errores durante el período. Se envían también LSSUs indicando si el enlace es un alineamiento normal o de emergencia. Si se detectan cuatro errores durante este período, el enlace vuelve al estado inicial (IDLE) y el procedimiento comienza de nuevo.

- *ALIGNED/READY.* Cuando el T4 expira, la transmisión de SIN/SIE finaliza, se inicia T1 y se transmiten FISUs. Si el T1 expira, se cesa la transmisión de FISUs y se transmiten LSSUs de tipo

SIOS.

- *IN SERVICE.* El contador T1 finaliza ya sea por recibir FISUs o MSUs. Cuando finaliza, el SUERM se vuelve activo.

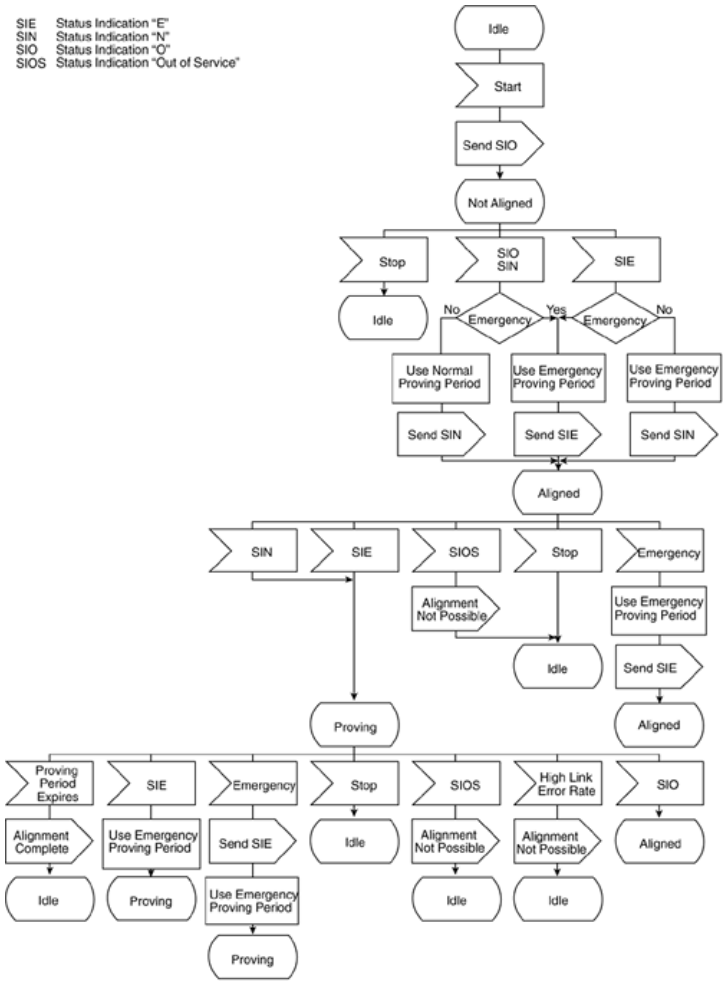

Figura 3.11: Alineamiento MTP2

Todos los contadores utilizados en este procedimiento tienen una duración que es un múltiplo del tiempo de transmisión de un octeto (Octet Transmission Time, OTT).

- **Control de Flujo**

  El control de flujo permite al tráfico entrante ser regulado cuando el buffer de recepción de MTP2 se congestiona. Cuando un SP detecta que el número de MSUs recibidas en su buffer de entrada excede un

valor particular, comienza a enviar LSSUs con su indicador de estado fijado en busy (SIB). Estas LSSUs se transmiten en intervalos fijos por un temporizador T5 (de 80 a 120 ms), hasta que la congestión desaparece. EL SP congestionado, continúa enviando MSUs y FISUs, pero descarta MSUs entrantes. Incluso congela los valores de BSN y BIB en las SUs que envía al valor de la última SU enviada antes de detectarse la congestión.

El temporizador T6, de congestión remota, se inicia cuando se recibe el primer SIB. Si T6 expira, se considera un error y el enlace se retira del servicio. La función de este contador T6 es asegurar que el enlace no permanece en estado de congestión durante un tiempo excesivo.

Cuando desaparece la congestión, se reanudan los asentimientos de las MSUs entrantes y se finaliza el envío temporizado de los SIB. Cuando el SP remoto recibe una SU con asentimiento positivo o negativo cuyo número de secuencia hacia atrás asiente una SU en su buffer de retransmisión (RTB), el temporizador T6 se detiene y se pasa a modo de operación normal en ambos extremos.

- **Control de Errores**

  MTP2 implementa dos métodos para la corrección, o mejor dicho, para el control de errores: *el Método Básico por Retransmisión y el Método de Retransmisión Cíclica Preventiva.*

  Debemos destacar en cualquier caso, que ninguno de los métodos intenta reparar una MSU corrupta, sino que el error se corrige forzando la retransmisión de la MSU. Por este motivo, los puntos de señalización tienen un buffer de retransmisión (RTB), donde van almacenando copias de todas las MSUs que han transmitido, hasta que reciben un asentimiento positivo de recepción de las mismas en el otro extremo del enlace.

  - **Método básico por retransmisión.** Es un sistema de corrección de errores por retransmisión, con asentimiento positivo y negativo. Cada mensaje es asentido cuando se recibe junto con un indicador de que el mensaje fue recibido libre de errores.

    En operación normal, este método asegura la transferencia correcta de las unidades de señalización, en secuencia y sin duplicidades sobre un enlace de señalización, por lo que no es necesario ninguna resecuenciación en MTP2.

La corrección básica de errores se logra utilizando un mecanismo de retransmisión, donde el emisor retransmite las MSUs corruptas (o desaparecidas) y todas las subsecuentes MSUs. El asentimiento positivo indica la correcta recepción de una MSU mientras que el asentimiento negativo implica una solicitud de retransmisión explícita. únicamente se asienten y reenvían, es decir se controlan, MSUs. FISUs y LSSUs no se asienten, ni por tanto reenvían, aunque sí se contabilizan para la monitorización de la tasa de errores.

Los campos de cada SU utilizados para la corrección básica de errores son cuatro: FSN, BSN, FIB y BIB. FSN y BSN son contadores cíclicos binarios en el rango de 0 a 127, mientras que el FIB y el BIB son banderas binarias utilizadas para indicar la solicitud de retransmisión. Veremos a continuación los aspectos básicos del método:

- *Número de Secuencia:* cada SU lleva dos números de secuencia, para el asentimiento y control de secuencia. El FSN se utiliza para el control de secuencia y el BSN se utiliza para el asentimiento. Antes de ser transmitida, a cada unidad de señalización se le asigna un FSN, cuyo valor se va incrementando linealmente con cada MSU transmitida. El FSN identifica de forma unívoca a cada MSU hasta que el SP receptor acepta su entrega sin errores y en el orden correcto. FISUs y LSSUs son enviadas con el mismo valor de FSN que la última MSU transmitida. Dado que el FSN varía en el rango de 0 a 127, es evidente que el buffer de retransmisión no puede almacenar más de 128 MSUs.

- *Asentimiento Positivo:* cuando el BIB en la SU recibida tiene el mismo valor que el FIB que fue previamente enviado, se indica un asentimiento positivo. El SP receptor permite aceptación positiva de una o más MSUs copiando el valor FSN de la última MSU aceptada dentro del BSN de la SU que transmite. Todas las subsecuentes SUs en esa dirección mantienen el mismo valor de BSN hasta que una nueva MSU entrante requiera asentimiento. El BIB se fija al mismo valor que el FIB recibido para indicar asentimiento positivo.

- *Asentimiento Negativo:* cuando el BIB en la SU recibida no coincide con el FIB que se envió previamente, se indica un asentimiento negativo. El SP receptor genera un asentimiento negativo para una o más MSUs invirtiendo el valor del BIB.

Luego copia el valor del FSN dela última MSU aceptada en el BSN de la SU a transmitir en la dirección opuesta.

- *Respuesta a Asentimiento Positivo:* el SP transmisor examina el BSN de la SU recibida. Dado que han sido asentidas positivamente, las MSUs almacenadas en el buffer de retransmisión que posean un FSN igual o menor que el BSN recibido, son eliminadas. Si se recibe una SU con un BSN que no es igual al BSN enviado previamente o a alguno de los FSNs en el buffer de retransmisión, la SU se descarta.

- *Respuesta a Asentimiento Negativo:* cuando el SP recibe un asentimiento negativo, la retransmisión comienza con la MSU almacenada en el buffer cuyo valor de FSN sea mayor en una unidad que la MSU asentida negativamente. Todas las MSUs que siguen en el buffer son retransmitidas en orden. Durante este período se paraliza la transmisión de nuevas MSUs. Al comienzo de la retransmisión, el FIB se invierte de manera que vuelve a tener el mismo valor que el BIB. El valor del FIB se mantiene en las siguientes SUs transmitidas, hasta que se solicita una nueva retransmisión. Si se recibe una SU con un FIB invertido (indicando el comienzo de una retransmisión) cuando no se ha enviado ningún asentimiento negativo, la SU se descarta.

En la figura 3.12 se recoge un ejemplo de un diálogo entre dos SPs en el que se muestra el funcionamiento del método del control de errores, acorde a lo explicado.

Se comprueba que la retransmisión es por rechazo simple, es decir, se retransmite la trama que ha fallado y las siguientes, a diferencia del rechazo selectivo, donde únicamente se retransmite la trama indicada.

- **Método de Retransmisión Cíclica Preventiva.** Es un sistema de corrección de errores hacia adelante, con asentimiento positivo y retransmisión cíclica. Al no haber asentimiento negativo el sistema se basa en la ausencia de asentimiento positivo para indicar la corrupción de las SUs.

  Como en el método básico, el FSN identifica la posición de una MSU en su secuencia original de trasmisión y el BSN identifica la última MSU asentida. Dado que aquí no hay asentimiento negativo los valores de FIB y BIB son ignorados y permanecen siempre a 1. El SP receptor simplemente acepta o descarta una MSU libre

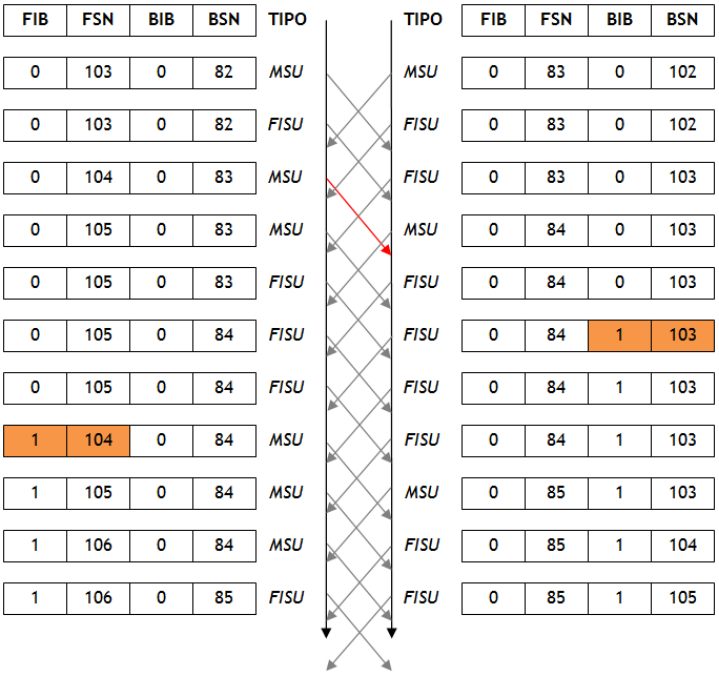

Figura 3.12: Ejemplo de Control de Errores MTP2

de errores basándose en el vaor del FSN, que debe ser superior en una unidad al FSN de la última MSU aceptada.

Una SU transmitida se mantiene en el buffer de retransmisión hasta que se recibe un asentimiento positivo para la misma. Cuando un SP no tiene nuevas LSSUs o MSUs que transmitir comienza a retransmitir las MSUs pendientes de asentimiento en el buffer, en secuencia, comenzando por la más antigua, es decir, la que posea el menor FSN. Si se asienten todas las MSUs, vaciando el buffer, se envían FISUs. Cualquier MSU retransmitida que ya haya sido aceptada por el SP receptor pero que aún no haya sido asentida de vuelta, llega fuera de secuencia y es por tanto descartada. Este método asegura que si ninguna MSU es aceptada, el SP receptor recibirá copias periódicamente hasta que devuelva un asentimiento positivo.

El método incorpora una retransmisión forzada, complementaria a la cíclica, que se inicia cuando se alcanza un valor límite de MSUs (N1) o de número de octetos de MSUs (N2) almacenados en el buffer. Se retransmiten todas las MSUs pendientes de asentimiento, paralizando el envío de nuevas MSUs y FISUs. El reenvío forzado permanece si se alcanza N1 o N2. Los valores de N1 o N2

dependen de la implementación individual de cada sistema.

Comparando el comportamiento de ambos métodos, el método de corrección básico se prefiere en enlaces que posean tiempos de propagación menores de 30 ms, ya que permite mayores cargas de MSUs que el método de retransmisión cíclica. El método de retransmisión cíclica alcanza menores cargas de MSUs ya que pierde una cantidad de tiempo relativamente alta en retransmisiones innecesarias de MSUs que ya han sido correctamente recibidas en el otro extremo, aunque no hayan sido asentidas de vuelta.

- **Supervisión de Errores**

  La monitorización de la tasa de error se realiza de manera continua cuando el enlace está en servicio y también cuando se realiza el procedimiento de alineación inicial como ya hemos comentado. Para esta tarea se han definido dos tasas de error: la tasa de error de las unidades de señalización (SUERM)y la tasa de error de alineamiento (AERM). La SUERM se utiliza cuando el enlace está en servicio y el AERM durante el proceso de alineación inicial.

  - **Signal Unit Error Rate Monitor (SUERM):** asegura la puesta en baja de un enlace con un excesivo número de errores, notificándolo al nivel superior. Se utilizan los siguientes contadores de unidades de señalización:
    - *Umbral T:* umbral de paso a no fiable, es decir, si se alcanza este umbral se considera que el enlace no es fiable y se comunica al nivel superior.
    - *Umbral D:* umbral de olvido de un error, es decir, cada D tramas recibidas (correctas o incorrectas) se descuenta un error.
    - *N:* número de octetos, para el modo de cómputo de octetos.

    Valores típicos para un enlace de señalización de 64 Kb/s son T=64, D=256 SUs, N=16 octetos.

    El conteo de errores se rige por un mecanismo de cubo agujereado o *leacky bucket*, en el que el número de errores se incrementa o bien con cada SU recibida con errores, o bien con cada N octetos (en el método de cómputo de octetos), mientras que el número de errores se decrementa cada D SUs recibidas, tal y como ya hemos indicado.

    Citando textualmente la normativa Q.703 de la ITU respecto al comportamiento de los contadores: *El monitor de la tasa de*

errores en las unidades de señalización puede realizarse en forma de un contador ascendente/descendente decrementado a una razón fija (cada D unidades de señalización recibidas o unidades de señalización erróneas indicadas por el procedimiento de aceptación), pero sin descender por debajo de cero, e incrementado cada vez que se detecte una unidad de señalización errónea por el procedimiento de aceptación de unidades de señalización (véase 4), pero sin rebasar el umbral [T (unidades de señalización)]. Se indicará una tasa excesiva de errores cada vez que se alcance el umbral T.

- **Alignment Error Rate Monitor (AERM):** el contador de errores se inicializa a 0 al comienzo del período de prueba y se incrementa con cada LSSU recibida con error o bien con cada N octetos, si el modo de cómputo de octetos está activado. En AERM no se decrementa nunca el contador de errores, es decir, no existe leacky bucket. El período de prueba se aborta si el contador alcanza el valor umbral. Se utilizan dos valores umbrales distintos, T_{in} y T_{ie}, para el modo de alineamiento normal y para el alineamiento de emergencia respectivamente. Si el período de prueba se aborta M veces, el enlace se retira del servicio y entra en estado ocioso.

  Los valores típicos para un enlace de señalización de 64 Kb/s son T_{in}=4, T_{ie}=1, M=5 y N=16.

3.3.3. MTP 3

La red de señalización SS7 está formada por nodos (SPs y STPs) y los enlaces de señalización entre ellos. El nivel 3 de MTP se adecua a la capa 3 del modelo OSI y realiza las funciones del nivel de red en la torre de protocolos SS7.

El principal objetivo de este protocolo es *asegurar la transferencia de mensajes de señalización entre los distintos nodos de la red SS7 de una manera fiable.*

Esta transferencia fiable debe garantizarse incluso en el caso de averías de los enlaces de señalización y de los STPs, por lo que es necesario informar a las partes distantes de la red de dichos errores y poder reconfigurar el encaminamiento de los mensajes.

Toda esta responsabilidad se divide en dos conjuntos de funciones, recogidas en la figura 3.13 y que estudiaremos en este mismo apartado.

- **Tratamiento de Mensajes de Señalización (Signal Message Handling (SMH)):** se encargan de enrutar los mensajes de señalización hacia el destino apropiado en la red SS7. Cada nodo analiza el mensaje entrante y basándose en el Código de Punto Destino (DPC) *discrimina* si el mensaje es destinado para él mismo. En caso afirmativo, el mensaje se entrega al usuario MTP3 correspondiente, para ello la Distribución de Mensajes consulta el SIO y en caso negativo se intenta *encaminar* el mensaje hacia el destino apropiado.

- **Gestión de la Red de Señalización (Signaling Network Management (SNM)):** formada por un conjunto de mensajes y procedimientos cuyo propósito es manejar posibles errores en la red, de manera que se consiga mantener el funcionamiento de la misma mientras sea posible, es decir, que se sigan enrutando y enviando mensajes de señalización. Todos estos procedimientos operan de manera conjunta para coordinar los recursos de la red SS7 que pueden cambiar su disponibilidad debido a las demandas de tráfico de usuario. Los nodos de la red SS7 se comunican entre ellos para tener constancia de qué rutas están disponibles para el envío de mensajes y poder así ajustar las rutas de tráfico apropiadamente.

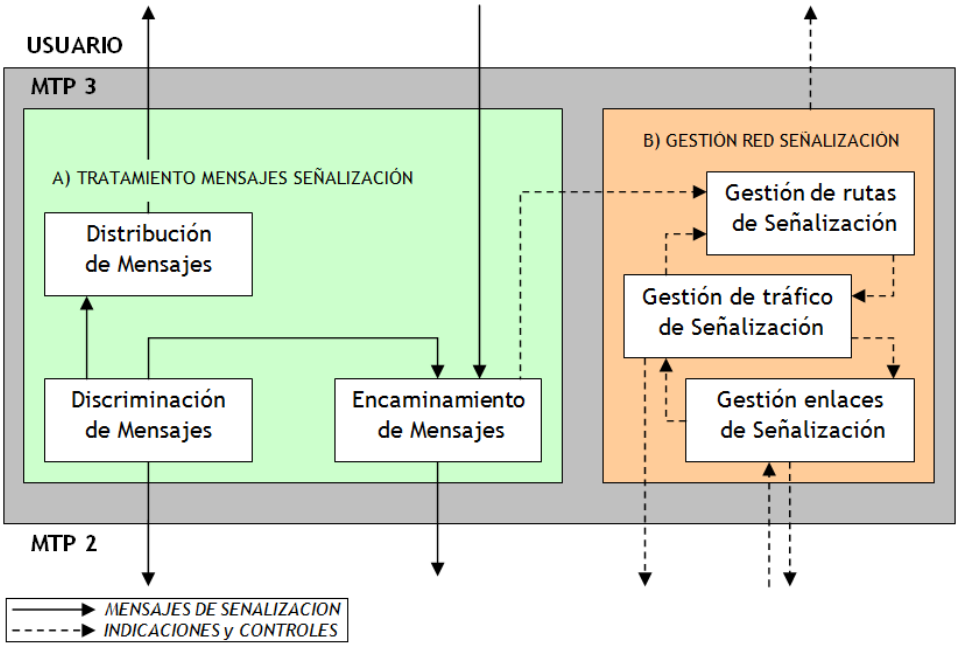

Figura 3.13: Funciones red de señalización MTP3

Antes de profundizar en estas funciones es necesario estudiar el direccionamiento en MTP3 y el formato completo de la Unidad de Señalización SS7 o MSUs.

Códigos de Punto

Como se comentó los primeros apartados, cada nodo de la red es identificado de manera unívoca por un Código de Punto, que es un número entero codificado con 14 bits, que son asignados jerárquica y geográficamente por la UIT. Un código de punto nacional identifica un nodo dentro de una red nacional mientras que un código de punto internacional identifica un nodo dentro de una red internacional. Los centros de conmutación internacionales se identifican mediante ambos.

Cada MSU contiene dos códigos de punto, el Código de Punto Origen (OPC) y el Código de Punto Destino (DPC)[6]. El DPC se utiliza para identificar el destinatario del mensaje y el OPC para identificar al nodo que originó el mensaje. El DPC es la entidad clave para poder enrutar los mensajes en la red.

La identidad del nodo originador del mensaje es necesaria para procesar el mensaje correctamente en el nodo destino. El OPC que se recibe se puede utilizar para determinar como rellenar el DPC cuando se formule un mensaje de respuesta.

Los códigos de punto son una parte esencial de SS7 y se podría profundizar más en su estudio, atendiendo a aspectos como sus jerarquías, utilización en áreas/redes, grupos, ... pero dicho estudio, aún siendo muy recomendable, se escapa del contexto de la asignatura.

Formato Unidad de Señalización

La parte de MTP3 de un mensaje SS7 está contenida en dos campos: el *Signaling Information Field (SIF*) y el *Service Information Octet (SIO)*, tal y como recoge la figura 3.14.

El SIF contiene la información de enrutado así como los datos transportados por el servicio MTP3. El SIO contiene características más generales del mensaje, para identificar el tipo de red, priorizar mensajes (en ANSI sólo) y poder entregarlos al usuario apropiado de MTP3.

- **Service Information Octet (SIO).** Es un octeto compuesto por dos partes de 4 bits, el *campo de Subservicio*, formado por los 4 bits más

[6]Se puede hacer una analogía con la IP origen y la IP destino en los datagramas IP.

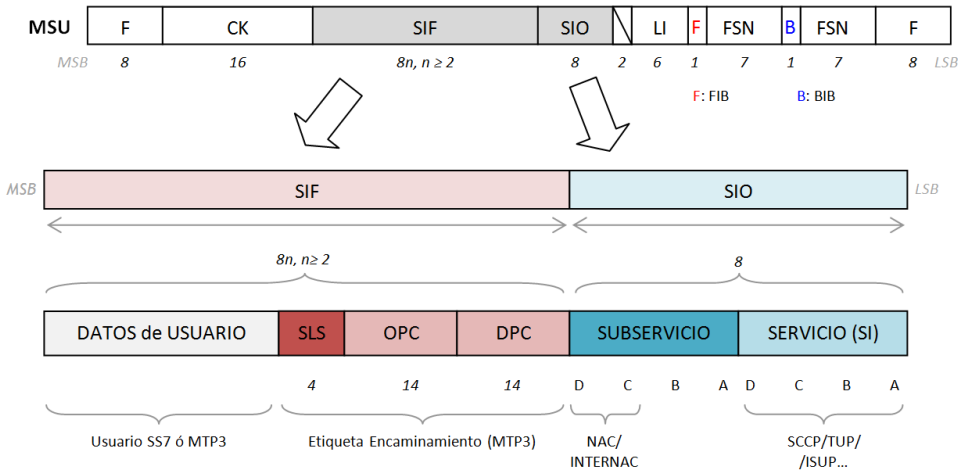

Figura 3.14: Formato Unidad de señalización MSU

significativos, y el campo de *Indicador de Servicio (Service Indicator, SI)*, formado por los 4 bits menos significativos.

El *Campo de Subservicio* consta de dos campos, el Indicador de Red, utilizado para indicar si la red es nacional o internacional, y el campo Prioridad, utilizado en redes ANSI y que puede ser implementado opcionalmente en redes nacionales UIT-T.

El *Indicador de Servicio* se utiliza para designar el tipo de carga MTP contenida en el SIF, es decir, indica el usuario de MTP, indicando el tipo de mensaje transportado. Los posibles valores de dicho campo se recogen en la tabla 3.3

- **Signaling Information Field (SIF).** El SIF contiene los datos de usuario que están siendo transportados por la red MTP, tales como números de teléfono, señales de control o mensajes de mantenimiento. El indicador de servicio, del SIO, indica el tipo de información contenida en el campo de Datos de Usuario del SIF. El comienzo del SIF contiene la denominada Etiqueta de Encaminamiento, utilizada para poder enrutar los mensajes dentro de la red, que esta formada por los siguientes campos:

  - *Signaling Link Selection (SLS):* identificador utilizado para seleccionar un enlace concreto, para balanceo o compartición de carga. Permite configuraciones para poder utilizar varios o todos los enlaces de señalización (que son todos de 64 Kb/s) en paralelo para aumentar la capacidad.

SI(ABCD)	Usuario MTP
0000	Mensajes de Gestión de Red de Señalización
0001	Mensajes de mantenimiento y Pruebas de Red de Señalización
0010	Mensajes de mantenimiento y Pruebas de Red de Señalización Especiales
0011	SCCP
0100	TUP
0101	ISUP
0110	Data User Part (llamadas y circuitos)
0111	Data User Part (registro y mensajes de cancelación)
1000	MTP Testing User Part
1001	Broadband ISUP
1010	Satellite ISUP
1011-1111	Reservado

Tabla 3.3: Valores campo Indicador de Servicio

- *Originating Point Code (OPC):* Código de Punto que identifica el nodo originario del mensaje.
- *Destination Point Code (DPC):* Código de Punto que identifica el nodo destinatario del mensaje.

Es importante destacar que todos los mensajes de señalización que correspondan a una misma llamada usarán el mismo SLS en todos los nodos que atraviesen, lo cual asegurará la transmisión en secuencia correcta de los mensajes.

A continuación estudiaremos los dos grandes bloques de funciones de la red de señalización recogidos en la figura 3.13: el *Tratamiento de los Mensajes de Señalización* y la *Gestión de la Red de Señalización.*

Tratamiento de Mensajes de Señalización

MTP3 procesa todas las MSUs entrantes para determinar cuáles deben ser enviadas a alguno de los usuarios de MTP3 y cuáles de ellas deben ser reenviadas o enrutadas hacia otro destino. Con el término usuario de MTP3 nos referimos a cualquier usuario de los servicios que proporciona MTP3, usuarios que vienen indicados en el campo Indicador de Servicio del SIO. Esto incluye mensajes generados por el propio nivel MTP3, como por ejemplo COO, COA, TFP, ... o aquellos que son transferidos de la parte de usuario, en el nivel 4 de la torre de protocolos de SS7, como por ejemplo ISUP o SCCP.

Cuando un nodo genera una MSU, MTP3 es el responsable de determinar como enrutar el mensaje hacia su destino, utilizando el código de punto destino en la etiqueta de encaminamiento y el indicador de red en el SIO.

El procesado de los mensajes por MTP3 se divide en 3 funciones: discriminación, distribución y encaminamiento, tal y como muestra la parte izquierda de la figura 3.13:

- **Discriminación:** es la tarea que determina si un mensaje entrante es destinado para el nodo que actualmente esta procesando el mensaje. La discriminación se realiza usando el indicador de red y el código de punto destino. Cuando un nodo recibe un mensaje, comprueba si el mensaje está destinado para él. para ello comprueba el DPC de la etiqueta de encaminamiento del mensaje con su propio código de punto. Si los códigos coinciden, el mensaje se envía a la siguiente función de *Distribución* de mensaje para ser nuevamente procesado. Si por el contrario los códigos no coinciden, son enviados a la función de *Encaminamiento*, suponiendo que el nodo tenga capacidad de encaminamiento.

- **Distribución:** cuando la función de discriminación ha determinado que el mensaje es destinado para el propio nodo, realiza el siguiente proceso de distribución, examinando el contenido del capo Indicador de servicio en el SIO. El indicador de servicio designa a qué usuario de MTP3 enviar el mensaje para su posterior procesado: en nuestro caso principalmente ISUP o SCCP.

- **Encaminamiento:** tiene lugar cuando se ha determinado que el mensaje debe ser enviado a otro nodo. Se dan dos circunstancias en las que ésto puede ocurrir. La primera de ellas se da cuando un nodo genera un mensaje que debe ser enviado por la red. Por ejemplo, un usuario de MTP3, como ISUP o SCCP genera un mensaje que necesita enviar utilizando para ello MTP3. El segundo caso se da cuando un STP recibe un mensaje cuyo destino es un nodo diferente, lo cual ha sido determinado por la función de discriminación. Si un mensaje llega a un Signaling End Point, sin capacidad de encaminamiento (SSP o SCP) y el mensaje no es para él, simplemente se descarta y se informa al nodo que envió el mensaje que el mensaje no pudo ser entregado, mediante un mensaje User Part Unavailable (UPU).

  En el caso de que el nodo transfiera el mensaje, el DPC determina la ruta hacia el destino. MTP3 utiliza encaminamiento por salto al siguiente, con lo cual el mensaje llegará al destino final nodo a nodo, según las tablas de encaminamiento existentes en cada nodo.

Comentar por último, que cuando se utiliza balanceo de carga, el campo SLS determina la distribución de mensajes a través de los enlaces y grupos de enlaces que atraviesan la red. El nodo originador del mensaje crea un código SLS y lo coloca en la etiqueta de encaminamiento. En cada nodo que atraviese el mensaje, se utiliza ese mismo SLS para poder enviar el mensaje por un enlace/grupo de enlaces específico, el SLS tiene pues un significado local en cada nodo pero a su vez tendrá un sentido global para los mensajes de una misma llamada, es decir, pueden existir distintas rutas origen-destino, aunque en general, todos los mensajes asociados a una llamada seguirán la misma ruta, pudiendo variar para otra llamada. Así se facilita también que los mensajes llegarán en orden correcto.

Gestión de la Red de Señalización

Errores en la red SS7 tienen un efecto potencialmente devastador sobre las infraestructuras de comunicaciones, dado que afectan a todos los abonados, afectando incluso al tráfico internacional y las acciones de recuperación y restauración pueden involucrar a varias redes. Como ejemplo significativo, SS7 fija un objetivo de indisponibilidad menor de 10 minutos por año en una ruta, es decir una disponibilidad del 99,999 % del tiempo.

La pérdida de las capacidades de señalización de un SP/STP lo aisla completamente del resto de la red. Las redes SS7 existentes hoy día son conocidas por su fiabilidad, principalmente debida a la robustez del protocolo SS7 en el área de gestión de red. Por supuesto, esta fiabilidad debe ir acompañada de un correcto diseño de la red en términos de capacidad y redundancia.

La gestión de red MTP3 está compuesta por un conjunto de mensajes y procedimientos que aseguran el correcto funcionamiento de la infraestructura de transporte de la señalización. Todo esto conlleva la aplicación automática de acciones correctoras basadas en eventos producidos en la red, como fallos de enlaces, y el informe del estado de la red a los distintos nodos de la misma.

Los distintos procedimientos de gestión implican la monitorización y el control de estado de todos los elementos que componen la red de señalización, es decir:

- *Enlaces de señalización:* que pueden encontrarse en estado Disponible o Indisponible. La indisponibilidad puede deberse a fallo del enlace, desactivación, bloqueado (SIPO) o inhibido (para mantenimiento y pruebas).

- *Rutas de señalización:* los posibles estados de una ruta son Disponible/Restringida/Indisponible.
- *Puntos de señalización:* un SP puede encontrarse Disponible o Indisponible.
- *Conjunto de rutas de señalización:* que pueden estar en Congestión o Sin congestión.

Nos centraremos en el estudio de los tres procesos recogidos en la parte derecha de la figura 3.13: gestión de enlaces de señalización, gestión de tráfico de señalización y gestión de rutas de señalización.

- **Gestión de Enlaces de señalización**

  Los enlaces son entidades físicas, disponibles para los usuarios de MTP3 una vez han demostrado ser capaces de transportar mensajes. Si un enlace falla, se produce un impacto directo entre los dos nodos que conecta el enlace. Es responsabilidad de la gestión de enlaces detectar cualquier pérdida de comunicación e intentar su restauración. Ambos nodos conectados al enlace, invocan una serie de procedimientos de restauración en un intento por restaurar la comunicación entre ambos.

  La gestión de enlaces puede a su vez subdividirse en tres procesos:

  - *Activación:* es el proceso por el cual se hace disponible un enlace para cursar tráfico de usuario MTP3. El personal de mantenimiento (o por proceso automatizado) típicamente lo realiza invocando comandos desde una interfaz OaM[7] para solicitar la activación del enlace para su uso, por ejemplo tomar el IT17 además del IT16 para señalización. Cuando un enlace es alineado al nivel 2 y supera el período de prueba, el enlace es declarado como disponible para gestionar tráfico.
  - *Desactivación:* proceso por el cual se retira un enlace del servicio, volviéndolo inaccesible para el transporte de tráfico. Al igual que la activación, el proceso se inicia usualmente invocando una serie de comandos desde una interfaz OaM. El enlace es declarado indisponible para la gestión del tráfico cuando es desactivado.
  - *Restauración:* procedimiento automático que intenta restaurar un enlace para el servicio tras un fallo, volviéndolo disponible para el uso de gestión de tráfico. El procedimiento de alineación del

[7] OaM: Operation and Management.

enlace se inicia cuando el nivel 2 detecta un fallo en el enlace. Cuando el enlace es alineado y supera el período de prueba, se realiza un chequeo del enlace de señalización. Una vez que el chequeo concluye exitosamente, la gestión del tráfico establece el enlace como disponible para su uso.

Aparte de la gestión de enlaces individuales hay que tener en cuenta dos aspectos adicionales:

- *Activación del conjunto de enlaces de señalización:* procedimiento por el que se activa un conjunto de enlaces no habiendo ninguno en servicio.
- *Atribución automática de los terminales de señalización*[8] *y de los enlaces de datos de señalización:* atribuye terminales a enlaces, entendiendo por enlace de señalización un terminal de señalización en cada extremo junto con el enlace de datos de señalización.

Estos procedimientos tienen lugar dentro de un mismo sistema, dialogando las capas MTP3 y MTP2 del mismo sistema.

- **Gestión de Tráfico de señalización**

La gestión del tráfico es el núcleo de la capa de gestión de red MTP, ya que coordina entre los distintas necesidades de comunicación de los usuarios y los recursos de enrutado o encaminamiento disponibles. Se podría hacer un símil con un policía de tráfico encargado de detener, iniciar y redigir el tráfico de vehículos ... pero no vamos a hacerlo. El tráfico debe ser desviado de enlaces indisponibles, reducido en el caso de producirse congestión y finalmente detenido en el caso de no existir rutas.

La gestión del tráfico depende de la información que suministran tanto la Gestión del Enlace como la Gestión de Rutas para dirigir el tráfico de usuario. Por ejemplo, cuando se recibe un mensaje TFP (se verá en gestión de rutas) por un destino, la gestión del tráfico debe determinar si existe alguna ruta alternativa disponible y desviar el tráfico por la misma. Durante esta proceso, se debe determinar también qué mensajes no llegaron al destino, para ser retransmitidos por el emisor y recibir su asentimiento por el destinatario, por la nueva ruta.

Los principales procedimientos que utiliza la gestión del tráfico son:

[8]Terminal de Señalización: recurso (normalmente software) encargado de generar y consumir la información de señalización en las centrales.

- *Retorno al enlace de servicio:* procedimiento por el cual se restablece el tráfico sobre un enlace que anteriormente estaba indisponible.
- *Reencaminamiento forzado:* procedimiento por el que se desvía el trafico a una ruta alternativa, como consecuencia de la indisponibilidad de una ruta.
- *Reencaminamiento controlado:* desviar el tráfico a una ruta que ha pasado a estar indisponible.
- *Re-arranque de la MTP:* actualizar el control y el estado de encaminamiento de la red cuando se desvía tráfico hacia un SP nuevamente disponible.
- *Inhibición por el sistema de gestión:* situar un enlace como indisponible para la parte de usuario con fines de prueba o mantenimiento.
- *Control del flujo de tráfico de señalización:* limitar el tráfico en su fuente cuando la red no es capaz de cursar todo el tráfico ofrecido a causa de fallos o congestión en la red.

A estos procedimientos se suma uno más, el **Paso a enlace de reserva (changeover)**, que será el único que estudiaremos. El paso a enlace de reserva es el procedimiento por el cual se desvía el tráfico hacia un nuevo enlace cuando un enlace se torna indisponible, como se recoge en la figura 3.15. Cuando un enlace dentro de un grupo de enlaces se torna indisponible, el tráfico se pasa hacia otro de los enlaces del grupo. Si no hay ningún enlace disponible, el tráfico se redirige hacia otro grupo de enlaces. La indisponibilidad puede ser detectada/determinada en ambos nodos del enlace incluso de manera simultánea[9]. El paso a enlace de reserva se gestiona con el uso de dos mensajes específicos:

- *Changeover Order (COO):* contiene FSN de la última MSU aceptada y el SLS del enlace defectuoso.
- *Changeover Acknowledgement (COA):* contiene FSN de la última MSU aceptada y el SLS del enlace defectuoso.

Cuando el enlace se determina indisponible (por ejemplo por tasa de errores alta), un mensaje de COO es enviado por el extremo que determina/detecta la situación problemática hacia el otro extremo. Cuando el otro extremo recibe el COO, compara el FSN recibido en el mismo con su buffer de retransmisión, determinando así qué mensajes deben ser retransmitidos, que serán aquellos con $FSN > FSN_{COO}$, que son

[9] Es decir, el COO de la figura podría haber sido enviado por STP2.

los que no ha recibido el extremo que avisa del error.

Cada mensaje COO debe ser respondido con un mensaje COA, asintiendo así al extremo que avisa del error que el otro extremo se ha percatado de la situación. Evidentemente, tanto el COO, como el COA, como los nuevos mensajes y los retransmitidos han de ser cursados por otro enlace distinto al defectuoso.

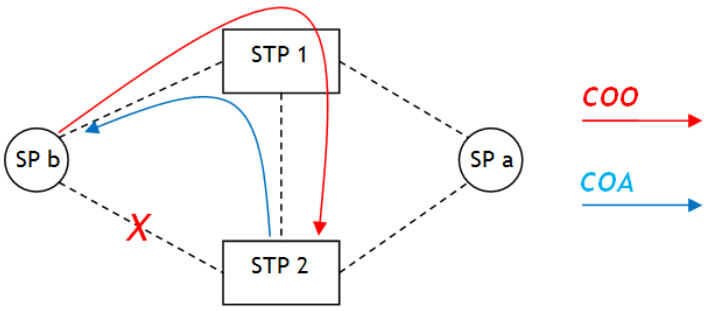

Figura 3.15: Paso a enlace de reserva

A continuación, en la figura 3.16 veremos unos ejemplos gráficos de pasos a enlace de reserva, en los que se ven afectados distintos nodos de la red.

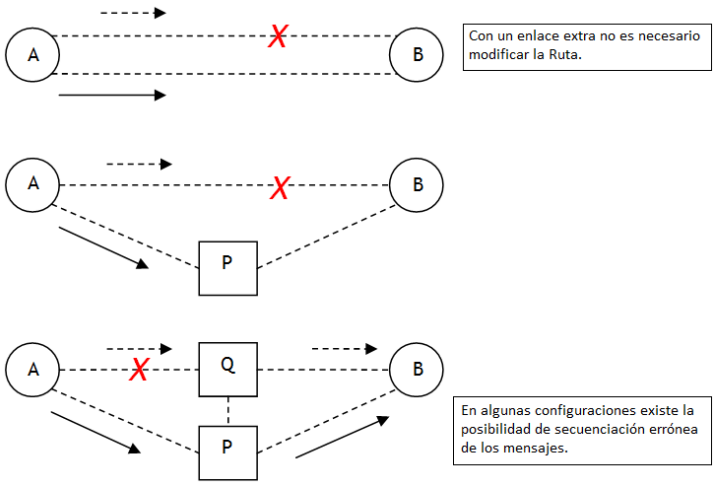

Figura 3.16: Paso a enlace de reserva: Ejemplos

Posteriormente, cuando el enlace inicialmente defectuoso vuelve a estar disponible se puede volver a cursar el tráfico por él. Para gestionar esta situación se intercambian dos tipos de mensajes:

- *Changeback Declaration (CBD):* mensaje utilizado para indicar el paso de los mensajes de señalización por el enlace recuperado.
- *Changeback Acknowledgement (CBA):* mensaje de asentimiento al CBD.

- **Gestión de Rutas de señalización**

  Su función es distribuir información sobre el estado de la red de señalización, con la finalidad de bloquear/desbloquear rutas. Es decir, se encarga de comunicar la disponibilidad de rutas existentes entre los distintos nodos de la red SS7, donde hay que ser consciente que un error en un enlace puede afectar más allá de la conexión local entre los nodos que forman el enlace.

  La gestión de rutas utiliza los siguientes mensajes o procedimientos para distribuir la información de disponibilidad/indisponibilidad de rutas entre los nodos de la red:

  - *Transferencia Prohibida (TFP):* STP informa a los SPs adyacentes que no deben encaminar ningún mensaje hacia un destino determinado a través del STP.
  - *Transferencia Autorizada (TFA):* STP informa a los SPs adyacentes que el encaminamiento hacia un destino determinado es normal.
  - *Transferencia Restringida (TFR):* STP informa a los SPs adyacentes de que si es posible, no deberían encaminar mensajes hacia un destino particular a través de él.
  - *Transferencia Controlada (TFC):* Utilizado para indicar congestión en una ruta hacia un destino particular[10]. El mensaje TFC implica congestión de transmisión, a diferencia de la congestión por recepción, cuando se llena el buffer de recepción, situación gestionada por el nivel MTP2. En la figura 3.17 se muestra un ejemplo típico en el que un STP recibe mensajes de un gran número de nodos hacia el mismo destino. STP1 encola un gran número de mensajes en su buffer de transmisión, pudiéndose dar varias situaciones en función del número de mensajes existentes en un instante dado en el buffer de salida:

    - Ocupación > T: comienza la congestión y se debe informar a los SPs de la situación con mensajes de transferencia controlada hacia z (TFC_z) periódicos.

[10] Se dice que una ruta está controlada cuando entra en congestión.

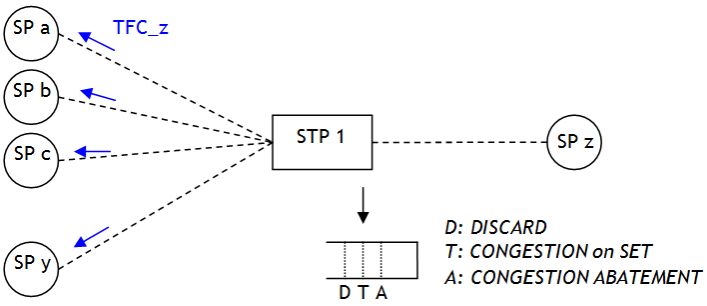

Figura 3.17: Ejemplo control de congestión de rutas

- Ocupación < A: se ha resuelto la congestión con lo que cesa el envío de mensajes TFC_z periódicos.
- Ocupación > D: los mensajes que llegan para enviar hacia SPz son descartados.

Como es lógico, se programa un efecto de histéresis en el control del buffer entre los límites A y T para prevenir continuos cambios de estado del enlace.

Los distintos SPs que han recibido mensajes de transferencia controlada, al recibir el primero de ellos inician dos contadores (T_{15} y T_{16}, de 0,66 y 1,4-2 segundos respectivamente) para controlar la desaparición de la congestión, ya que el STP congestionado no avisa de forma explícita de la desaparición de la misma, sino que simplemente deja de enviar los mensajes TFC_z periódicos. En la figura 3.18 se recoge el comportamiento de los mismos correspondiente a la situación de la figura 3.17, es decir, los mensajes indicados se corresponden a un diálogo entre un SP y STP1.

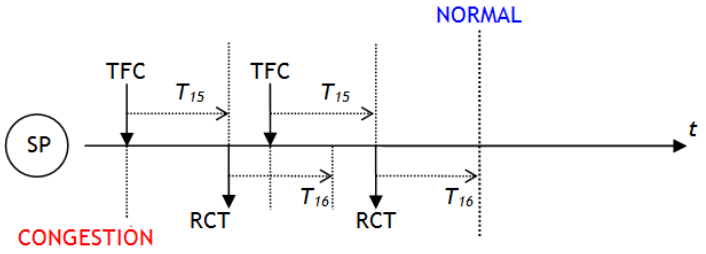

Figura 3.18: Ejemplo control de congestión de rutas: temporizadores

- *Prueba de Conjunto de Rutas (RST):* Los SPs que reciben mensajes de transferencia prohibida y transferencia restringida lo emplean para recuperar la información de la ruta de señalización que

podrían no haber recibido debido a algún fallo.

- *Prueba de Congestión de un Conjunto de Rutas (RCT):* Para actualizar el estado de congestión asociado a una ruta hacia un destino particular.

Para entender el funcionamiento de los procedimientos, veremos un ejemplo de control de disponibilidad de rutas, recogido en la figura 3.19. En 3.19-(1), inicialmente todos los enlaces funcionan correctamente, cuando se produce un error en en enlace entre SPb y STP2. Ante el error, STP2 informa de la situación a los nodos adyacentes[11].

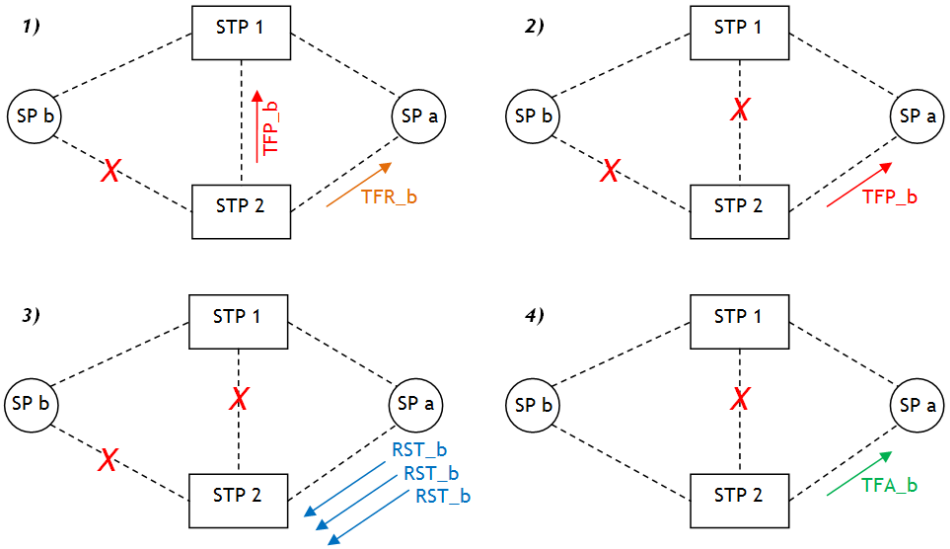

Figura 3.19: Ejemplo control de disponibilidad de rutas

Posteriormente, en 3.19-(2) cae el enlace entre STP1 y STP2, con lo que STP2 informa a SPa que no puede cursar tráfico en ningún caso hacia SPb, con un mensaje de transferencia prohibida TFPb.

Conforme transcurre el tiempo, SPa trata de averiguar si la ruta ha sido recuperada, enviando mensajes de prueba de conjunto de rutas RSTb a STP2, en 3.19-(3) hasta que finalmente el enlace se recupera y por tanto la ruta vuelve a estar disponible, informando STP2 a SPa de la situación con un mensaje de transferencia autorizada TFAb, tal y como vemos en en 3.19-(4).

Todos los mensajes estudiados en este apartado: COO, COA, TFP, TFR, TFA, RST, ... son mensajes de nivel MTP3, por lo tanto, tienen una eti-

[11] Simultáneamente se comenzaría el procedimiento de paso a enlace de reserva.

queta de encaminamiento, es decir, un código de punto origen y un código de punto destino. Aparte, y dependiendo de la funcionalidad requerida pueden llevar en sus parámetros como información opcional códigos de punto correspondientes a otros nodos de la red.

3.4. SCCP

SCCP, Signaling Connection Control Part, se define en las Recomendaciones Q.711 a Q.716 de la UIT-T. Situada encima de MTP3 en la torre de protocolos de SS7, provee funciones adicionales, propias del nivel de red para tener capacidad de transferencia no relacionada con circuitos.

MTP3 no soporta todas las capacidades de encaminamiento y direccionamiento de la capa de red del modelo OSI, proporcionando un direccionamiento bastante limitado. SCCP se añade sobre MTP3, para poder proporcionar unos sistemas de direccionamiento más sofisticados a SS7, cumpliendo con todas los requerimientos del nivel de red del modelo OSI.

Así, tal y como se mostraba en la figura 3.8, la combinación de MTP y SCCP se denomina Parte de Servicios de Red (Network Service Part (NSP)).

SCCP provee las siguientes capacidades adicionales sobre MTP:

- Extiende las capacidades de MTP hasta cumplir con la capa 3 del modelo OSI.
- Mecanismos de encaminamiento más flexibles y sofisticados.
- Mejora la capacidad de transferencia, incluyendo segmentación y reensamblado cuando un mensaje es demasiado largo para ser encapsulado en una única MSU.
- Proporciona servicios de transferencia de datos orientados a conexión y no orientados a conexión.
- Gestión y direccionamiento de subsistemas (utilizado principalmente para aplicaciones basadas en bases de datos).

SCCP se utiliza de manera intensiva en redes móviles como veremos la final del tema, aunque también se utiliza en redes fijas para aplicaciones de inteligencia de red y servicios suplementarios avanzados.

En este apartado estudiaremos en detalle las funciones de SCCP, comenzando con su arquitectura, clases de protocolos, procedimientos orientados

y no orientados a conexión, funciones de gestión, y sobre todo lo más importante, las capacidades de direccionamiento, incluyendo el uso de títulos globales.

3.4.1. Direccionamiento

Las capacidades de direccionamiento de SCCP extienden las encontradas en MTP, que se limitaban a la entrega de un mensaje a un nodo específico, identificado por su código de punto, y utilizando además un indicador de servicio de 4 bits (el Indicador de Servicio del SIO) que identificaba un usuario dentro del propio nodo.

SCCP mejora esta capacidad añadiendo los denominados **Números de Subsistema (Subsystem Number, SSN)** al código de punto. Es decir, una dirección SCCP se compone de un Código de Punto y de un Número de Subsistema.

El número de subsistema porta información de direccionamiento local que identifica a cada uno de los usuarios de SCCP en un nodo, complementando los 4 bits del SIO ya utilizados. Se puede entender, haciendo una analogía al mundo TCP/IP, como un número de puerto.

Además, SCCP aporta otra importante mejora en las capacidades de direccionamiento que es el uso de **Títulos Globales**. Un título global es una dirección, como por ejemplo los dígitos marcados, los cuales no contienen información que permita el encaminamiento directo en una red SS7, sino que es necesaria una *función de traducción* de títulos globales a direcciones DPC+SSN.

La tabla 3.4 recoge los distintos números de subsistema (Sub System Numer, SSN).

Es importante destacar que SCCP no es necesario para la señalización de llamadas telefónicas por conmutación de circuitos. Para esta función es suficiente con ISUP sobre MTP3.

3.4.2. Arquitectura de SCCP

SCCP está compuesto por cuatro áreas funcionales, recogidas en la figura 3.20.

- **SCCP Connection-Oriented Control (SCOC).** Responsable del establecimiento y liberación de conexiones virtuales entre dos usuarios SCCP. SCOC puede ofrecer características como secuenciación, control de flujo, segmentación, pudiendo incluso ignorar procedimientos de congestión asignando prioridad a datos.

SSN	Aplicación
1	SCCP Management
2	TUP
3	ISUP
4	OMAP
5	MAP
6	MAP/HLR
7	MAP/VLR
8	MAP/MSC
9	MAP/EIR
10	MAP/AuC
11	ISUP/SS ISUP
248	MUP
253	OMC
254	BSSAP

Tabla 3.4: SCCP: Números de Subsistema

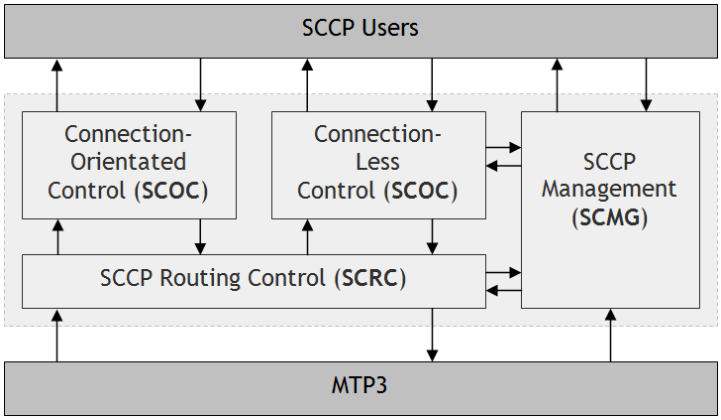

Figura 3.20: Arquitectura SCCP

- **SCCP Connection-Less Control (SCLC).** Responsable de la transferencia de datos entre usuarios SCCP sin la creación de una conexión virtual. Además de segmentación, puede ofrecer una capacidad de secuenciación limitada.
- **SCCP Routing Control (SCRC).** Proporciona encaminamiento adicional al ofrecido por MTP3, gracias al uso de los llamados titulos globales, que veremos más adelante.
- **SCCP Management (SCMG).** Responsable del seguimiento del estado de la aplicación y de informar al SCMG de otros nodos SCCP cuando sea necesario.

El término usuarios de SCCP hace referencia a las aplicaciones que utilizan los servicios de SCCP, que son mayoritariamente aplicaciones basadas en sistemas de bases de datos. Tales aplicaciones usan los servicios ofrecidos por TCAP, como veremos en la última sección del tema, para la comunicación entre pares y los servicios de SCCP para gestionar el transporte de mensajes entre dichas aplicaciones.

Las aplicaciones que utilizan los servicios de SCCP se conocen como *subsistemas*.

3.4.3. Clases de Servicios SCCP

SCCP proporciona servicios de transferencia de mensajes mejorados sobre MTP3, y lo hace ofreciendo 4 clases de servicios, organizados en 2 **categorías de servicios para transferencia de datos:** servicios orientados a conexión y servicios no orientados a conexión. Así, dentro de cada categoría se definen dos clases de servicio:

- **Servicios No orientados a conexión**
  - *Clase 0:* provee un servicio básico sin conexión y sin control de secuencia, tipo datagrama. No impone ninguna condición en los valores del Signaling Link Selection (SLS) que MTP3 utiliza, por lo tanto las NSDUs (Network SDU), mensajes SCCP pueden ser entregados fuera de secuencia.
  - *Clase 1:* Sin conexión, con entrega en secuencia. Servicio equivalente a MTP modificando el servicio ofrecido por la clase 0, forzando a que todos los mensajes tengan el mismo código de enlace de señalización (SLC/SLS)[12], logrando así que las NSDUs se entreguen en secuencia, siempre que no haya errores en la capa MTP.

[12]Signaling Link Code/Signaling Link Selector)

TCAP es el usuario típico de los servicios no orientados a conexión ofrecidos por SCCP. El otro usuario clásico es BSSAP, el cual se utiliza únicamente en los sistemas de señalización de las redes GSM.

- **Servicios Orientados a conexión**

  Operan sobre conexiones lógicas denominadas *conexiones de señalización*, que equivalen a circuitos virtuales a través de la red de señalización, donde cada conexión lógica dispone de un código de enlace de señalización único.

  - *Clase 2:* proporciona un servicio básico orientado a conexión, asignando los números de referencia locales para crear una conexión de señalización. No proporciona control de flujo, pérdidas o error de secuencia.
  - *Clase 3:* servicio mejorado orientado a conexión, que ofrece tanto detección de pérdida de mensajes como de errores de secuencia. Ofrece también control de flujo utilizando una función de datos acelerados (expedited data). Debe el lector percatarse de lo descrito para la clase 3, donde se dice detección de errores y no corrección, es decir, en caso de detección de error se notifica al nivel superior, que será el encargado de actuar en consecuencia.

  Cabría comentar que la UIT-T especificó en su momento el servicio de clase 4, pero que nunca llegó a ser implementado en redes activas y que posteriormente fue eliminado en las posteriores revisiones del protocolo.

Servicios orientados a conexión

Los servicios orientados a conexión ofrecidos por SCCP están basados en el modelo de servicio de red OSI, definido en las Recomendaciones X.213 e ISO 8348. Sus principales características tal son:

- *Independencia de las facilidades de comunicación subyacentes:* los usuarios no necesitan preocuparse de los detalles de las facilidades de la subred utilizada.
- *Transferencia extremo a extremo:* encaminamiento y retransmisión realzados por la capa de red, sin que concierna al usuario del servicio.
- *Transparencia:* no se restringe el contenido, formato o codificación de los datos de usuario.
- *Selección de la calidad del servicio:* el usuario del servicio puede solicitar una calidad de servicio dada.

- *Direccionamiento de usuario:* se usa un sistema de direccionamiento que permite a los usuarios del servicio referirse sin ambigüedad a otro usuario.

Las primitivas del servicio se recogen en la tabla 3.5.

N. Genérico	**N. Específico**	**Parámetros**
N-CONNECT	Petición	Dirección llamada/llamante/que responde
	Indicación	Selección de datos acelerados
	Respuesta	Calidad de Servicio
	Confirmación	Datos de Usuario
		Importancia
		Identificación de la conexión
N-DATA	Petición	Importancia
	Indicación	Datos de Usuario
		Identificación de la conexión
N-EXPEDITED DATA	Petición	Datos de Usuario
	Indicación	Identificación de la conexión
N-DISCONNECT	Petición	Originador
	Indicación	Motivo
		Datos de Usuario
		Dirección que responde
		Importancia
		Identificación de la conexión
N-RESET	Petición	Originador
	Indicación	Motivo
	Respuesta	Identificación de la conexión
	Confirmación	
N-INFORM	Petición	Motivo
	Indicación	Identificación de la conexión
		Nueva calidad de servicio (0/1/2/3) pedida/indicada

Tabla 3.5: SCCP: Primitivas Servicio Orientado a Conexión

En la figura 3.21 se recogen las secuencias en que deben usarse dichas primitivas.

El **establecimiento de la conexión** comienza con la petición de un usuario, contenida en una primitiva *N-CONNECT.request*. En dicha primitiva se pueden requerir ciertos servicios a mantener en la conexión solicitada,

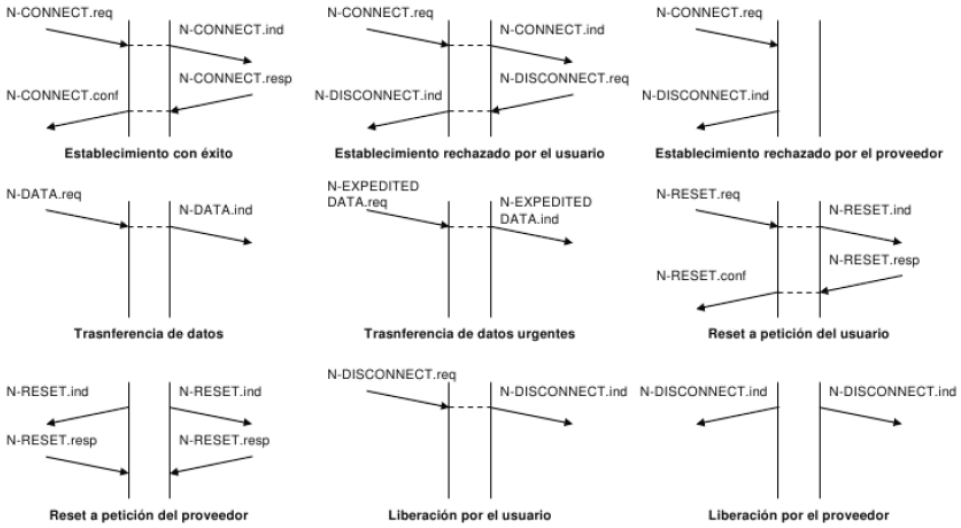

Figura 3.21: Secuencia de Primitivas Servicios Orientados a Conexión

como por ejemplo confirmación de la recepción, uso de datos acelerados (expedited data) o calidad de servicio.

Una vez solicitada la conexión, ésta puede ser denegada de varias maneras. Cuando el usuario llamado recibe la *N-CONNECT.indication* puede ocurrir que no disponga de los recursos necesarios para atenderla, por lo que el usuario llamado responde con un *N-DISCONNECT.request* que se traduce en el paso de una *N-DISCONNECT.indication* al usuario llamante. De forma parecida, si fuese la red la que no pudiera soportar la conexión, respondería inicialmente al usuario llamante con un *N-DISCONNECT.indication*, entregado directamente por SCCP.

Una vez que la conexión lógica está establecida entre los usuarios SCCP, entramos en la fase de **transferencia de datos.** Los datos de usuario son transportados en primitivas *N-DATA*, pudiendo usarse con o sin confirmación de entrega. También se pueden utilizar las primitivas *N-EXPEDITED-DATA*, para el envío ocasional de datos urgentes, si fueron previamente solicitados en el establecimiento de la conexión. Así la red da preferencia al transporte de estos datos, pudiendo incluso adelantar en la entrega a datos normales enviados anteriormente.

Las primitivas *N-RESET* se utilizan en los servicios de clase 3, forzando a SCCP a iniciar un procedimiento de reinicio para los números de secuencia. Durante este procedimiento se pueden perder algunas unidades de datos. Este proceso puede ser necesario si se pierde la sincronización en algún extremo o bien lo puede solicitar el usuario que por algún motivo necesite detener el

actual intercambio de datos pero sin finalizar la conexión.

Por último, las primitivas *N-DISCONNECT* se utilizan en la fase de **liberación de la conexión**, o bien en la fase de establecimiento para denegar una solicitud de conexión como ya hemos comentado. Es habitual que incluyan en sus parámetros los motivos que originan la liberación de la conexión así como el extremo que la solicita.

Servicios No orientados a conexión

Los servicios no orientados a conexión ofrecidos por SCCP, están igualmente basados en los servicios de red no orientados a conexión recogidos en las recomendaciones X.213 e ISO 8348. Dan la posibilidad de transferir mensajes de señalización a través de la red sin necesidad de establecer una conexión de señalización.

Mejora el servicio ofrecido por MTP con la posibilidad de mapear la dirección de llamada sobre el código de punto de señalización de MTP. Utiliza dos modos de transferencia:

- *Con control de secuencia:* garantiza la entrada en secuencia de los mensajes que contienen el mismo SLC. El usuario de SCCP utiliza el servicio incluyendo el parámetro de control de secuencia. SCCP pondrá el mismo SLC cuando tengan el mismo valor de control de secuencia.
- *Sin control de secuencia:* SCCP inserta SLCs aleatoriamente o con respecto a la compartición de carga dentro de la red de señalización.

La tabla 3.6 recoge la lista de primitivas utilizadas en los servicios no orientados a conexión.

La transferencia de datos se logra con el uso de primitivas *N-UNIT DATA*. Si el usuario desea ser informado de la no entrega de mensajes, se utiliza el parámetro opcional de respuesta «*return message on error*» en la primitiva *N-UNIT DATA.request*.

Si el usuario ha seleccionado dicha opción, SCCP utilizará la primitiva *N-NOTICE* para notificar al usuario originador del mensaje el error en la entrega del mensaje, es decir, se notifica al usuario pero no se hace nada para remedia la situación.

3.4.4. Protocolos SCCP

El protocolo SCCP se divide en cuatro clases de protocolos, uno para cada tipo de clase de servicio.

Nombre Genérico	N. Específico	Parámetros
N-UNIT DATA	Petición Indicación	Dirección llamada/llamante Control de secuencia Opción de devolución Importancia Datos de usuario
N-NOTICE	Indicación	Dirección llamada/llamante Motivo devolución datos de usuario Dirección que responde Datos de usuario Importancia

Tabla 3.6: SCCP: Primitivas Servicio No Orientado a Conexión

- Clase 0
- Clase 1
- Clase 2
- Clase 3

Los protocolos clase 0 y 1 son protocolos no orientados a conexión mientras que los clase 2 y 3 son orientados a conexión. Por tanto, cada servicio dispone de su propio protocolo siendo los formatos y algunos procedimientos compartidos entre todos los protocolos.

3.4.5. Mensajes y Parámetros SCCP

Recogemos en la tabla 3.7 la función de los principales mensajes SCCP, indicando en la última columna la clase de protocolo (C) a la que pertenecen. Las notas en dicha tabla indican:

- (1) XUDT (Extended UDT) y LUDT (Long UDT).
- (2) XUDTS (Extended UDTS) LUDTS (Long UDTS).

En la figura 3.22 se recoge el formato de los mensajes SCCP.
Pasamos a describir los principales campos de un mensaje SCCP.

- **Etiqueta de Encaminamiento:** en los protocolos orientados a conexión (clases 2 y 3) identifica una conexión particular. En los protocolos no orientados a conexión puede ser usada para el secuenciamiento y el equilibrado de carga.

MENS.	SIGNIFICADO	FUNCIóN	C.
CR	Connection Request	Solicitud de establecimiento de una conexión de señalización	2,3
CC	Connection Confirm	Respuesta para indicar que se ha realizado el establecimiento	2,3
CREF	Connection Refused	Rechazo a la solicitud de establecimiento de conexión	2,3
DT1	Data form 1	Transporte de datos de usuario de forma transparente (CL2)	2
DT2	Data form 2	Transporte de datos de usuario y asentimiento (CL3)	3
AK	Data Acknowledgment	Control de flujo por ventana	3
ED	Expedited Data	Similar a DT2 pero evitando el control de flujo (CL3)	3
EA	ED Acknoledgment	Asentimiento de un mensaje ED (CL3)	3
IT	Inactivity Test	Comprueba si la conexión esta activa en ambos extremos	2,3
ERR	PDU Error	Se envía al detectar cualquier error de protocolo	2,3
RLSD	Released	Se desea liberar la conexión y los recursos asociados	2,3
RLC	Release Complete	Respuesta a RLSD para asentir liberación y liberar los recursos	2,3
RSR	Reset Request	Se desea iniciar un procedimiento de reinicialización de secuencia	3
RSC	Reset Confirm	Respuesta a RSR para asentir reinicialización	3
UDT(1)	Unit Data	Envío de datos en el modo sin conexión	0,1
UDTS(2)	Unit data Service	Indica al origen que una UDT enviada no ha podido entregarse	0,1

Tabla 3.7: Función de los mensajes SCCP

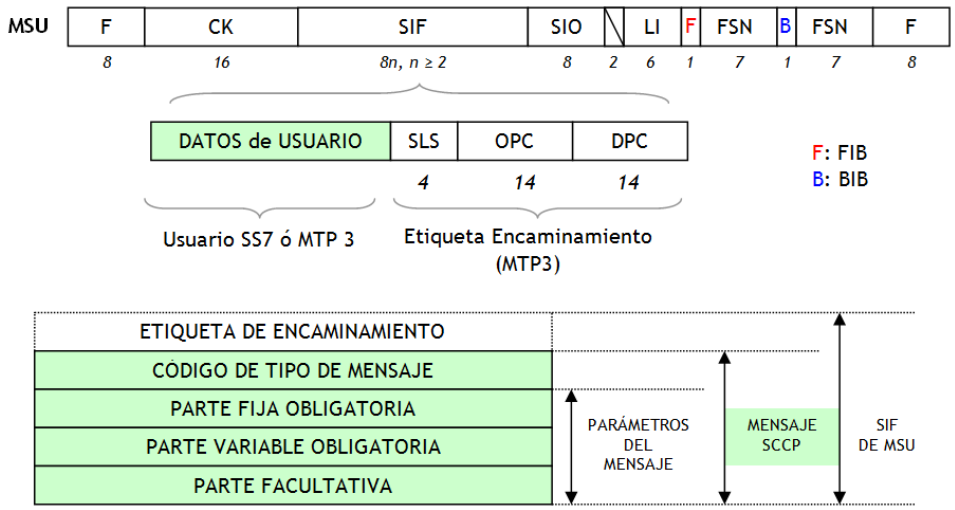

Figura 3.22: Formato mensaje SCCP

- **Tipo de Mensaje:** identifica a un mensaje entre el conjunto de mensajes SCCP.
- **Parámetros del Mensaje:** distinguimos entre obligatorios y facultativos. Los obligatorios pueden ser de longitud fija (sólo valor) o de longitud variable (longitud y valor). Los facultativos pueden ser de longitud fija o variable (etiqueta, longitud y valor).

Por último, estudiaremos los distintos servicios ofrecidos por SCCP para transferencia de datos, esto es, las distintas clases de servicio ofrecidas.

- **Operación Clase 0: Transferencia de Datos Sin Conexión.** Al ser un servicio sin conexión únicamente hace uso de los mensajes UDT y UDTS. El modo de funcionamiento se puede resumir como:
  - SCCP debe traducir el parámetro dirección llamada a un código de punto destino (DPC) que pueda ser utilizado por MTP.
  - Selecciona una ruta a través de la red y solicita a MTP que transmita el mensaje.
  - Selecciona un SLS aleatorio para compartir la carga.
  - En el extremo destino hay dos opciones. Si el mensaje ha llegado correctamente se utiliza *N-UNITDATA.ind*, si por el contrario, el mensaje ha sido descartado y la opción de retorno ha sido seleccionada se enviará UDTS hacia el otro extremo, donde se generará *N-NOTICE.ind*.
- **Operación Clase 1: Transferencia de Datos Sin Conexión.** Mantiene los procedimientos de la clase 0 pero en este caso, además se

utiliza el parámetro *Control de Secuencia* en la primitiva *N-UNITDATA.req*. Se utiliza el mismo código de enlace de señalización para todos los mensajes que tengan que ir en secuencia.

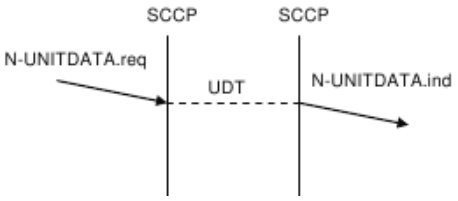

Figura 3.23: SCCP: Transferencia Clase 1

Antes de estudiar las operaciones clase 2 y 3 vamos a anticipar como se realiza la fase de **establecimiento de la conexión** en SCCP. Para el establecimiento de una conexión de señalización con una clase de protocolo acordada debe utilizarse el mensaje CR, que debe incluir:

- La dirección de la parte llamada.
- La clase de protocolo a utilizar (2 ó 3).
- El crédito (sólo para clase 3).
- El número de referencia local fuente, que identifica la conexión lógica en el extremo llamante.

Si se selecciona una conexión clase 3 puede acordarse incluso un tamaño de ventana para el control de congestión.

Recogemos a continuación en la figura 3.24 el intercambio de primitivas existente en el establecimiento de una conexión aceptada (parte izquierda) y de una conexión rechazada (parte derecha).

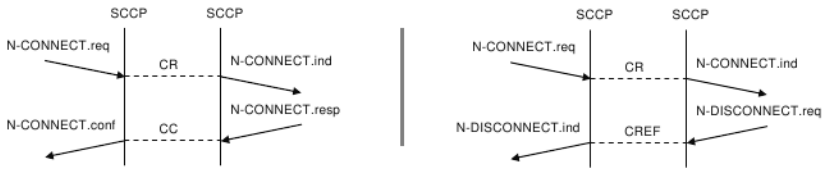

Figura 3.24: SCCP Primitivas establecimiento conexión

Ahora sí, pasamos a ver las operaciones de transferencia de datos orientadas a conexión.

- **Operación Clase 2: Transferencia de Datos Con Conexión.** Utiliza mensajes DT1 y el mismo SLS para todos los DT1, así se

garantiza la correcta entrega en secuencia. Se admite segmentación de la NSDU y su envío sobre una secuencia de mensajes DT1. Para la segmentación y reensamblado se utiliza un parámetro binario que indica a 1 que aun faltan datos y a 0 que éste es el último mensaje de la secuencia.

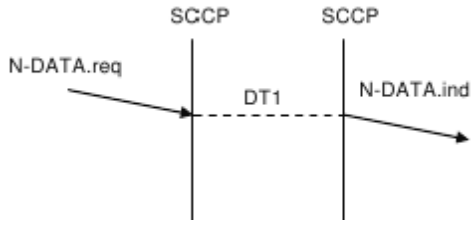

Figura 3.25: SCCP: Transferencia Clase 2

- **Operación Clase 3: Transferencia de Datos Con Conexión.** Utiliza mensajes DT2 y el mismo SLS para todos los mensajes DT2, garantizando así la entrega en secuencia.

  Detecta pérdidas de mensajes o secuencia incorrecta. Admite segmentación de la NSDU y su envío sobre una secuencia de mensajes sobre DT2, aunque a diferencia de la clase 2, el parámetro de secuenciación/-segmentación utiliza una numeración secuencial, distinguiendo:

  - *P(S):* Número de secuencia en emisión (7 bits).
  - *P(R):* Número de secuencia en recepción (7 bits).
  - *M:* indicador de más bits (1 bit).

  Implementa un mecanismo de control de flujo basado en *asignación de crédito* para transmisión, en el que separa el control de flujo del asentimiento de mensajes característicos del esquema de ventana deslizante es decir, el asentimiento de los mensajes recibidos está desacoplado del tamaño de la ventana, que además puede ir variando en ejecución. Recogemos un ejemplo de funcionamiento de dicho mecanismo en la figura 3.26.

  Antes de comenzar la transmisión de datos, en la fase de establecimiento de la conexión ambos extremos deben acordar el tamaño inicial de la ventana, donde en el ejemplo inicialmente tenemos un crédito de 7 unidades, es decir, una ventana de 7 mensajes. Comenzamos a enviar mensajes (N=0,1,2) y gasto 3 créditos. Entonces se envía un ACK de esos 3 primeros mensajes. Mientras se recibe el ACK se han enviado 2 mensajes más. En el ACK uno de los parámetros es el crédito que

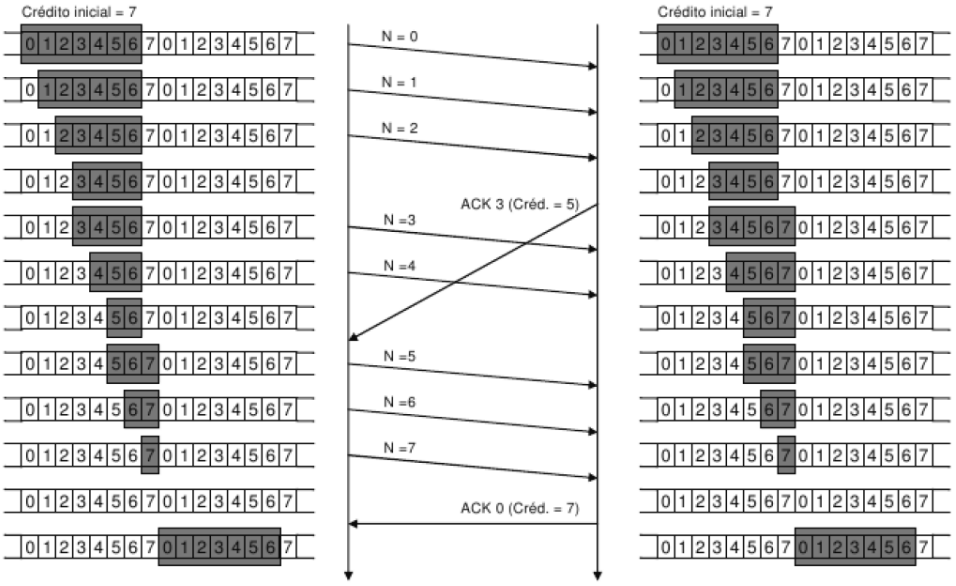

Figura 3.26: SCCP: Mecanismo Asignación de Crédito Transferencia Clase 3

puede ser variado por tanto en cuanto haga falta. En este ACK se modifica el crédito a 5 unidades por lo que al ser recibido, sólo se añade un mensaje más a las lista. En la figura aparecen para enviarse 5, 6 y 7, pero quedaban por recibir ACK 3 y 4 (ventana = 5 y crédito = 3). Se envían 5, 6 y 7 y nuestro crédito se agota. Cuando llega el ACK con crédito = 7 ya volvemos a poder disponer de los mensajes para enviar. ACK 3 significa que se espera el mensaje con N = 3 al igual que ACK 0.

Los servicios de transferencia de datos con conexión (clases 2 y 3) admiten la transferencia de datos urgentes (acelerados), mediante el paso de mensajes ED y EA. Existen una serie de limitaciones para los datos acelerados, como por ejemplo que sólo puede haber un ED pendiente de asentimiento en cada momento, por lo que antes de enviar otro ED hay que recibir el asentimiento (EA) del ya enviado.

Al ser un servicio orientado a conexión, cuando finalice la transferencia de datos hemos de **liberar la conexión**, lo cual se realiza con el intercambio de mensajes RLSD y RLC.

3.5. ISUP

La parte de usuario de RDSI o ISDN User Part, ISUP, definida en las recomendaciones Q.761 a Q.769 de la UIT-T, es responsable del estableci-

miento y liberación de enlaces utilizados para el intercambio de llamadas. Como su nombre indica, ISUP fue diseñada para proporcionar señalización en el núcleo de red, compatible con la señalización de acceso de RDSI. La combinación de señalización de acceso RDSI junto con la señalización troncal ISUP proporciona un mecanismo de transporte de datos de señalización extremo a extremo entre abonados RDSI.

Hoy en día, el uso de ISUP en la red ha superado su objetivo inicial, proporcionando señalización tanto para usuarios RDSI como no RDSI. De hecho, la mayoría del tráfico ISUP viene generado inicialmente por usuarios con accesos analógicos, como por ejemplo los proporcionados por el acceso al servicio de telefonía básica.

ISUP define funciones, procedimientos y flujo de señalización, para proporcionar servicios por conmutación de circuitos, junto con facilidades de servicio asociadas, para llamadas tanto vocales como no vocales.

Como vemos en la arquitectura de SS7, recogida en la figura 3.8, ISUP reside en el nivel 4 de dicha torre de protocolos, teniendo interfaces tanto con MTP3 como con SCCP. ISUP utiliza los servicios de transporte proporcionados por MTP para intercambiar los mensajes de red utilizados para el establecimiento, liberación de llamadas, etc. La conexión con SCCP se utiliza para el transporte de señalización extremo a extremo, aunque a pesar de que SCCP proporciona esta capacidad, normalmente la señalización ISUP extremo a extremo se transporta también sobre MTP3.

Resumiendo, ISUP confía en MTP o NSP[13] para la transmisión de mensajes y debe interfuncionar con el protocolo de control de llamadas usuario-red de RDSI (Q.931), además de presentar una cierta flexibilidad para acomodarse a futuras mejoras de las capacidades de RDSI.

Destacamos la diferencia entre Q.931 e ISUP, siendo Q.931 un protocolo para facilidades de señalización por canal común usadas por el *usuario* de RDSI para el control de llamadas, mientras que ISUP proporciona facilidades de señalización empleadas por el *proveedor* de la red en nombre del usuario RDSI para proporcionarle los requisitos solicitados en el control de llamadas. Es decir, Q.931 es señalización entre el abonado y la red mientras que ISUP es señalización dentro de la red, entre las centrales.

Para facilitar o poner un poco en contexto ISUP, recurrimos al escenario de la figura 3.27.

[13]NSP: Network Service Part ≡ MTP+SCCP.

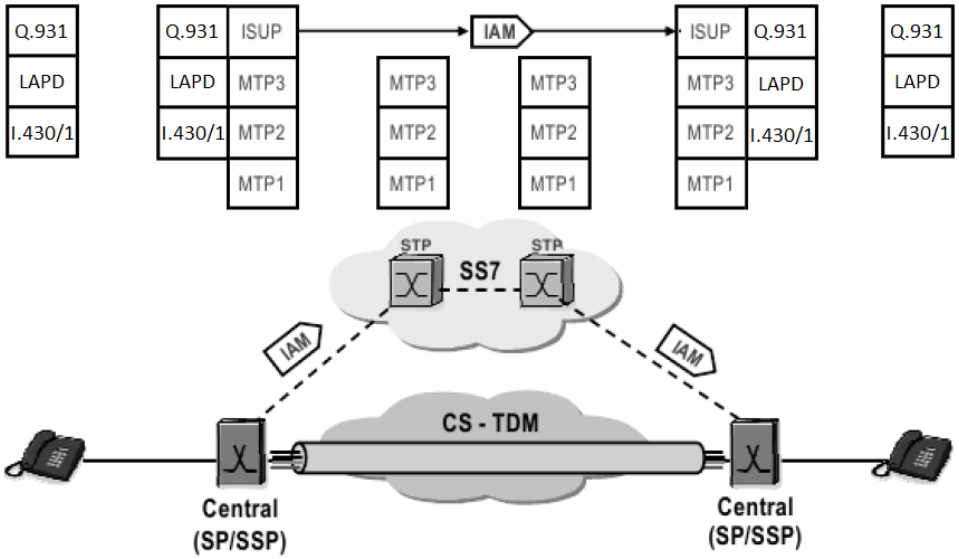

Figura 3.27: Idea básica ISUP

En dicho escenario, vemos que para establecer una llamada, es decir establecer un circuito, es necesario el uso de señalización en ambos extremos entre el usuario y la red, señalización ya estudiada en el tema dedicado a RDSI. Pero para llegar desde la central del abonado llamante al llamado es necesario ir reservando circuitos entre centrales para establecer el circuito definitivo. Ésta, y no otra, es la función principal de ISUP, es decir, ISUP es el protocolo que hablan los elementos internos de la red, es decir las centrales, para la reserva de circuitos compartidos entre ellos. Para hacer llegar los mensajes ISUP entre las centrales (SPs) en principio nos es suficiente con MTP.

3.5.1. Mensajes ISUP

El campo de datos de usuario del SIF de MTP3 contiene o encapsula los mensajes ISUP, identificados por un valor de 5 en el campo del Indicador de Servicio en el SIO de MTP3, tal y como vemos en la figura 3.28. Los mensajes ISUP se rigen por un formato estándar que incluye los siguientes campos:

- **Etiqueta de Encaminamiento:** forma parte de la cabecera MTP3. Indica los puntos fuente y destino del mensaje, incluyendo también el código del enlace de señalización (SLS) para compartir la carga entre múltiples enlaces físicos. Para cada conexión de circuito individual se debe usar la misma etiqueta de encaminamiento para todos los mensaje asociados a esa conexión.

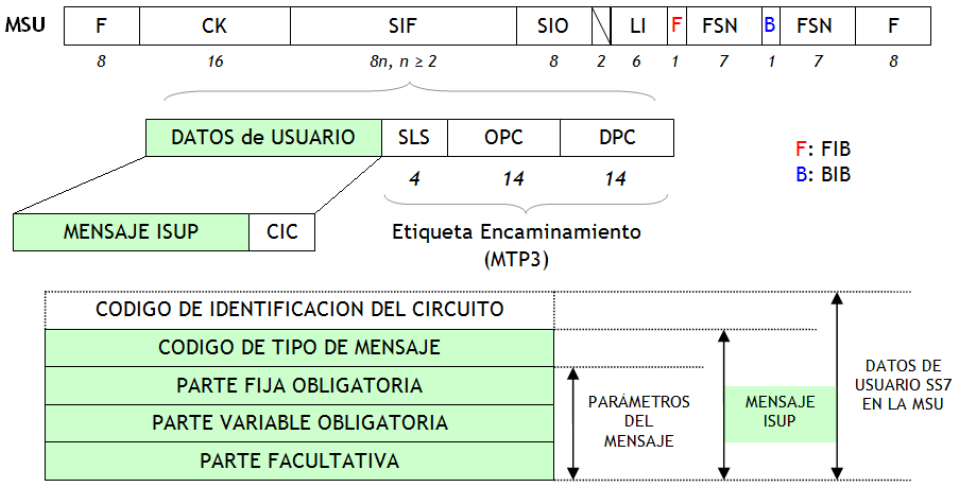

Figura 3.28: Encapsulado mensaje ISUP

- **CIC:** es el código de identificación de circuito al cual el mensaje esta asociado, es decir, especifica el circuito con el que está relacionado el mensaje. Dado que conexiones de n x 64 Kb/s siempre usan time slots adyacentes, basta con un CIC.
- **Tipo de Mensaje** indicador de tipo de mensaje ISUP, como por ejemplo IAM, ACM, ... que explicaremos a continuación. El contenido del resto del mensaje dependerá del tipo de mensaje enviado, pues tendrá más o menos campos fijos o variables, parte opcional, ...
- **Parte obligatoria de longitud fija:** parámetros obligatorios del mensaje y de longitud fija.
- **Parte obligatoria de longitud variable:** parámetros obligatorios del mensaje pero de una longitud variable. Cada parámetro variable debe indicar en primer lugar su longitud y después incluir el contenido del propio parámetro.
- **Parte facultativa (opcional):** parámetros que pueden ir incluidos o no en el mensaje. Cada parámetro debe incluir su nombre, longitud y su propio contenido.

En la figura 3.29 se muestra la estructura del mensaje ISUP introducida aquí. Esta estructura de mensaje proporciona una gran flexibilidad en la construcción de nuevos mensajes. Cada tipo de mensaje define sus parámetros fijos obligatorios necesarios para la construcción del mensaje, sin necesidad de incluir la longitud de los mismos ya que los estándares ISUP definen la longitud de los mismos. Los parámetros variables sin embargo, incluyen un puntero que indica el comienzo de cada parámetro (el valor del

puntero es el número de octetos tras el propio puntero donde se encuentra el parámetro), siendo el primer dato apuntado la longitud del mismo. Los punteros se incluyen justo después de los mensajes obligatorios de longitud fija.

Los parámetros opcionales se rigen de manera similar, por un último puntero que apunta al resto de la parte opcional del mensaje.

Los mensajes ISUP pueden clasificarse en las siguientes categorías:

- **De establecimiento**
  - *Hacia adelante:* establecimiento de un circuito. Identifica las centrales y las características de la llamada.
  - *Generales:* cualquier información adicional durante el establecimiento. Comprobación de características en caso de varias RDSI.
  - *Hacia atrás:* soportan el proceso de establecimiento de una llamada. Inician los procesos de tarificación y contabilidad.
- **De supervisión**
  - *De llamadas:* adicionales para el establecimiento de la llamada. Indican si ha sido respondida e intervenciones manuales.
  - *De circuitos:* relativas a un circuito previamente establecido. Principalmente liberación, suspensión y reanudación.
  - *De grupos de circuitos:* para tratar un grupo de circuitos como una unidad simple. Similares a las de la categoría de supervisión de circuitos.
- **De modificación dentro de una llamada:** alterar las características o las facilidades de red asociadas a una llamada activa.
- **De extremo a extremo:** capacidades de *paso de largo* y de información de usuario extremo a extremo.

A continuación recogemos los mensajes ISUP esenciales junto con sus principales características, utilizados en los procesos de establecimiento, supervisión y liberación de llamadas, cuyos diálogos y progresos estudiaremos en la siguiente sección.

- **IAM - Initial Address Message.** Mensaje hacia adelante ($\Longrightarrow$) que contiene la información necesaria para establecer una llamada, generado al recibir el mensaje de SETUP (Q.931) del terminal llamante que intenta solicitar una llamada a la red. En una llamada básica, éste es el primer mensaje enviado y es habitualmente el mensaje de mayor

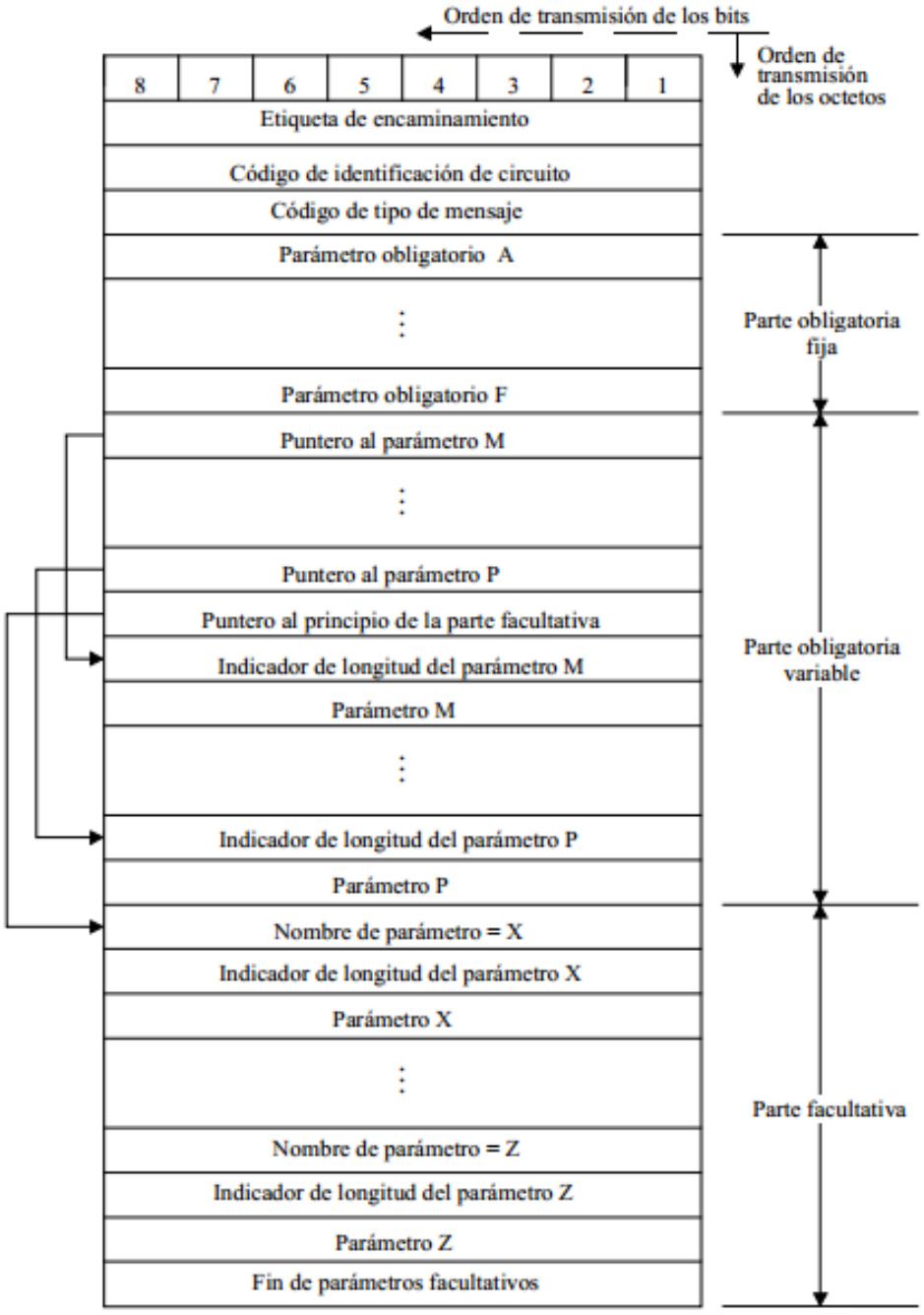

Figura 3.29: Formato mensaje ISUP

tamaño. Los principales campos del mensaje IAM, de entre los 62 posibles, se recogen en la tabla 3.8. IAM podría interpretarse como: «*Tomo X circuito para la llamada Y*».

- **SAM - Subsequent Address Message**. Mensaje hacia adelante ($\Longrightarrow$), que tras el IAM pueden ser utilizados (uno o más) para enviar información relativa a la dirección de la parte llamada. Es utilizado en el marcado solapado.

- **ACM - Address Complete Message.** Mensaje hacia atrás ($\Longleftarrow$), enviado inicialmente por la central destino y utilizado para indicar que se han recibido todas las señales necesarias (dígitos) para encaminar la llamada hacia la parte llamada. En la señalización en bloque, el ACM es enviado justo tras la recepción del IAM mientras que en la señalización solapada se envía tras la recepción del último SAM y tras el SETUP (Q.931) al terminal llamado. Puede utilizarse para llevar información asociada al estado del abonado llamante (libre, ocupado, ...). ACM podría interpretarse como: «*Dirección completa. No me mandes más números, no me hacen falta para encaminar*».

- **CPG - Call Progress.** Mensaje hacia adelante y/o hacia atrás ($\Longrightarrow\Longleftarrow$) utilizado para indicar la ocurrencia de un evento durante el establecimiento de la llamada que debería hacerse llegar a la parte llamante o la parte llamada. Típicamente para indicar si el abonado llamado está disponible u ocupado, si no se ha avisado antes en el ACM. CPG podría interpretarse como: «*Ha ocurrido X evento*».

- **ANM - Answer Message.** Mensaje hacia atrás ($\Longleftarrow$), enviado por la central destino cuando la parte llamada responde, es decir, al descolgar y haber recibido por tanto la central destino el mensaje CONNECT (Q.931). No contiene ningún campo de información salvo el de tipo de mensaje. Se utiliza para iniciar el cómputo de la tasación a aplicar e inicia también la medición de la duración de la llamada. ANM podría interpretarse como: «*El usuario llamado ha descolgado*».

- **REL - Release Message.** Mensaje hacia adelante y/o hacia atrás ($\Longrightarrow\Longleftarrow$) utilizado para indicar que el circuito se libera y está preparado para pasar al estado de reposo al recibir un mensaje RLC. En los campos obligatorios del mensaje se incluye el motivo de la liberación

- **RLC - Release Complete Message.** Mensaje hacia adelante y/o hacia atrás ($\Longrightarrow\Longleftarrow$) enviado como respuesta a un mensaje REL, o si procede,a un mensaje de reiniciación de un circuito cuando se ha puesto en la condición de reposo.

Parámetro	Tipo	Long.(oct.)
Tipo de mensaje	F	1
Indicadores de la naturaleza de la conexión	F	1
Indicadores de llamada hacia adelante	F	2
Categoría de la parte llamante	F	1
Requisitos del medio de transmisión	F	1
Número de la parte llamada	**V**	**4-?**
Selección de la red de Tránsito (uso nacional)	O	4-?
Referencia de llamada (uso nacional)	O	7
Número de la parte llamante	O	4-?
...	...	...
Información de usuario a usuario	O	3-131
Información de teleservicio de usuario	O	4-5
Requisitos principales del medio de transmisión	O	3

Tabla 3.8: Parámetros Mensaje IAM

A continuación, se verán una serie de ejemplos de control de llamadas, donde se muestran las interacciones entre los distintos mensajes ISUP aquí explicados.

3.5.2. Ejemplos control de llamadas

El primer ejemplo, recogido en la figura 3.30, se recoge como se van modificando salto a salto los códigos de punto destino de la trama MTP3, así como se van reservando los circuitos, mediante mensajes IAM hasta llegar a la central de la que cuelga el abonado. Es un ejemplo simplificado donde faltarían mensajes de respuesta.

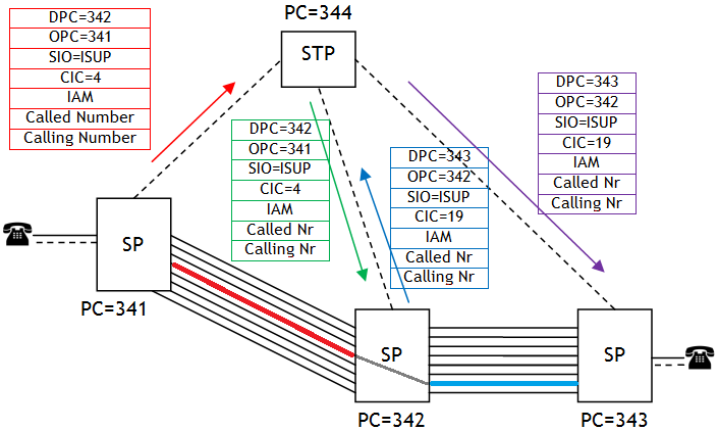

Figura 3.30: Llamada por Conmutación de Circuitos

Es importante destacar que los mensajes IAM, no recorren la red extremo a extremo como pudiera parecer en un diagrama simplificado, sino que en cada salto se genera un nuevo mensaje, utilizado para reservar un circuito entre cada dos centrales.

En la figura 3.31 se recoge un diálogo simplificado, es decir que faltan mensajes en las interfaces Q.931, para el establecimiento de una llamada ordinaria, con envío en bloque.

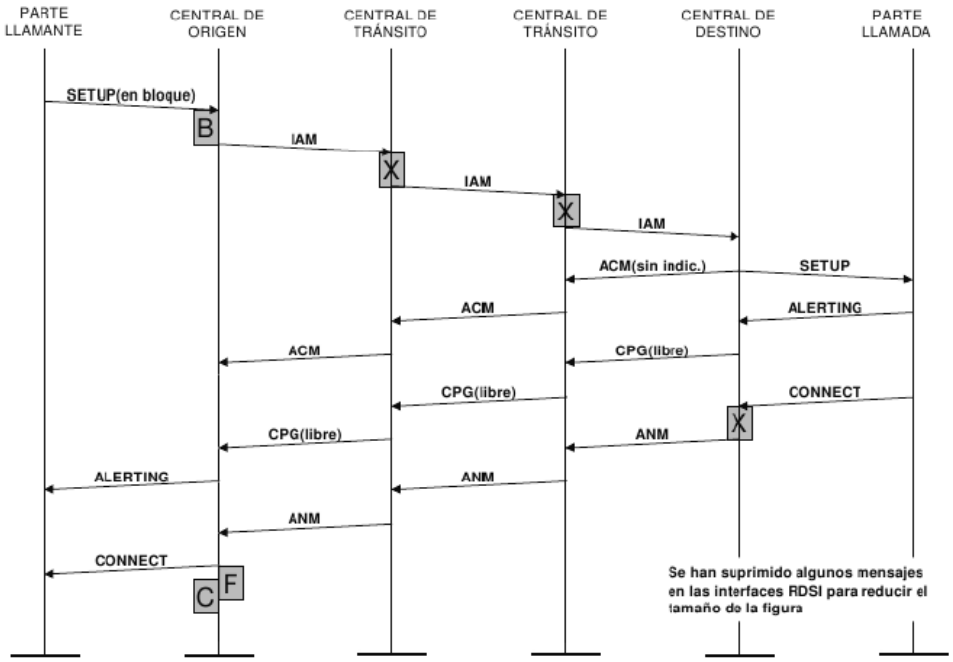

Figura 3.31: ISUP: Llamada ordinaria completa, en bloque

Mientras que en la figura 3.32 se recoge un diagrama simplificado para el establecimiento de una llamada ordinaria, con envío solapado.

Finalmente, se recoge un diálogo simplificado de liberación de llamada normal en la figura 3.33, donde vemos como se van liberando los circuitos salto a salto.

Algunos detalles importantes a destacar en estos ejemplos:

- *ACM:* el ACM puede llevar de vuelta como parámetros información de estado del abonado llamante, con lo que podría evitarse el envío de un mensaje CPG. Ejemplos de dicha información de estado son:
  - Sin indicación: implicaría que se desconoce el estado del abonado

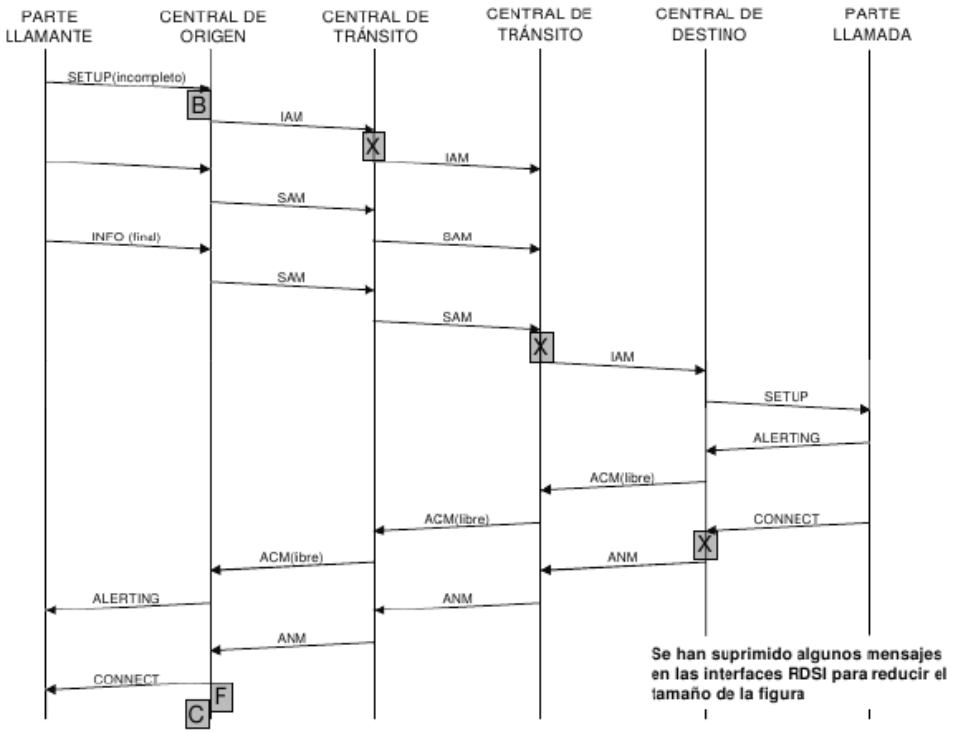

Figura 3.32: ISUP: Llamada ordinaria completa, solapado

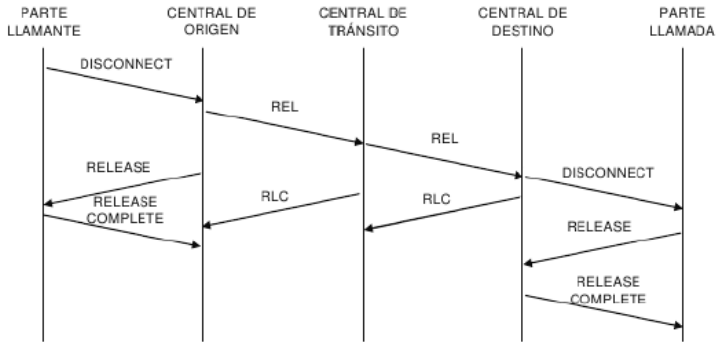

Figura 3.33: ISUP: Liberación de llamada normal

llamante (si está libre u ocupado, si tiene teléfonos en su casa, ...
    - Libre: se puede cursar la llamada. Implica que se ha recibido un mensaje de ALERTING por parte del abonado llamado.
    - Ocupado: no se puede cursar la llamada.
- *B:* el punto (B) indica que se reserva el canal B hacia atrás para la llamada en establecimiento.
- *X:* los puntos (X) indican que se están reservando circuitos hacia atrás entre las centrales para la llamada en establecimiento.
- *F:* indica reserva del canal B hacia adelante para la llamada en establecimiento.
- *C:* punto donde la UIT-T recomienda comenzar la tarificación de la llamada.

3.5.3. Señalización Extremo a Extremo

Es la capacidad para transferir información de señalización directamente, en dos situaciones específicas:

- **Situación (A):** entre dos extremos de una conexión por conmutación de circuitos establecida, como por ejemplo las centrales origen y destino de una llamada.
- **Situación (B):** entre dos SPs que no estén interconectados por una conexión de conmutación de circuitos.

Para la señalización extremo a extremo se implementan dos métodos:

- **Método paso de Largo (pass along):** utilizado sólo para la situación (A), donde *ISUP utiliza MTP* directamente. Utilizado para el traspaso de señalización relacionada con la conexión existente. En el establecimiento de una llamada se constituye tanto el circuito como la conexión SS7 extremo a extremo, donde dicha conexión extremo a extremo consiste en un número de secciones de conexión. Se envía a través de la ruta de señalización de una conexión previa, establecida a la vez que se estableció el circuito. El mensaje pasa a lo largo de las centrales de tránsito que constituyen la ruta del circuito,sin que se produzca procesamiento de la información en las centrales de tránsito, únicamente reenvío.
- **SCCP:** válido en ambas situaciones (A) y (B), donde *ISUP utiliza SCCP*. Puede usarse tanto si existe un circuito establecido entre las centrales origen y destino del mensaje como si no. La ruta seguida por el mensaje estará determinada por SCCP. Puede no estar relacionada con ningún circuito de usuario.

3.5.4. Servicios ISUP

ISUP ofrece capacidades para soportar servicios básicos y servicios suplementarios. Sus principales características son:

- **Básicos:** ISUP ofrece establecimiento y liberación de llamadas por conmutación de circuitos.
- **Suplementarios:** ISUP proporciona numerosos mensajes y parámetros que han sido específicamente creados para soportar servicios suplementarios a través de la red. ISUP ha ayudado a estandarizar el uso de servicios, permitiendo la interoperabilidad entre distintas redes y proveedores de servicios. Las características de los servicios pueden variar según las distintas redes o mercados, e ISUP posee capacidad para adaptarse a todos ellos, ya que posee un amplio abanico de mensajes, así como de parámetros opcionales para ellos.

  Los principales servicios suplementarios soportados en ISUP son:

  - *Identificación de línea llamante* (presentación o restricción).
  - *Desvíos:* incondicional, si la línea llamada esta ocupada, si no contesta, ...
  - *Grupo cerrado de usuarios:* acceso de salida, de entrada, prohibición de llamadas entrantes, salientes, ...
  - *Marcación directa de extensiones.*
  - *Señalización usuario a usuario*(UUS1, UUS2, UUS3).

A pesar de que ISUP posee una gran capacidad de soporte para servicios, sí hay que destacar que es un sistema actualmente *no extensible*, pues tanto los mensajes como los parámetros tienen un formato cerrado y es difícil hoy día dar cabida a nuevos servicios.

3.5.5. Portabilidad

Históricamente los números de teléfono han estado asociados a una zona geográfica o región concreta o bien a un operador específico, situación que ha ido perdiendo sentido progresivamente tras la introducción de las portabilidades, numéricas o geográficas, con lo cual el número de teléfono deja de ser útil para encaminar.

La *portabilidad del número local (Local Number Portability, LNP)*, la única que estudiaremos, es el concepto de tener un número de teléfono que permanece invariable para el abonado, a pesar de que éste cambie de proveedor de servicio.

En este escenario, distinguimos dos tipos de operadores, el *donante* (red donante), que es aquel que originalmente poseía el número, y el *receptor* (red receptora), que es el operador que actualmente acoge al usuario con su número.

A continuación estudiaremos los diferentes mecanismos utilizados para proporcionar la portabilidad de servicios (numérica en este caso) y como estos mecanismos se implementan durante el establecimiento de llamadas en ISUP.

Actualmente hay cuatro mecanismos definidos para la implementación de la portabilidad numérica (recogidos en la Recomendación E.164 - Sup. 2): *el encaminamiento hacia adelante (OR), encaminamiento con retroceso (RTP), consulta tras la liberación (QoR) y consulta de toda la llamada (ACQ)*, que detallaremos a continuación:

- **Encaminamiento hacia adelante (OR: Onward Routing).** En el encaminamiento hacia adelante, se encamina la llamada hasta llegar a la red donante del número portado. La red donante no devuelve la llamada hacia la red originadora de la misma, sino que realiza la consulta a la base de datos de portabilidad para determinar el nuevo número de encaminamiento[14] asociado al número portado, y es la propia central de la red donante la que utiliza este nuevo número para encaminar la llamada.

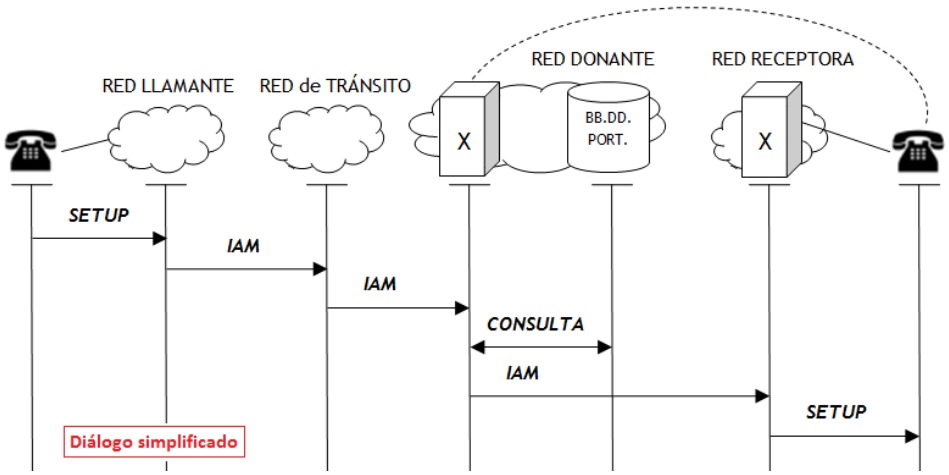

Figura 3.34: Portabilidad: Encaminamiento hacia adelante (OR)

[14]El número de encaminamiento se corresponde con un plan de numeración especial no visible al usuario.

- **Encaminamiento con retroceso (RTP: Release To Pivot).** La llamada se encamina nuevamente hasta llegar a la red donante que vuelve a realizar la consulta a la base de datos de portabilidad. En este caso, a diferencia del encaminamiento hacia adelante, la red donante no cursa la llamada, sino que devuelve un tipo de mensaje especial denominado mensaje de RETROCESO[15] a la central inmediatamente anterior. En el mensaje de RETROCESO se incluye el número de encaminamiento que puede utilizar la central para cursar la llamada hacia el número portado.

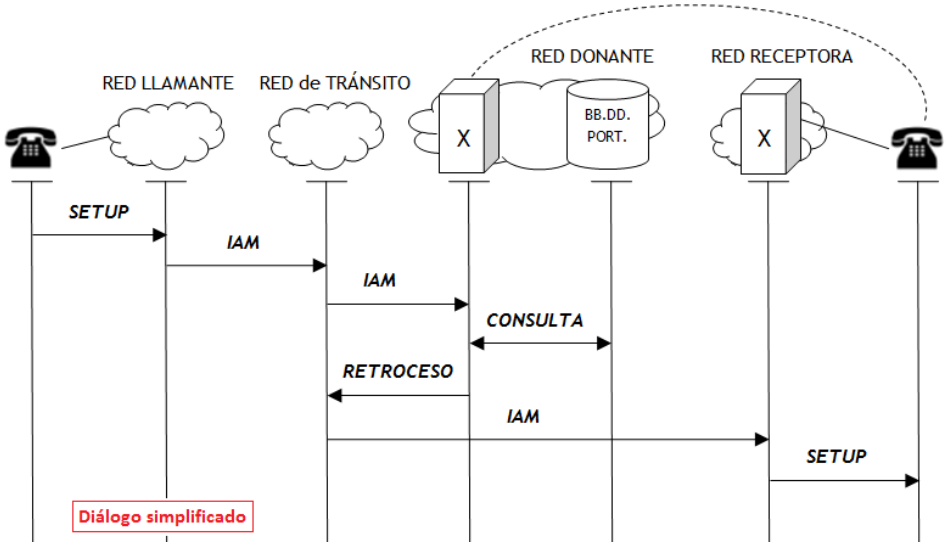

Figura 3.35: Portabilidad: Encaminamiento con retroceso (RTP)

- **Consulta tras las liberación (QoR: Query On Release).** QoR encamina la llamada desde la red originadora hacia la red donante del número portado de la misma manera que se hacía antes de existir la portabilidad numérica. La red donante libera la llamada de vuelta, incorporando en su mensaje de RELEASE[16], el parámetro de causa originadora *Number Portability QOR number not found*, con un valor de 14 (redes UIT) o de 27 (redes ANSI). Es por tanto la central o red inmediatamente anterior a la donante la que debe realizar la consulta a la base de datos de portabilidad, tras recibir el RELEASE, para determinar que número de encaminamiento utilizar en su mensaje IAM para poder alcanzar a la red receptora.

[15] Este mensaje es distinto al mensaje de RELEASE y por tanto no hay REL ni RLC, sino que directamente devuelve el número portado y libera automáticamente el circuito reservado en el IAM.

[16] Aquí sí será necesario el diálogo completo para liberación del circuito: RLC.

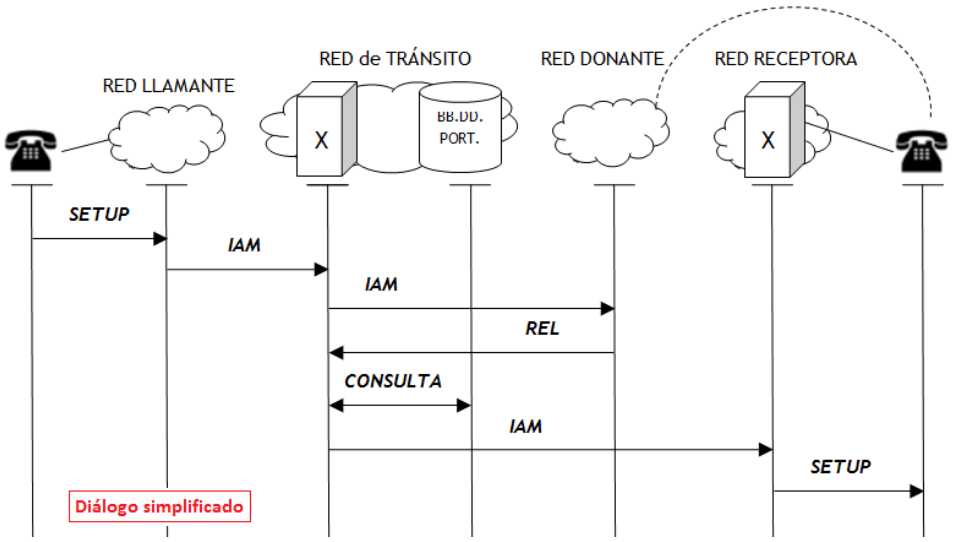

Figura 3.36: Portabilidad: Consulta tras las liberación (QoR)

- **Consulta de toda la llamada (ACQ: All Call Query).** Con la estrategia ACQ, es la red llamante la que directamente envía una consulta de red inteligente (INAP) a la base de datos de portabilidad para determinar la dirección física o la dirección de encaminamiento. El formato de respuesta de la base de datos varía según el estándar internacional de la red, pero la idea general es que es la red originadora de la llamada la que consulta y obtiene la información para encaminar la llamada.

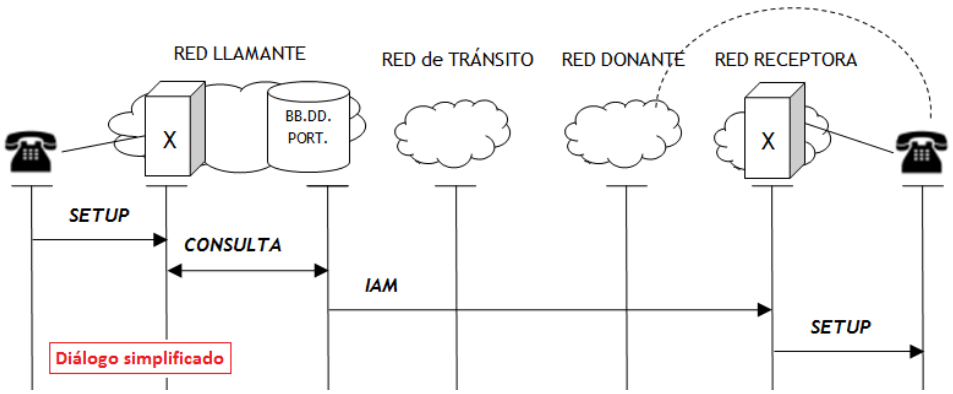

Figura 3.37: Consulta de toda la llamada (ACQ)

El encaminamiento hacia adelante se implementó para combatir las situaciones monopolistas, ya que este sistema es perjudicial para la operadora donante ya que mantiene un circuito ocupado sin obtener beneficio de la

llamada. El uso de QoR o RTP, implica el envío de un mensaje IAM y la recepción de un mensaje REL de vuelta desde la red donante, por lo que se hace necesario un reintento de llamada, es decir, un nuevo IAM desde la red originaria de la llamada. Los mecanismos ACQ y OR no liberan recursos ni requieren de reintentos de llamada. El mecanismo OR crea diálogos adicionales, ya que la llamada está siendo conectada a través de la red donante en lugar de realizarse directamente hacia la red receptora.

Aparte de estas conclusiones más o menos evidentes, cada uno de estos métodos tiene sus características específicas en cuanto a eficiencia, implicación de recursos, sostenibilidad y capacidad competitiva sobres las redes de los distintos operadores, aspectos, que evidentemente se escapan del contenido del manual.

En España para redes fijas, el operador mayoritario, Telefónica implementa QoR mientras que el resto hacen ACQ. En redes móviles todos los operadores utilizan ACQ. La base de datos de portabilidad es única e independiente para todas las compañías operadoras. Su gestión sale a concurso público y actualmente es (o al menos ha sido) mantenida por Informática el Corte Inglés (`http://www.ieci.es/`).

3.6. TCAP

La Parte de Aplicación de Capacidades de Transacción (*Transaction Capabilities Application Part, TCAP*) del protocolo SS7, recogido en las recomendaciones de la serie Q.700 de la UIT-T, permite a los servicios de los nodos de la red comunicarse entre ellos, utilizando un conjunto acordado de elementos de datos. Anteriormente a SS7, uno de los problemas en la implementación de los servicios de conmutación más allá de los límites de la conmutación local era la naturaleza propietaria de las centrales de conmutación. Además, los circuitos de voz tenían poca capacidad para la información de señalización con lo cual no era posible implementar estos servicios. La aparición de los sistemas de señalización por canal común, con una capacidad propia para la señalización de la red permitió tener la capacidad de transferencia de información para una gran cantidad de servicios.

TCAP proporciona en SS7 una interfaz genérica entre servicios que está basada en el concepto de *componentes*. Los componentes entienden las instrucciones que las aplicaciones de servicio intercambian en los diferentes nodos de la red.

TCAP se utiliza pues para el intercambio de mensajes no relacionados con circuitos sino principalmente para entidades relacionadas con bases de

datos y sistemas centralizados (consultas). Proporciona un entorno orientado a conexión y transferencia fiable de información entre dos aplicaciones distribuidas en una red, por ejemplo una aplicación situada en una central local y otra en una entidad de la red, típicamente el *Service Control Point SCP*, encargado del servicio de traducción de números 900(800), en el que al contratar un número de este tipo, no se identifica un área geográfica para el encaminamiento sino que se necesita un número extraído de una base de datos. Cualquier abonado (operador) puede originar la llamada y teniendo en cuenta que el número 900 (800) puede ser portable a cualquier otro operador.

Así pues, TCAP es un conjunto de protocolos y servicios, que se encuadran en el nivel de aplicación OSI, para la realización de operaciones remotas, principalmente diálogos entre bases de datos, alineado con ROSE (Remote Operations Service) de OSI. Proporciona transferencia de información entre centrales no relacionada con ningún circuito permitiendo la transferencia de señalización extremo a extremo.

Las aplicaciones típicas donde se usa TCAP mayoritariamente son:

- *Servicios asociados a Red Inteligente (INAP):* números 90X (80X), bases de datos de información de línea (tipo de abonado, servicios contratados, ...), servicios suplementarios (desvíos, rellamada automática, ...), activación/desactivación remota de facilidades y servicios en otra central, portabilidad, ...
- *Redes celulares (MAP):* gestión de la itinerancia (roaming), controlando el acceso a HLR, VLR, intercambio de actualización entre ambas.

La funcionalidad de TCAP es ofrecer un medio para que usuarios finales SS7 accedan a otros usuarios finales, siempre en una relación entre pares, entendiendo por usuario final en SS7 una aplicación dentro de una entidad de red.

3.6.1. Estructura TCAP

TCAP, tal y como se muestra en la figura 3.38 está organizado en dos subcapas, la *subcapa de componente* y la *subcapa de transacción*, así en cada mensaje TCAP habrá una parte destinada a cada una de las subcapas.

Una transacción es un conjunto de mensajes TCAP relacionados intercambiados entre los nodos de la red. La subcapa de transacción identifica los mensajes que pertenecen a la misma transacción utilizando para ello un identificador de transacción (Transaction ID, TRID). La parte de componente contiene las instrucciones u operaciones actuales, que están siendo

enviados a la aplicación remota.

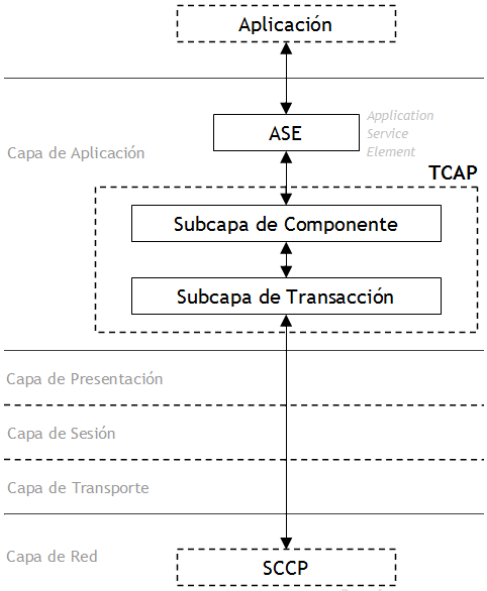

Figura 3.38: Estructura TCAP

La subcapa de componente se responsabiliza del intercambio de componentes entre usuarios TCAP. Una componente es equivalente a una PDU de ROSE, es decir, una solicitud de una acción (invocación de un proceso) en el extremo remoto o bien, los datos indicando la respuesta a la operación requerida. Por ejemplo, componentes son la pregunta y la respuesta que nos va a dar la base de datos de portabilidad cuando se le hace una consulta para encaminar.

La subcapa de transacción se responsabiliza del intercambio de mensajes que contienen o transportan los componentes. Se encarga por tanto del establecimiento y gestión del diálogo (transacción) entre los usuarios TCAP.

Subcapa de Transacción

Definiremos en primer lugar un **diálogo**, como una asociación entre dos usuarios de TCAP mientras que definimos una **transacción** como una asociación entre dos subcapas de transacción pares, definiendo el contexto de una operación remota al completo.

Una transacción es pues un conjunto de mensajes interrelacionados que son intercambiados entre procesos de aplicación en dos nodos diferentes de una red SS7, como por ejemplo un intercambio de consultas y respuestas entre usuarios. En un instante determinado, un nodo puede mantener múltiples

transacciones simultáneas activas, enviando y recibiendo múltiples mensajes TCAP.

En TCAP existe pues una correspondencia biunívoca entre diálogos y transacciones, salvo en el caso de un diálogo no estructurado[17], que incluso carece de identificador de transacción.

La subcapa de transacción es responsable de la gestión del diálogo, utilizando para ello los servicios sin conexión que ofrece SCCP, definiéndose dos tipos de diálogo entre subcapas de transacción:

- **Diálogo no estructurado:** utilizando los servicios SCCP clase 0, el usuario TCAP envía a su usuario par una o más componentes que no requieren respuesta, como por ejemplo actualizar la posición en TE móvil. Las componentes enviadas son empaquetadas en mensajes unidireccionales, por lo que no se establece una asociación explícita.
- **Diálogo estructurado:** usa los servicios clase 1 de SCCP.
  - TC-BEGIN por parte del usuario TCAP conteniendo un identificador de diálogo a la subcapa de componente. Todas las sucesivas componentes contendrán el mismo identificador de diálogo (dialogue ID).
  - TR-BEGIN por parte de la subcapa de componente conteniendo un identificador de transacción (transaction ID), estableciendo una correspondencia entre transaction ID y dialogue ID.

Subcapa de Componente

La subcapa de componente se basa en la especificación X.410 para Operaciones Remotas en Sistemas de Manejo de Mensajes, sustituida posteriormente por la recomendación ITU X.229.

Un componente es un medio para invocar una operación en un nodo o servicio remoto, es decir es una solicitud de operación o bien una respuesta.

Un mensaje TCAP puede contener varias componentes, que invoquen varias operaciones de manera simultánea, aunque sólo se puede emitir una respuesta a una solicitud. El usuario puede enviar varias componentes antes de que la subcapa las transmita en un mensaje. En el otro extremo dichas componentes se entregan individualmente y en orden.

[17] Envío unidireccional de información, también denominado diálogo degenerado.

Así, el diálogo lo forman la secuencia de componentes, donde hemos de tener en cuenta que se permiten varios diálogos simultáneamente.

Es necesaria una función de asociación entre solicitud y respuesta, para ello se utilizará un identificador de invocación único (Invoke ID) pudiendo existir varias invocaciones de la misma operación simultáneamente, que se corresponderán a mútiples Invoke IDs.

Se definen cuatro Unidades de Datos de Protocolo Operacionales (Operation Protocol Data Unit, OPDU), es decir, cuatro tipos de componentes:

- **INVOKE:** solicita una operación para ser realizada. Distinguimos a su vez:
  - *Clase 1:* se informa tanto si hay éxito como si hay fracaso en la ejecución.
  - *Clase 2:* sólo se informa en caso de fallo.
  - *Clase 3:* sólo se informa en caso de éxito.
  - *Clase 4:* no se informa en ningún caso, ni del éxito ni de fracaso.-.
- **RETURN RESULT:** informa de la ejecución con éxito de una operación previamente solicitada.
- **RETURN ERROR:** informa de la ejecución sin éxito de una operación previamente solicitada.
- **REJECT:** informa de una violación del protocolo, como por ejemplo una OPDU incorrecta o mal formada (error de sintaxis).

Es decir, tenemos definidas cuatro operaciones remotas, las cuatro clases de INVOKES y tres posibles respuestas a dichas operaciones, RETURN RESULT, RETURN ERROR y REJECT. En TCAP se admite la *segmentación* de la respuesta, algo que no se permite en el estándar ROSE.

Cada uno de los tipos de componentes de TCAP se correlaciona directamente con una de los cuatro tipos de OPDU. Las componentes INVOKE and RETURN RESULT se utilizan para el manejo de mensajes en un funcionamiento normal entre usuarios TCAP mientras que RETURN ERROR y REJECT se utilizan como es lógico para el manejo de errores.

Los contenidos de las componentes INVOKE y RETURN RESULT incluyen la siguiente información: Tipo de Componente, Identificador de Componente, Código de Operación (únicamente en INVOKE) y Parámetros.

Los contenidos de las componentes RETURN ERROR y REJECT son similares a las anteriores, exceptuando que el código de operación usado en INVOKE es reemplazado por un código de error.

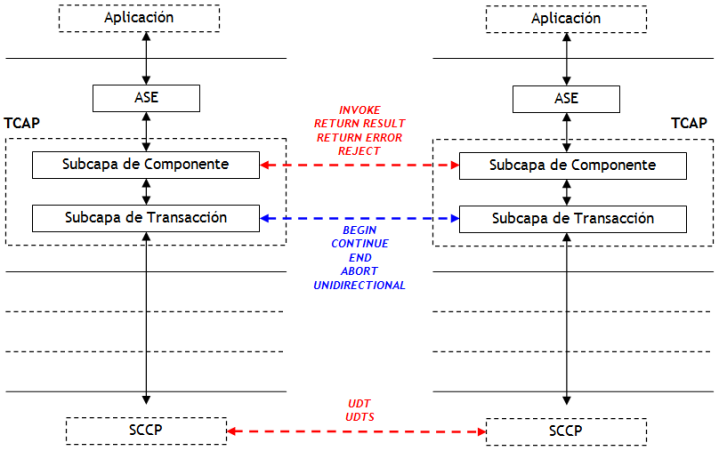

Figura 3.39: Mensajes subcapa TCAP

3.6.2. Mensajes TCAP

Los mensajes TCAP, cuya estructura se muestra en la figura 3.40, se dividen en tres secciones distintas, a saber, *porción de transacción*, *porción de componente* y una *porción de diálogo*, opcional.

La **porción de transacción** identifica la naturaleza de la transacción y permite encaminar la información de componente a su destino. Contiene la identificación de transacción (transaction ID) como referencia para el seguimiento de mensajes TCAP.

Por su parte, la **porción de componente**, obtiene su información de la OPDU recibida de la aplicación. La OPDU, como hemos visto, contiene las primitivas y los parámetros necesarios para invocar una operación o solicitar servicios de otra entidad, como por ejemplo una consulta a una base de datos.

3.6.3. Ejemplo de uso de TCAP

En las figuras 3.41 y 3.42 se muestra el diálogo correspondiente a un ejemplo sencillo de uso de TCAP para el tratamiento de una llamada de tarificación premium, tipo 806, donde se han suprimido los mensajes en las interfaces de usuario RDSI, para no complicar excesivamente los diagramas.

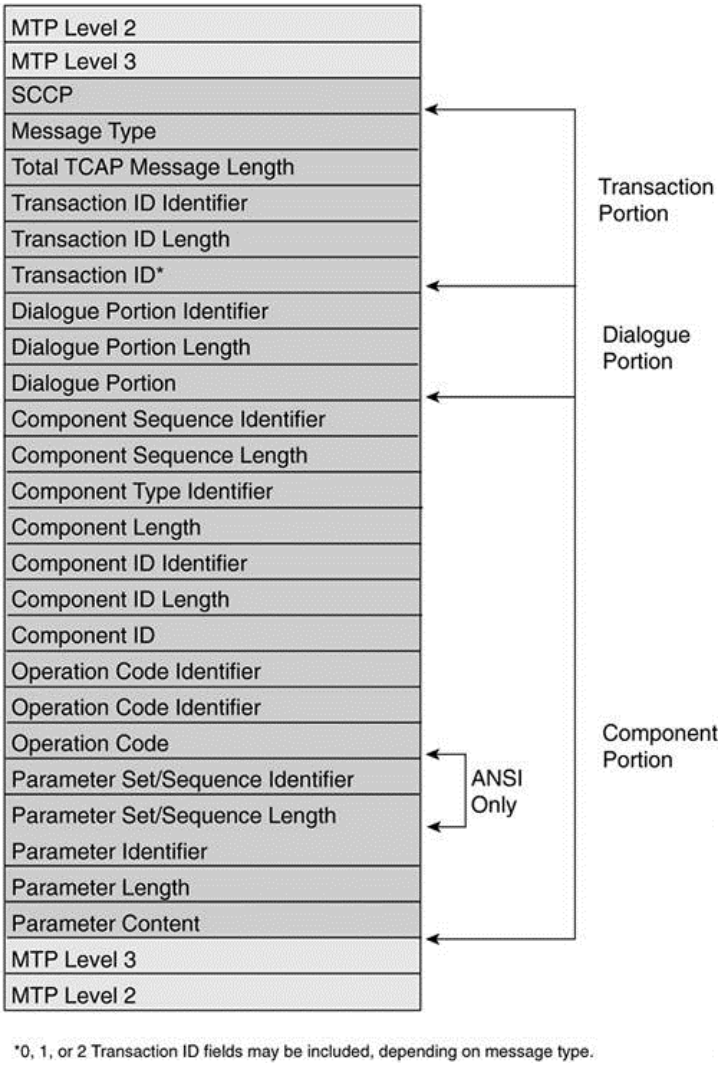

Figura 3.40: Estructura mensajes TCAP

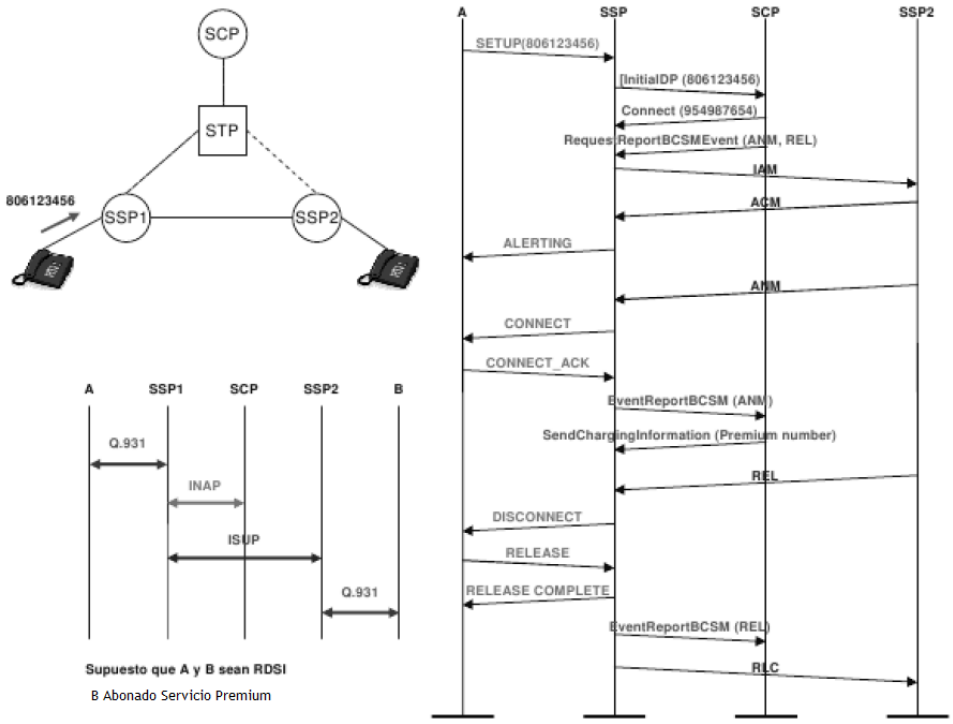

Figura 3.41: Escenario ejemplo uso TCAP (I)

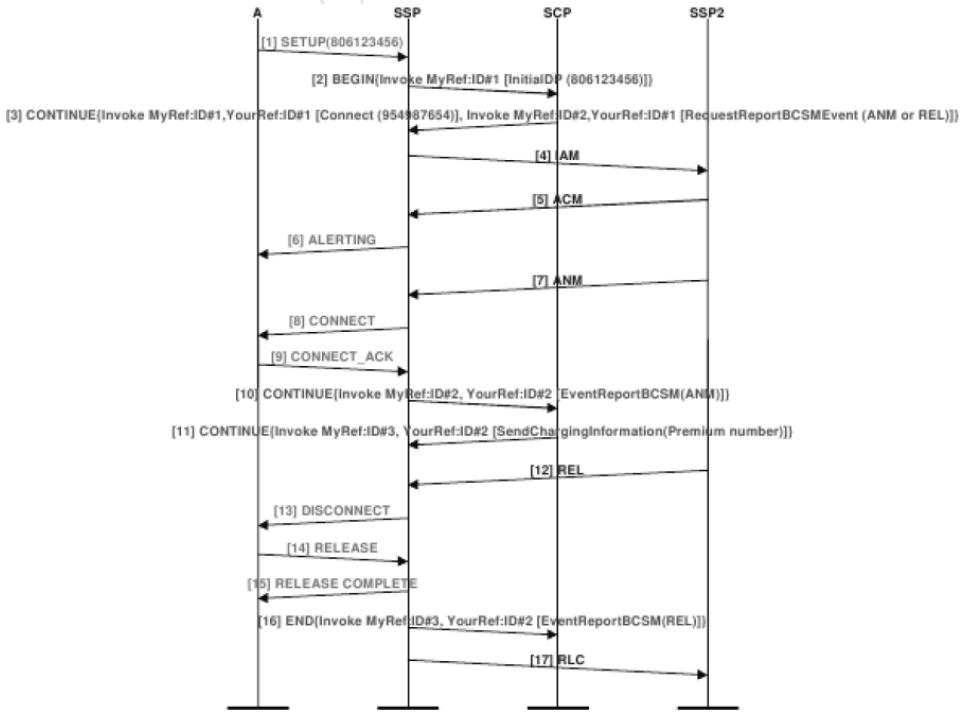

Figura 3.42: Escenario ejemplo uso TCAP (II)

3.7. MAP

En este apartado final realizaremos en primer lugar una introducción al sistema GSM, conocido estándar para redes móviles celulares, repasando su arquitectura y principales interfaces, para proceder posteriormente a estudiar el protocolo MAP, utilizado en GSM y UMTS y finalizar el tema con una serie de ejemplos de gestión de movilidad y localización en una red móvil usando MAP.

3.7.1. GSM: Global System for Mobile Communications

GSM es un estándar formulado por el European Telecommunication Standard Institute (ETSI). La primera fase de las especificaciones de GSM data de 1990, y su operación comercial, explotando la banda de 900 MHz comenzó en 1991. Ese mismo año apareció un derivado de GSM, conocido como Digital Cellular System 1800 (DCS 1800), que trasladó o extendió GSM a la banda de 1800 MHz.

Las redes móviles previas a GSM eran sistemas analógicos que variaban entre los distintos países, que adoptaron distintos estándares, por ejemplo en Estados Unidos se adoptó AMPS (Advanced/American Mobile Phone service) mientras que en el Reino Unido se utilizó TACS (Total Access Communicatin System). Con tanta variedad de estándares era imposible poder operar con un único terminal en diferentes países, reduciendo la operatividad y movilidad de los mismos.

Como problemas añadidos a la naturaleza analógica de los sistemas encontramos una calidad de servicio relativamente pobre, la inexistencia de servicios suplementarios, falta de seguridad/privacidad en las comunicaciones, etc.

Situación que mejoró en la calidad y capacidades del servicio con la salida al mercado del estándar GSM que se realizó en diferentes fases, aumentando sus funcionalidades y servicios de manera progresiva, hasta extenderse a un total 509 redes GSM operando en 182 países, con un total de 684 millones de abonados (datos extraídos de GSM Association, 2004).

Arquitectura de Red GSM

La arquitectura de GSM se puede dividir en tres áreas funcionales:

- *BSS:* Base Station Subsystem
- *NSS:* Network Switching Subsystem
- *OSS:* Operations Support Subsystem

En la figura 3.43 se recoge la arquitectura general de una red GSM, donde se ilustra el alcance de las entidades que componen cada uno de los subsistemas.

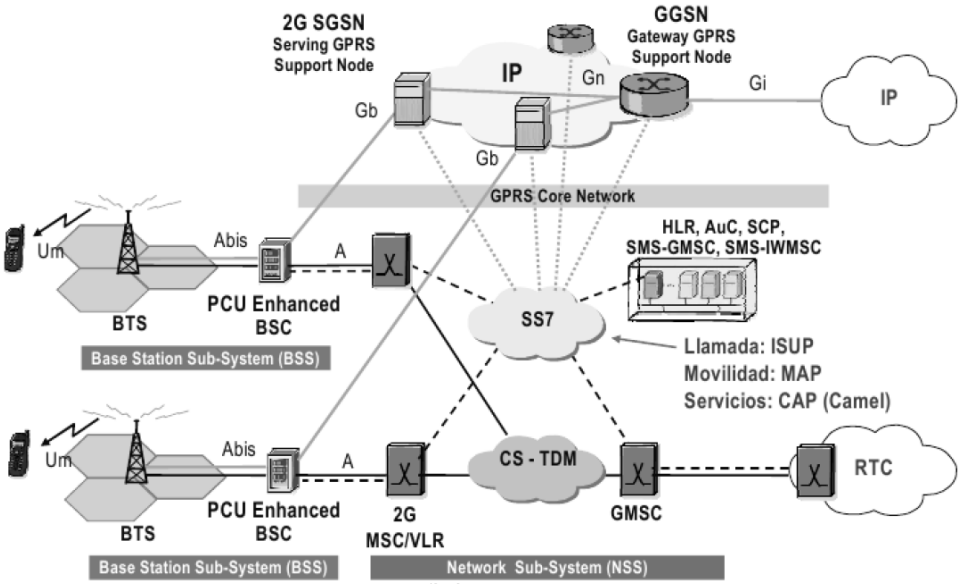

Figura 3.43: Arquitectura Sistema GSM

En la figura se recoge además el acceso a datos mediante GPRS (General Packet Radio Service), añadido posteriormente al estándar GSM formado por una red IP propia de la operadora donde se transportan encapsulados el tráfico de datos de los usuarios, sin alterar en ningún caso el segmento radio.

Centrándonos exclusivamente en el sistema GSM, el BSS está compuesto por BTS (Base Transceiver Station) y el BSC (Base Station Controller) y se encarga de proporcionar el medio de transmisión entre las MS (Mobile Stations) y el siguiente subsistema, el NSS, gestionando los canales de trasmisión.

El subsistema NSS es el cerebro de la red GSM, y está formado por el MSC (Mobile Switch Center) a los que se suman cuatro nodos inteligentes de red, conocidos como HLR (Home Location Register), VLR (Visitor Location Register), EIR (Equipment Identity Register) y el AuC (Authentication Center).

El último subsistema OSS está formado únicamente por los OMCs (Operation and Maintenance Centers), utilizados para tareas de operaciones remotas y centralizadas, administración y mantenimiento. El OSS proporciona los medios para que el proveedor de servicio pueda controlar y gestionar la

red. El OSS es normalmente un sistema propietario y no tiene por tanto interfaces normalizadas, por lo cual no volveremos a incidir sobre él, ya que su estudio carece de interés en nuestro contexto.

El subsistema BSS es la parte radio de la red móvil, algo en lo que no entraremos y su estudio en este contexto se justifica pues es en este subsistema donde se utiliza el protocolo MAP. Repasaremos a continuación cada uno de los elementos que componen la arquitectura GSM completa:

- **Mobile Station (MS).** En GSM se denomina a los equipos terminales como MS. Aparte de los teléfonos móviles también podemos incluir las tarjetas PCMCIA que se usan/usaban en PCs portátiles, que permitían la transferencia de datos por la red GSM. Es importante destacar, que según el estándar el MS está formado por el equipo términal del usuario más la tarjeta inteligente llamada SIM, que permite identificar al abonado en la red (MS = Equipo Móvil + SIM).

  En GSM es posible utilizar la tarjeta SIM para poder separar la identidad del usuario del equipo terminal. Así, la SIM es totalmente intercambiable entre distintos equipos móviles (ME). EL MS tiene asociadas distintas entidades que repasamos a continuación y que intervienen en los procesos de señalización en la red:

  - *IMEI (International Mobile Equipment Identity):* cada equipo móvil tiene un IMEI almacenado en él de forma permanente, no es únicamente un número de serie, sino que además identifica al equipo móvil con un código que contiene fabricante, fábrica y país de fabricación. Permite realizar un control sobre usos fraudulentos del terminal y permite realizar un control de acceso a la red por motivos técnicos.
  - *IMSI (International Mobile Subscriber Identity):* identifica al abonado con un código que incluye país, red base y abonado. Está físicamente almacenado en el SIM, proporcionado por el operador.
  - *TMSI (Temporary Mobile Subscriber Identity):* es un alias utilizado por el VLR (y por el SGSN en redes con GPRS habilitado) que permite proteger la confidencialidad del abonado. Se utiliza de manera temporal como sustituto del IMSI para limitar el número de veces que el IMSI es retransmitido por la interfaz radio, ya que el IMSI puede ser utilizado para identificar a un abonado GSM. El TMSI se utiliza durante el procedimiento de actualización de posición, que veremos más adelante. Tanto el VLR como el SGSN deben ser capaces de correlacionar un TMSI asignado con el IMSI del MS al cual está asignado. El VLR asigna el TMSI al MS durante la transacción inicial del abonado con

el MSC (por ejemplo, al realizar una actualización de posición). Es importante destacar que el TMSI únicamente tiene significado local, en el área controlada por el VLR. Una práctica interesante para evitar asignaciones dobles en situaciones de error es hacer una parte del TMSI asignado dependiente del tiempo.

- *MSISDN (Mobile Station Integrated Services Digital Network):* es el número de teléfono que la parte llamante marca para alcanzar a la parte llamada, es decir, es el número de teléfono del abonado GSM. Como detalle, destacar que puede haber más de un número de teléfono asignado a una misma SIM.
- *MSRN (Mobile Station Roaming Number):* utilizado para encaminar la llamada. Es un identificador local temporal, que permite encaminar una llamada de la puerta de enlace MSC hacia el MSC/VLR en servicio. El MSC/VLR en servicio es el MSC/VLR de la zona en la que el usuario está actualmente posicionado. El VLR asigna un MSRN cuando recibe una petición de información de encaminamiento desde el HLR. Cuando la llamada finaliza, el MSRN es liberado de vuelta al VLR.

- **Base Transceiver Station (BTS).** Contiene los transceptores radio y maneja la interfaz radio, es decir, proporciona la conectividad o acceso entre los MS y el resto de la red móvil.

- **Base Station Controller (BSC).** Un número de BTSs están conectadas a un mismo BSC, por la interfaz Abis. Gestiona los radiocanales, encargándose de funciones como la configuración, liberación, saltos en frecuencia y traspasos (handovers).

- **Mobile Switching Center (MSC).** Es el componente central del subsistema de red. Básicamente es un conmutador RDI que está conectado a los BSCs mediante la interfaz A. Proporciona encaminamiento de llamadas entrantes y salientes y asigna canales de usuario sobre la interfaz A. Es decir, son las centrales de conmutación de las redes móviles.

  Las MSCs implementan por tanto ISUP para controlar los circuitos necesarios entre ellas y el GMSC para establecer conversaciones.

  Actúa como un nodo normal de una red RTC o RDSI, estando por supuesto preparadas para sooportar toda la funcionalidad necesaria para el manejo de una MS, incluyendo las tareas de registro, autenticación, actualización de posición, traspasos entre MSCs y encaminamiento de llamadas para abonado móvil. Junto con el HLR y el VLR, proporcio-

nan las capacidades de encaminamiento de llamadas y de itinerancia en GSM.

- **The Gateway Mobile Switching Centre (GMSC).** Es un tipo especial de MSC que actúa como pasarela para otras redes públicas.

- **Home Location Register (HLR).** Es una gran base de datos que contiene los datos administrativos y de localización de los abonados. Aunque desde un punto de vista lógico existe un único HLR en una red GSM, físicamente puede implementarse como una base de datos distribuida. La localización de cada MS asociada a un VLR es almacenada para poder enrutar llamadas a los abonados suscritos a dicho VLR. La información de localización es simplemente la dirección VLR que actualmente sirve al abonado. Es decir, el HLR almacena en qué VLR está suscrito cada terminal móvil en cada instante. Si por ejemplo se pretendiese llamar a un terminal se debe consultar al HLR para saber hacia qué VLR encaminar la llamada[18]. El HLR no tiene por tanto control directo sobre los MSCs. Dos números están asociados a cada suscripción de MS que se almacenan en el HLR son el IMSI y el MSISDN. El HLR también almacena información adicional, incluyendo información de localización (VLR), servicios suplementarios, información de suscripción de servicio básico, restricciones de servicio (como permisos de roaming), tipo de abonado (contrato o prepago), ...

- **Visitor Location Register (VLR).** Como el HLR, el VLR contiene datos del abonado. Sin embargo, almacena un subconjunto (información administrativa específica) de los datos necesarios para el control de llamadas y otros de provisión de posibles servicios de cada terminal actualmente localizado en el área geográfica controlada por el VLR. Los datos del VLR son almacenados temporalmente mientras el abonado se encuentra bajo su área de influencia. Un VLR es responsable para uno más MSCs. Cuando un usuario llega a un área de influencia de un nuevo MSC se inicia un procedimiento conocido como actualización de posición. Cuando el abonado abandona la zona de influencia servida por el VLR, el HLR solicita al VLR que remueva los datos de usuario que tenía almacenados, tal y como veremos en el ejemplo final del protocolo MAP.

  A pesar de que un VLR puede ser implementado como una unidad física independiente, hoy día, la mayoría de fabricantes de hardware de equipamiento de conmutación implementan los VLRs junto con

[18] Esta consulta se realiza incluso si la llamada es realizada entre dos terminales suscritos al mismo VLR.

el MSC, teniendo el control completo de una zona geográfica en un mismo equipo con la dupla MSC/VLR. La proximidad entre el VLR y el MSC acelera los intercambios de información que se requieren durante la llamada, motivo extra para implementarlos juntos.

- **Equipment Identity Register (EIR).** Es una base de datos que contiene una lista de de los equipos móviles válidos en la red. Contiene pues una lista de IMEIs, que son marcados como válidos o inválidos, en caso de haber sido informados de su robo o uso fraudulento.

- **Authentication Center (AuC).** Es una base de datos protegida que almacena una copia de las claves privadas almacenadas en las SIMs de los abonados y que son utilizadas para labores de autenticación y cifrado en la interfaz radio.

- **Serving GPRS Support Node (SGSN).** Conmutador responsable de la entrega de paquetes al terminal móvil en su área geográfica de servicio. Entre sus tareas encontramos transferencia y encaminamiento de paquetes, gestión de movilidad, gestión de enlace lógico y labores de autenticación y cobro. Almacena información de localización (como la célula y VLR actuales del terminal) y perfiles de usuario (como IMSIs y direcciones usadas en la red de paquetes) de todos los usuarios GPRS registrados en el SGSN.

- **Gateway GPRS Support Node (GGSN).** Conmutador de paquetes responsable de encapsular los paquetes al SGSN apropiado y encargado del acceso a redes y servicios. Es función suya por ejemplo asignar una dirección IP pública[19] a cada terminal móvil para permitir el acceso a Internet.

Es interesante hacer al menos referencia a las interfaces y protocolos que se utilizan en la red GSM ente los distintos elementos que componen su arquitectura. Los protocolos SS7 como MTP, SCCP, ISUP fueron definidos antes de la aparición de las redes digitales móviles, con lo que pudieron utilizarse en GSM, aunque luego fue necesario definir nuevos protocolos, como MAP, adaptados para la particular naturaleza de este tipo de redes.

La tabla 3.9 recoge las interfaces y protocolos que intervienen en una red GSM.

En términos de capa física, la interfaz Abis (BTS-BSC) utiliza un canal de 64 Kb/s sobre cualquier medio físico conveniente en cada instalación concreta (cableada, óptica o radioenlace). El resto de interfaces en GSM utilizan

[19] Por lo tanto no hace NAT.

Interfaz	Entre	Descripción
Um	MS - BSS	En la interfaz radio se utiliza señalización mediante LAPDm, una modificación del LAPD de RDSI.
Abis	BSC - BTS	No estandarizado.
A	BSS - MSC	Gestiona la reserva de recursos radio para las MSs y la gestión de movilidad. Utiliza los protocolos BSSAP.
B	MSC - VLR	Utiliza MAP/B para la señalización entre ambos. Normalmente esta interfaz es interna en la dupla MSC/VLR.
C	GMSC - HLR ó SMSG - HLR	Utilizada para señalizar llamadas fuera de la red GSM mediante el protocolo MAP/C. También se usa para información de facturación.
D	HLR - VLR	Protocolo MAP/D para intercambiar datos de localización y del abonado.
E	MSC - MSC	Protocolo MAP/E para señalizar el handover entre MSCs.
F	MSC - EIR	Protocolo MAP/F para verificar el estado del IMEI que el MSC ha obtenido del MS.
G	VLR - VLR	Protocolo MAP/F para tansferir informacón de abonado, por ejemplo durante el procedimiento de actualización de posición.
H	MSC - SMSG	Protocolo MAP/H para soportar el envío de mensajes cortos.
I	MSC - MS	Los mensajes en la interfaz I se reenvía de forma transparente a través de la BSS.

Tabla 3.9: Interfaces y Protocolos en GSM

SS7/MTP1 como capa física.

La capa de enlace usada en la interfaz radio es LAP-Dm mientras que en la interfaz Abis (BTS-BSC) se utiliza LAP-D. El resto de interfaces de GSM utilizan SS7/MTP2 en su nivel de enlace.

Respecto a los niveles de red, decir que en interfaz radio es inexistente mientras que en el resto de interfaces se implementa mediante SS7/MTP3.

Las capas de transporte, sesión y presentación, no se utilizan en SS7, sino que las funciones necesarias se agrupan en la capa de aplicación, que en SS7 es conocida como hemos visto como el nivel 4. Las interfaces entre GSM y las redes fijas utilizan como es lógico ISUP ó TUP según el caso.

Se deja como ejercicio llegados a este punto, en pensar las torres de protocolos que implementan los principales elementos de la red GSM, como MSC, VLR, HLR, ... Para solucionar este ejercicio es importante pensar en las funciones y tareas de cada elemento, como por ejemplo *¿quién maneja circuitos? ¿quién realiza consultas? ...*

GSM ha sido uno de los estándares de mayor impacto y penetración, hasta tal punto que las redes móviles de tercera generación, como por ejemplo el sistema UMTS R99, siguen una filosofía en su arquitectura similar a la establecida por GSM, llegando a tener incluso equipamientos análogos, tal y como se recoge en la figura 3.44.

La modificación más importante a nivel de arquitectura es la inclusión de una interfaz adicional (el resto de interfaces se mantienen aunque con un cambio en su nomenclatura) respecto a GSM, la interfaz Iur. La interfaz Iur, conecta RNCs (Radio Network Controllers), que son los equivalentes a los BSCs en GSM, implementando canales tanto de datos como de señalización y permite que las redes UMTS ejecuten el denominado *soft-handover* o traspaso suave de células.

Otro importante cambio es la utilización de la tecnología ATM en la agregación de los distintos nodos B a su correspondiente RNC. Se incidirá sobre este aspecto en el capítulo 4, dedicado a la tecnología ATM.

GSM fue un estándar de amplísima aceptación, al que se le añadió GPRS para proporcionar el acceso a datos a terminales móviles con la premisa de no modificar el segmento radio. UMTS, nace como evolución de GSM, curiosamente con una premisa contraria, modificar y mejorar principalmente el segmento radio, manteniendo la arquitectura y filosofía de GSM en el núcleo de la red.

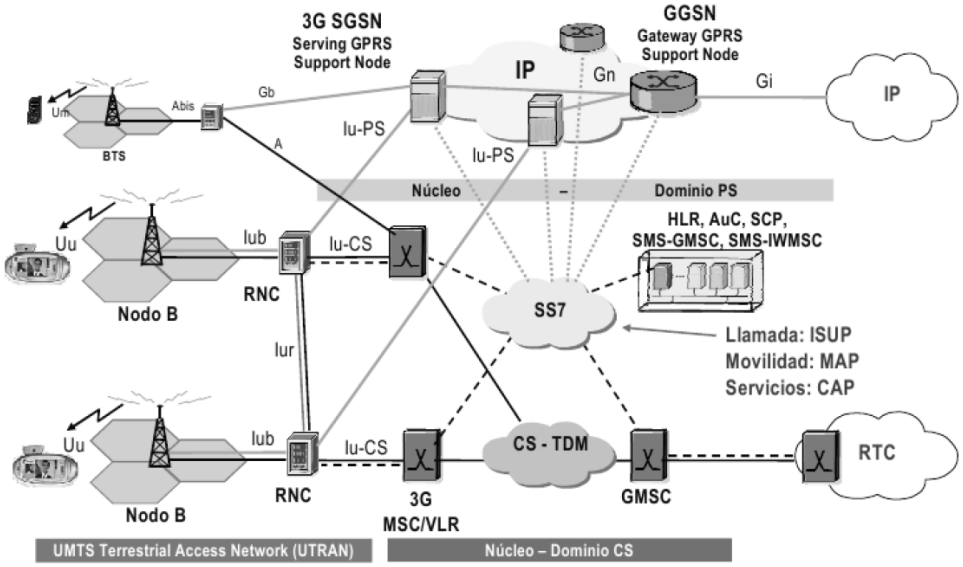

Figura 3.44: Arquitectura UMTS R99

De hecho, en la propia figura 3.44 se recoge también la actual coexistencia de ambos sistemas GSM/GPRS(2G) y UMTS(3G).

3.7.2. MAP: Mobile Application Part

El protocolo MAP es una extensión de SS7, que utiliza TCAP sobre SCCP y MTP, añadida para dar soporte a redes móviles celulares. Define operaciones entre componentes de red (como el MSC, BTS, BSC, HLR, VLR, EIR, MS y el SGSN/GGSN en GPRS) para la transferencia de información no relacionada con un circuito.

MAP permite la realización de tareas como:

- Actualización de la ubicación.
- Gestión del traspaso (handover entre diferentes VLRs (GSM) o RNCs (UMTS) e itinerancia (roaming).
- Soporte para la autenticación.
- Encaminamiento de las llamadas entrantes.
- Short Message Service (SMS).
- Operación y Mantenimiento.
- Control de llamada.

- Servicios suplementarios.

MAP especifica una serie de servicios, haciendo que la información fluya entre los distintos componentes de la red GSM para implementar dichos servicios.

Los protocolos MAP, recogidos en la figura 3.45 se designan como MAP/X según la interfaz X sobre la que se ejecuta el protocolo. Por ejemplo, la señalización MAP entre el GMSC y el HLR se denomina MAP/F.

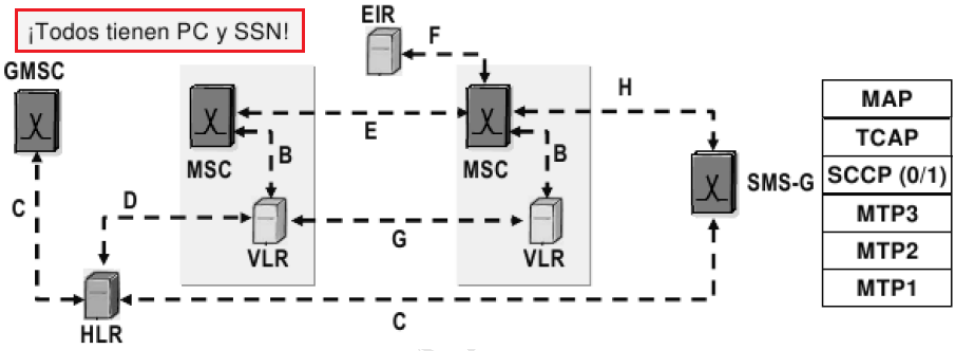

Figura 3.45: Protocolos MAP-X

Al ser una red SS7, es necesario decir que todos los elementos tienen asignado un código de punto (PC) y un número de subsistema (SSN) para cada protocolo MAP, que estaban recogidos en la tabla 3.4.

Para cerrar el tema, veremos un ejemplo de diálogo para la gestión de movilidad, donde se muestra una **actualización de localización** en la que un usuario en movimiento pasa de la zona de servicio de un VLR a otro diferente (handover).

El VLRb detecta en su zona un TE que se identifica como (TMSI, VLRa) por lo que da comienzo el diálogo entre los dos VLRs. El diálogo representado tiene lugar entre VLRs y el HLR, por lo que en ningún caso se produce en la interfaz radio.

Una vez que VLRb obtiene una confirmación simple de VLRa, solicita o invoca al HLR el procedimiento de actualización de la posición. Así, el HLR en primer lugar ordena a VLRa que elimine y libere los datos relativos al abonado/terminal para posteriormente enviar a VLRb la información del abonado/terminal.

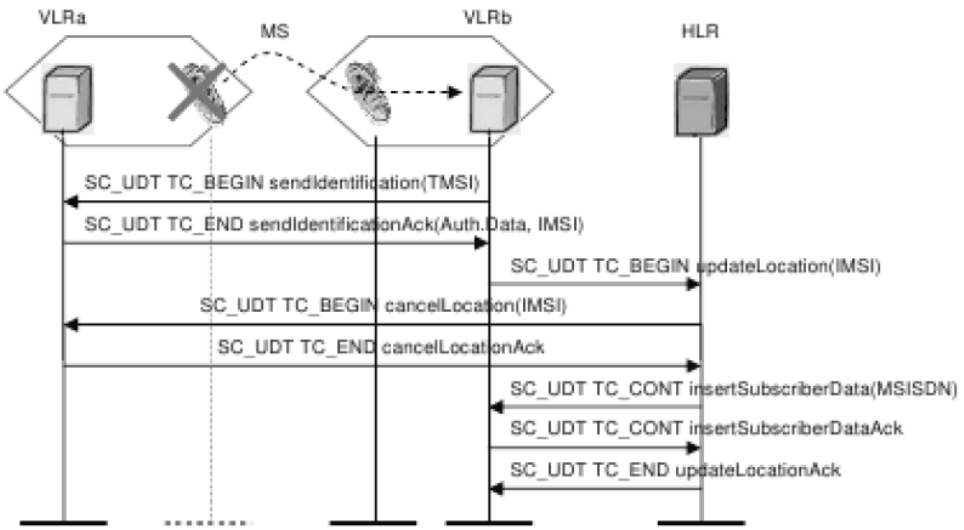

Figura 3.46: MAP: Ejemplo actualización localización

Capítulo 4

ATM y MPLS [1]

4.1. Introducción

A finales de los años 80, y con una tendencia continuamente alcista que se ha mantenido hasta hoy en día, se observaban continuos avances en todos los campos de la ciencia y la tecnología, situación que era particularmente visible en el campo de las telecomunicaciones, donde existía una continua demanda creciente de capacidades y aplicaciones cada vez más complejas.

Para poder desarrollar nuevos servicios, tales como videoconferencias o vídeo a demanda, así como mejorar el ancho de banda para el tráfico tradicional de datos, se desarrolló una nueva tecnología para servicios con diferentes requerimientos de anchos de banda.

Esta tecnología es el **Modo de Trasferencia Asíncrono o ATM (Asynchronous Transfer Mode)**.

En 1988, ATM fue elegido por la UIT-T como modo de transferencia preferente para las redes digitales de servicios integrados de banda ancha (B-ISDN). En 1990 se decidió finalmente basar los servicios B-ISDN en ATM y SONET/SDH (Synchronous Optical Network Systems/Synchronous Digital Hierarchy).

Para lograr una rápida estandarización y establecimiento en la industria, se creó el ATM Forum en octubre de 1991 que publicó sus primeras especificaciones tan sólo 8 meses después. El ATM Forum tenía como objetivo acelerar el uso de productos y servicios ATM buscando una mejor convergencia de las especificaciones en interoperabilidad. Además el ATM Forum pretendía promover la cooperación industrial y conciencia de mercado en torno a la tecnología ATM.

[1] Este capítulo está basado en los trabajos [10], [4], [8] y [3].

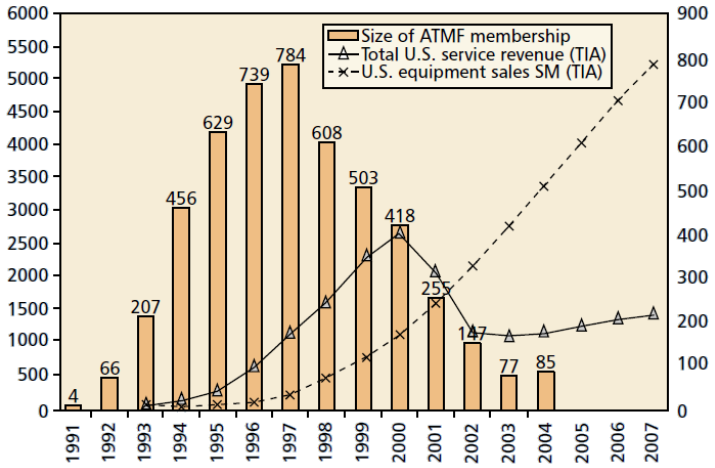

Figura 4.1: Evolución de equipos y servicios ATM

Como recoge la figura 4.1[2], la expansión de ATM tuvo su momento álgido a finales de los años 90, encontrándose actualmente en el final de su ciclo de vida, debido curiosamente al mismo motivo que originó su nacimiento, un nuevo incremento en las necesidades o capacidades de transmisión, que ATM ya no es capaz de soportar.

Sin embargo, ATM sigue teniendo una importancia notable en su uso en accesos tanto en tecnologías ADSL como UMTS, además de haber supuesto el punto de arranque para la tecnología MPLS (Multi Protocolo Label Switching) que estudiaremos al final de este mismo capítulo.

4.2. Principios generales de las redes ATM

A finales de los años 80, cuando se discutía el formato de las células ATM, dos importantes aspectos fueron tratados en intensos debates. El primero de ellos consistía en decidir si las células[3] ATM tendrían un tamaño fijo o variable, mientras que el segundo debate se centró en el tamaño apropiado de las células una vez que se resolvió el primero con la resolución de establecer un tamaño fijo de célula.

En el momento de tomar esas decisiones, e incluso hoy en día, la mayoría de las tecnologías de trasmisión de conmutación de paquetes utilizan un tamaño variable de trama o paquete, indicando la longitud del paquete

[2] `http://www.comsoc.org/files/Publications/Magazines/gcn/pdf/gcn1105.pdf`
[3] Las tramas ATM se denominan células.

en uno de los campos de cabecera del mismo.

Sin entrar en detalle, las tramas de tamaño fijo presentan dos inconvenientes fundamentales frente a las de tamaño variable:

1. Existe desperdicio de ancho de banda para el envío de paquetes de datos pequeños, pues al ser de tamaño fijo deben incluirse bits de relleno.

2. Es necesaria una capa extra de segmentación y reensamblado para el caso que los datos a transmitir excedan el tamaño máximo de célula, lo cual introduce más computación y retraso en comunicaciones.

A pesar de todo, se eligió un tamaño fijo de célula ya que ATM fue diseñado para comunicaciones tanto de voz como de datos, y es en este aspecto donde el tamaño fijo tiene una ventaja frente al variable, que consiste en la capacidad de mantener el retardo dentro de unos límites aproximadamente fijos, algo fundamental para la transmisión de voz.

Así pues, se decidió utilizar **células de tamaño fijo**, con un tamaño de **53 octetos**[4] repartidas en una **cabecera de 5 octetos** utilizando los 48 octetos restantes para carga útil. Es decir, se utilizó un formato de célula que desperdiciaba aproximadamente un 10 % de su capacidad en la cabecera.

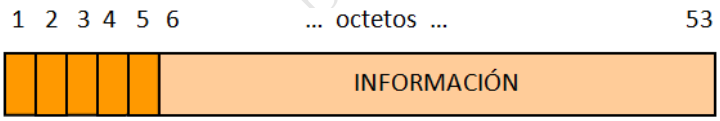

Figura 4.2: Célula ATM

En esencia, la disyuntiva entre tamaño fijo o variable fue una batalla entre el mundo de las telecomunicaciones vocales clásicas y el mundo de las comunicaciones de datos. El primero de ellos estaba preocupado por las variaciones en el retraso mientras que el segundo se preocupaba de la eficiencia de trasmisión. Al final, pareció triunfar el mundo de las comunicaciones, algo que era de esperar pues ATM estaba siendo diseñado principalmente por la UIT-T.

ATM se diseñó como una tecnología orientada a conexión[5] caracterizada por factores como:

- ATM implementa conexiones virtuales para la conmutación de células de un nodo a otro. Cada conexión virtual es definida mediante dos

[4] Interesante ver en la bibliografía recomendada [10] el por qué de este tamaño.
[5] Algo lógico ya que la cabecera es pequeña y no puede llevar dentro una dirección

identificadores, denominados Virtual Path Identifier (VPI) y Virtual Channel Identifier (VCI), que estudiaremos en detalle más adelante. Los valores VPI/VCI se transmiten en las cabeceras de las células y se conocen como identificadores de conexión.

- Células pertenecientes a una misma conexión virtual siguen el mismo camino, con lo que la secuenciación correcta está garantizada de forma implícita.
- El ancho de banda reservado para una conexión virtual se asigna al inicio en la configuración de la conexión y se basa en un compromiso entre las necesidades de la fuente de datos y la capacidad disponible.
- Cada conexión virtual se proporciona con una cierta calidad de servicio (QoS).
- Las conexiones son bidireccionales por naturaleza, aunque el ancho de banda puede ser asimétrico, llegando incluso a ser nulo en sentido de vuelta, lo que proporcionaría un enlace unidireccional.
- Los mismos valores de VPI/VCI se utilizan a través del enlace en ambas direcciones.
- Las conexiones pueden ser punto a punto o multipunto.

Las conexiones virtuales en ATM son establecidas de forma estática o dinámica. Una **conexión estática** se caracteriza porque los extremos de la conexión son definidos por adelantado con un ancho de banda determinado. Estas conexiones estáticas se establecen mediante suscripciones y se nombran como *Conexiones Virtuales Permanentes (Permant Virtual Connections PVC)*. Se gestionan en unos mecanismos previos a la comunicación y por lo tanto no requieren de señalización para su establecimiento.

Las **conexiones dinámicas** ofrecen mucha más flexibilidad. Se establecen cuando existen datos disponibles para ser trasmitidos y son liberadas cuando finaliza la transmisión. Se las conoce como *Conexiones Virtuales Conmutadas (Switched Virtual Connections SVC)*. Requieren por tanto del uso de señalización para establecerse, lo cual nos hace distinguir también entre conexiones de señalización y de usuario. Dichos procedimientos de establecimiento se estudiarán más adelante.

Se prefiere el uso de PVC cuando existe un flujo relativamente estable de datos entre dos puntos finales, mientras que las SVC se utilizan para comunicaciones breves o esporádicas de datos. La mayoría de proveedores de servicios sobre redes ATM generalmente ofrecen conexiones PVC únicamente, como ocurre en los accesos residenciales ADSL que estudiaremos en

el último capítulo.

Otra de las capacidades de ATM es su habilidad para proveer diferentes **Calidades de Servicio (Quality of Service QoS)**. La QoS de una conexión ATM puede centrarse en mantener unos mínimos exigidos en parámetros como pérdida de células, retraso de tránsito, variación de retraso, ... Es decir, garantizar una cierta QoS es garantizar que una conexión obtiene lo que requiere en términos de recursos de red para ser mantenida, como por ejemplo, garantizar QoS para una conversación vocal a máxima calidad es asegurar un retraso máximo menor de 50 ms con una tasa de 64 Kb/s para voz PCM.

De hecho, una de las mayores capacidades competitivas de ATM frente a sus competidores (como Frame Relay) es su capacidad de ofrecer varias QoS.

4.3. Arquitectura de Protocolos ATM

El actual modelo de referencia de ATM está definido en la recomendación I.321 de la UIT-T, modelo que se recoge en la figura 4.3. Se corresponde con un modelo tridimensional, que comprende tres planos distintos: plano de usuario, plano de control y plano de gestión.

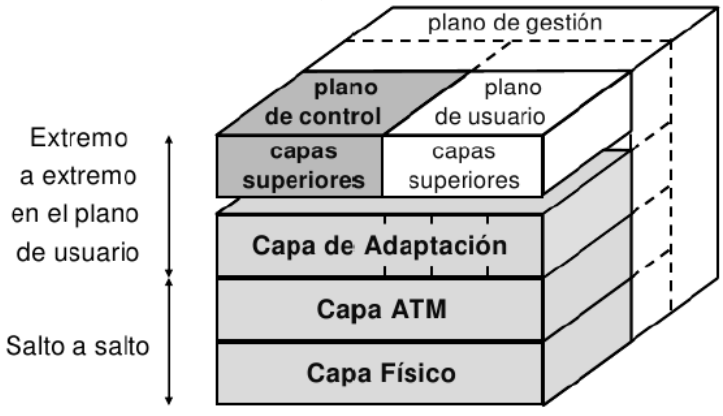

Figura 4.3: Arquitectura de protocolos ATM

El **plano de usuario** proporciona la capacidad para la transferencia de la información de usuario, el plano de control realiza las funciones de control de conexiones, incluyendo establecimiento, monitorización y liberación de conexiones virtuales, mientras que el plano de gestión es responsable del mantenimiento y de las tareas de gestión.

Las funciones del **plano de gestión** se categorizan a su vez en dos bloques, las funciones de capa de gestión y las funciones de plano de gestión. La primera de ellas se encarga de los flujos de operación y mantenimiento (*Operation and Management, OAM*) de cada capa específica y también maneja los recursos y parámetros residentes en sus entidades de protocolo, mientras que la segunda de ellas proporciona coordinación entre todos los planos, por lo que no contiene una estructura en capas.

La UIT-T únicamente especifica las tres primeras capas de ATM, dejando sin definir las superiores que pueden abarcar un amplio rango de protocolos existentes hoy día, como IP o IPX. Realizaremos a continuación una pequeña introducción de cada una de las capas de ATM, dejando su estudio en detalle para las próximas secciones:

- **Capa Física:** las funciones de esta capa se dividen en dos, la subcapa dependiente del medio físico (Physical Medium Dependent, PMD) y la subcapa de convergencia de trasmisión (Transmission Convergence, TC). Las funciones de la subcapa PMD se refieren a las relacionadas con el medio físico, tales como transferencia de bits, alineamiento de bit, tansformaciones electro-ópticas y codificación de línea. Las funciones de la capa TC incluyen delimitación de célula, procesado de cabeceras, ensamblado/desensamblado, generación de tramas y recuperación.

- **Capa ATM:** el núcleo de las funciones ATM incluye multiplexión/demultiplexión de células, traducción de VPI/VCI, generación y extracción de cabeceras, además de otras funciones como control de flujo, Usage Parameter Control/Network Parameter Control (UPC/NPC), notificación de congestión, asignación y eliminación de conexiones.

- **Capa de Adaptación:** dependiendo del tipo de aplicación, la capa de adaptación (ATM Adaptation Layer AAL) realiza una amplia variedad de funciones específicas. Actúa en los extremos de la conexión y sí puede incluir control de errores extremo a extremo en la información de usuario. La AAL se descompone en la subcapa de Convergencia (Convergence Sublayer, CS) y la subcapa de Segmentación y Reensamblado (Segmentation And Reassembly, SAR). Se han definido diferentes tipos de capas de adaptación, AAL1, AAL2, AAL3/4 y AAL5, asociadas cada una de ellas a distintos tipos de servicios.

4.4. Capa Física

La capa física ATM, similar a la capa física OSI, es responsable del transporte de flujos de binarios a través de la red. La capa física ATM, sin

embargo tienen un sentido más amplio en el sentido de que realiza algunas de las funciones que normalmente son realizadas por las capas de nivel 2 en sistemas que basados en el modelo OSI.

La capa física como ya hemos comentado, está dividida en dos subcategorías:

- Physical Medium Dependedent (PMD): las funciones de la subcapa dependiente del medio físico son aquellas relacionadas específicamente con el medio físico, como transmisión de bits, codificación de línea, conversión electro/óptica, ..., es decir, con el nivel 1 del modelo OSI.
- Transmission Convergence (TC): Las funciones de la subcapa de convergencia de trasmisión incluyen la inserción/extracción de células de relleno, generación de trama de transmisión, control de errores de la cabecera de las células y delimitación de células. Estas serían las funciones típicamente enmarcadas en el nivel 2 del modelo OSI, que en ATM se implementan en su primera capa. Pasamos a realizar una descripción más completa de ambas subcapas.

4.4.1. Subcapa dependiente del medio físico (PMD)

Las funciones PMD son aquellas relacionadas específicamente con el medio físico, es decir, como se representan los bits sobre el medio físico y como son interpretados en el receptor. Las dos principales funciones de esta subcapa son:

- **Temporización y sincronización:** Para permitir al receptor recibir e interpretar de manera correcta los patrones binarios enviados por el emisor, debemos establece una relación temporal entre ambos. esta relación puede ser establecida de forma implícita o explícita. En una relación explícita de temporización, emisor y receptor deben mantener una frecuencia de reloj común, de modo que el tiempo de duración de bit es conocido por ambos y determinado por dicha frecuencia de reloj. Si la relación es implícita, se obtiene mediante un esquema de codificación particular, como Alternate Mark Inversion (AMI).
- **Codificación y transmisión:** los bits pueden ser ingresados en el medio físico de varias maneras. En líneas de cobre, la codificación de ceros y unos puede realizarse con multitud de niveles de voltaje o de frecuencias. En medios ópticos, básicamente la presencia de ceros y unos se realiza con la presencia o ausencia de fotones en la línea. Es la subcapa PMD la que define pues el método a utilizar.

Existe un amplio número de estándares de capa física definidos tanto por el ATM Forum como por la UIT-T, recogidos en la tabla 4.1. En el contexto

de este manual, no tiene sentido estudiarlos todos, por lo que nos centraremos en revisar una serie de conceptos que ayudan a entender diferentes enfoques.

Estándar	**Descripción**
ITU-T I.432	Define funciones subcapa TC. Especifica mapeado de células ATM en interfaces 155.52 Mb/s y 622.08 Mb/s.
ATMF DS1	Especifica mapeado de células ATM en DS1 (T1), con interfaces a 1.544 Mb/s.
ATMF DS3	Especifica mapeado de células ATM en DS3 (T3), con interfaces a 44.736 Mb/s.
ATMF E1	Especifica mapeado de células ATM en DS1 (T1), con interfaces a 2.048 Mb/s.
ATMF E3	Especifica mapeado de células ATM en DS3 (T3), con interfaces a 34.268 Mb/s.
ATMF FRA E1/T1	Especifica mapeado de células ATM en E1/T1 fraccional, con interfaces a n*64 Kb/s.
ATMF UNI 3.1	Especifica mapeado de células ATM en SONET STS-3c, con interfaces a 155.52 Mb/s.
ATMF PHY 2.4G	Especifica mapeado de células ATM en SONET STS-48c, con interfaces a 2.4 Gbps.
ATMF UTOPIA Lx	Define un interfaz estándar común entre ATM y capas físicas de subsistemas ATM. 'x' indica los niveles 1,2,3, y 4.
ITU-T G.804	Define modos de mapear células ATM sobre interfaces PDH como DS1, DS3, E1 y E3.

Tabla 4.1: Capas Físicas ATM estandarizadas

Tal y como hemos anticipado, ATM se basa en la transmisión de células de tamaño fijo, 53 octetos, de los cuales 5 octetos se reservan para la cabecera de la célula.

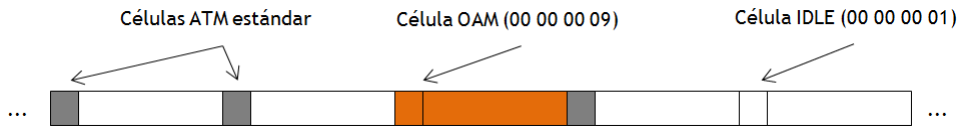

Figura 4.4: Tipos de células ATM

En el entramado de células, que conforman el flujo binario ATM, junto a las células ATM estándar se incluyen 2 tipos de células especiales como se

indica en la figura 4.4.

- *Células OAM:* células de operación y mantenimiento, se introduce 1 de cada 27, por lo que tenemos disponible para ATM 26/27, es decir aproximadamente un 96 % de total del régimen binario.

- *Células IDLE:* células ociosas, que pueden introducirse según necesidades, para mantener y ajustar el flujo binario.

En general, existen dos clases de estándares para mapear las células ATM sobre un flujo de transmisión, unos utilizan la *Jerarquía Digital Plesiócrona (PDH)* y otros utilizan la *Jerarquía Digital Síncrona (SDH).* Precisamente, el modo específico en que se realiza esta tarea es lo que especifican los estándares de la tabla 4.1.

- **ATM sobre Jerarquía Digital Síncrona (SDH).** Las células ATM se transportan en la carga útil de la estructura, generando flujos de distintas velocidades, según la trama utilizada: STM-1, STM-4, STM-16.

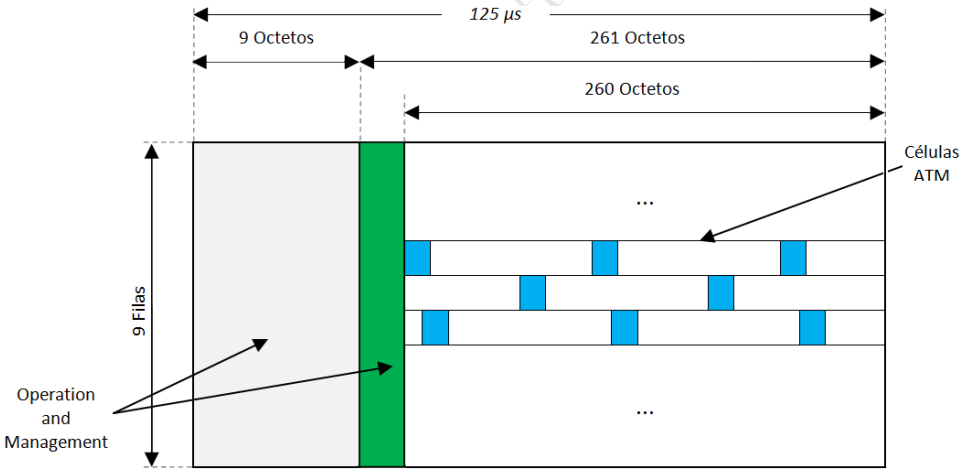

Figura 4.5: Estructura de trama de STM-1.

Usando una trama STM-1 se obtiene un régimen binario de:

- Total: $270 \times 9 \times 8 \div 125\mu s = 155,52Mb/s$
- Útil: $261 \times 9 \times 8 \div 125\mu s = 149,76Mb/s$

Dichas velocidades se van multiplicando por cuatro en función de la trama STM superior utilizada.

- **ATM sobre Jerarquía Digital Plesiócrona (PDH)**

  Las células ATM se mapean directamente sobre las jerarquías TDM, consiguiendo diferentes tasas binarias, como muestra la tabla 4.2.

Nivel	Bit Rate (Mb/s)	Canales Voz
E1	2.048	30
E2	8.448	120
E3	34.368	480
E4	139.260	1920

Tabla 4.2: Jerarquía TDM

Es importante, destacar también en PDH el uso del *multiplexado inverso para ATM*, más conocido por sus siglas IMA (del inglés Inverse Multiplexing for ATM),que es una tecnología usada para transportar tráfico ATM sobre un conjunto de líneas E1 o T1, al que se da el nombre de grupo IMA (en inglés IMA group). Esta tecnología permite un incremento gradual de la capacidad de transporte de tráfico, como vemos en el ejemplo de la figura 4.6.

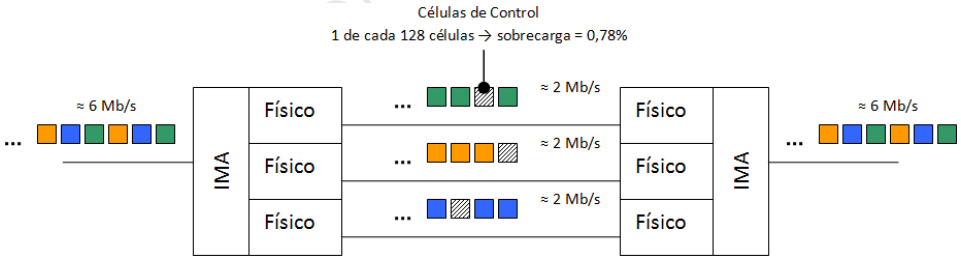

Figura 4.6: Multiplexado inverso de ATM (IMA)

La inserción de células ATM se realiza siguiendo un algoritmo *round robin*, y es un proceso transparente en los extremos del enlace. La funcionalidad IMA requiere cierta sobrecarga de tráfico: las células ICP, del inglés IMA Control Protocol, se envían a razón de una por cada marco IMA, generalmente compuesto por 128 células; y usando CTC, del inglés Common Transmit Clock, se requiere una célula ICP de relleno por cada 2048 células ATM. También requiere una subcapa IMA en el nivel físico.

4.4.2. Subcapa de convergencia de trasmisión (TC)

La subcapa de convergencia de transmisión se encarga de realizar una serie de funciones que son requeridas, independientemente del medio físico

subyacente. Realiza funciones como el ensamblado de células, adaptación de la trama de transmisión y el desacoplo de la tasa de células, funciones que no estudiaremos.

Nos centraremos sin embargo en las funciones relacionadas con la cabecera de las células ATM, concretamente en el control de errores y en la delimitación de célula.

- **Control de errores en la cabecera (Header Error Control, HEC).** Se implementa un mecanismo que proporciona corrección de errores simples y capacidades de detección de errores múltiples. En el quinto octeto de la cabecera, conocido como campo HEC, se inserta una suma de comprobación (checksum) calculada sobre los cuatro primeros octetos de la propia cabecera.

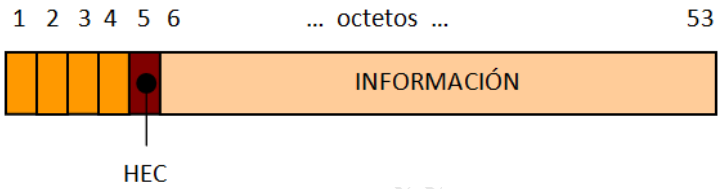

Figura 4.7: Célula ATM: Header Error Control

El emisor calcula el checksum sobre los cuatro primeros octetos de la cabecera, almacenando el resultado en el quinto octeto. El receptor, recomputa el checksum (llamado ahora *síndrome*) y comprueba si es coincidente con el recibido en el quinto octeto para ver si existe algún error.

Encontramos dos modos de operación, el modo de corrección y el modo de detección. Los procedimientos de control de errores a ejecutar sobre la célula recibida dependen del modo en el que se encuentre el receptor. El diagrama de estados para el cambio de modo se recoge en la figura 4.8.

Inicialmente, el receptor está en el modo de corrección. para cada célula entrante calcula el síndrome de su cabecera. Si el síndrome coincide con el incluido en la cabecera, no se ha producido error y permanecemos e el modo de corrección. Si hay diferencia aparecen dos posibilidades. Si la diferencia es de un único bit, el error es corregido y el receptor cambia a modo de detección. Si la diferencia es de más de un bit, igualmente pasamos a modo de detección pero descartamos la célula directamente. A partir de aquí, únicamente volveremos al modo

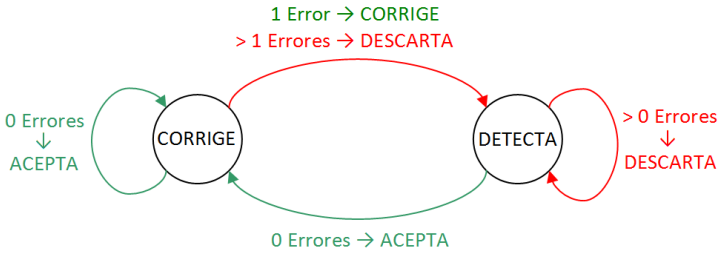

Figura 4.8: HEC: Protección contra errores y ráfagas

de corrección cuando recibamos una célula con la cabecera correcta, descartando todas aquellas que lleguen con errores[6].

Existe un motivo específico para no corregir errores simples (de un bit) consecutivos y es que este tipo de errores, en sistemas basados en redes de fibra son muy poco habituales con lo cual, si se produjeran dos o más seguidos, indicaría un problema distinto, como un posible error de ráfaga o el malfuncionamiento de algún equipo en la red.

- **Delimitación de célula.** Ya hemos estudiado algún método para delimitación de tramas, como el estudiado en RDSI con la detección de un patrón bandera junto con bit stuffing en los datos para evitar falsas detecciones por si el patrón aparece en los datos de usuario, un método que tiene unas desventajas inherentes, como el aumento del tamaño de la cabecera.

  La subcapa TC de ATM implementa una filosofía distinta para esta labor, aprovechando la detección de errores de cabecera explicada antes. El método HEC se basa en el hecho de que el quinto octeto de una célula tiene un valor definido por sus cuatro octetos previos. Viéndolo de otro modo, si un octeto dado aparece como el checksum de los cuatro anteriores, podemos decir con una cierta confianza que hemos identificado la cabecera de la célula.

  En el procedimiento de delimitación de célula, se definen tres posibles estados,como recoge la figura 4.9: HUNT, SYNCH y PRESYNCH, donde se muestran también las transiciones entre las mismas. Cuando se inicia el receptor, se encuentra en estado HUNT, es decir, va buscando bit a bit por límites de célula. Cuando encentra un HEC correcto, con el síndrome calculado igual al quinto octeto, pasa a estado PRESYNCH, donde pasa a verificar un número, DELTA, de células

[6]En el modo de detección se descartan las tramas erróneas de manera directa aunque el error sea de un único bit.

posibles consecutivas. Si las DELTA células resultan positivas pasa al estado SYNCH, donde a pesar de que los límites de las celdas son conocidas, pues recordemos que tienen longitud fija, se seguirán comprobando y calculando los síndromes.

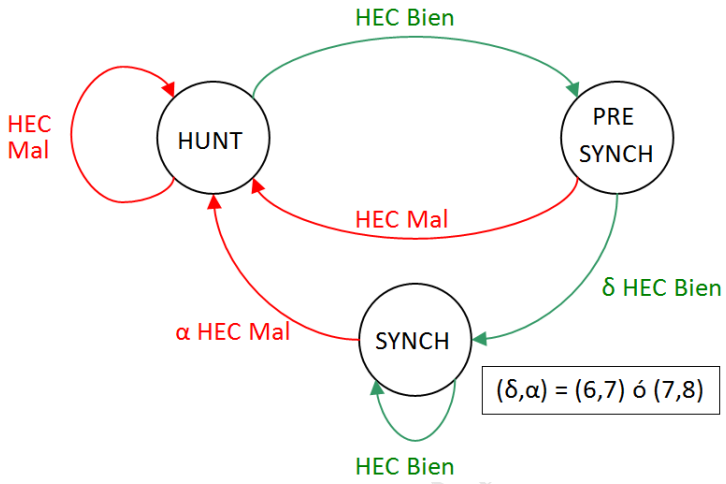

Figura 4.9: Delimitación de célula

En el estado SYNCH mientras se reciban menos de ALPHA células incorrectas se permanecerá en dicho estado, asegurando así que un error puntual no fuerza el reinicio de todo el procedimiento de delimitación.

Los valores de DELTA y ALPHA se han estimado tratando de hacer el proceso seguro y robusto. Parejas de valores típicos de (DELTA,ALPHA) son (6,7) y (8,7).

4.5. Capa ATM

La capa ATM es el núcleo de la pila de protocolos ATM. Toda la funcionalidad esencial de ATM se realiza en este nivel y por lo tanto es lógico que se le de su mismo nombre a la torre completa. Esta capa, multiplexa varios flujos de células de usuario en un único flujo, y lo demultiplexa en el destino. En los nodos intermedios, la capa ATM traduce los identificadores de conexión (VPI/VCI) y realiza la conmutación de células. En esta capa se implementan también mecanismos de vigilancia del tráfico y de indicación de congestión.

4.5.1. Caminos y canales virtuales

ATM utiliza los campos VPI/VCI de una conexión virtual para conmutar células. En cada nodo intermedio, los valores VPI/VCI son sustituidos por unos nuevos. Este proceso se conoce como reenvío de células. En la figura 4.10 se recoge el intercambio de pares VPI/VCI realizado en un conmutador ATM.

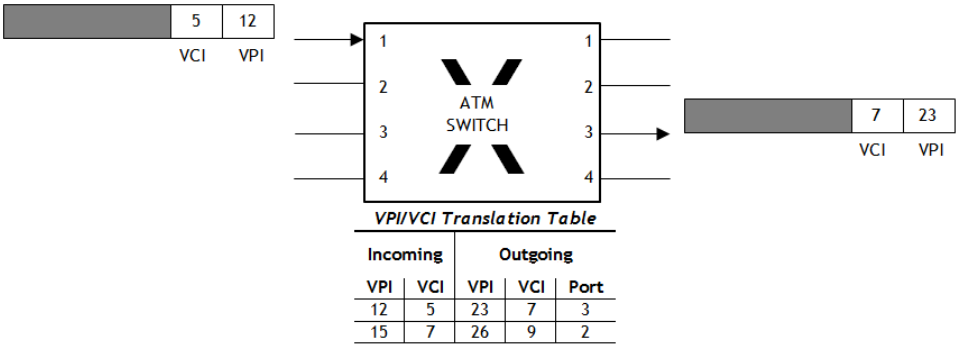

Figura 4.10: Conmutador ATM

El par VPI/VCI de la célula entrante se utiliza como índice para buscar en la tabla de traducción VPI/VCI del conmutador. En dicha tabla, se mantiene una entrada separada para cada circuito virtual establecido. Los valores en la tabla se rellenan cuando se establece la conexión.

Los nuevos valores VPI/VCI consultados en la tabla se sobreescriben en la cabecera de las células entrantes para posteriormente ser retransmitidas por el número de puerto que es también indicado por la tabla de traducción.

La conmutación en ATM no es algo tan sencillo como lo explicado hasta ahora. Actualmente, las conexiones virtuales conexiones en ATM se clasifican en dos categorías, lo que establece dos niveles de jerarquía en la retransmisión de células:

- **Canal Virtual (Virtual Channel, VC) y Conexión de Canal Virtual (VCC):** VC es un concepto lógico utilizado para describir el transporte de células ATM basado en un valor de identificador único llamado VCI. Un VCC es un término mucho más formal, definido como *una concatenación de enlaces de canales virtuales, que se extiende entre dos extremos, y es conmutado con la combinación de los pares VPI/VCI.* Específicamente, un VCC se extiende entre dos extremos donde se accede a la capa de adaptación. Un enlace de canal virtual se refiere a la conexión lógica, ya sea entre dos nodos intermedios o mediante un nodo intermedio y uno final.

- **Camino Virtual (Virtual Path, VP) y Conexión de Camino Virtual (VPC):** VP es un concepto lógico utilizado para describir el transporte de células ATM, basándose en un valor de identificador único llamado VPI. Un VPC es un concepto mucho más formal, definido como *una concatenación de enlaces de caminos virtuales, que se extiende entre el punto donde se asignan los valores VCI y el punto donde dichos valores son traducidos o eliminados.* Un VPC es conmutado usando únicamente los valores VPI.

En la figura 4.11 se muestra la relación entre VCs, VPs y el camino de transmisión. Un camino de trasmisión contiene uno o más caminos virtuales, mientras que a su vez, un camino virtual contiene uno o más canales virtuales.

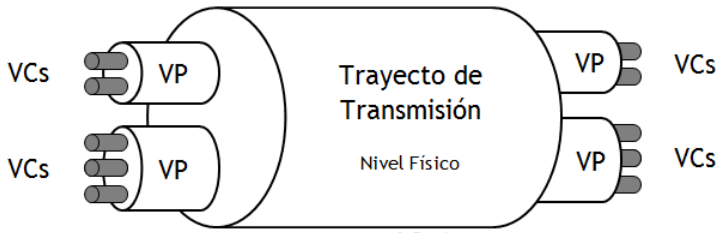

Figura 4.11: ATM: Caminos y Canales Virtuales

La conmutación se puede realizar bien a nivel de camino virtual o bien a nivel de canal virtual.

En el primer caso, únicamente se utiliza el valor del campo VPI, y el proceso se conoce como conmutación de camino virtual, tal y como se recoge en la figura 4.12. Los equipos que realizan este tipo de conmutación se conocen como *repartidores digitales.*

En el segundo caso, se utilizan ambos valores VPI/VCI para realizar la conmutación y el proceso se conoce como conmutación de camino virtual, tal y como se recoge en la figura 4.13. Los equipos que realizan esta función se conocen como *conmutadores ATM.*

En la figura 4.14 se muestra un ejemplo de ambos tipos de conmutación funcionando de manera conjunta en una red ATM.

Puede no parecer tan obvio el porqué existen dos identificadores (VPI y VCI) para realizar las labores de conmutación en ATM, ya por ejemplo, tecnologías como X.25 o Frame Relay, que están también basadas en conexiones virtuales utilizan un único indicador.

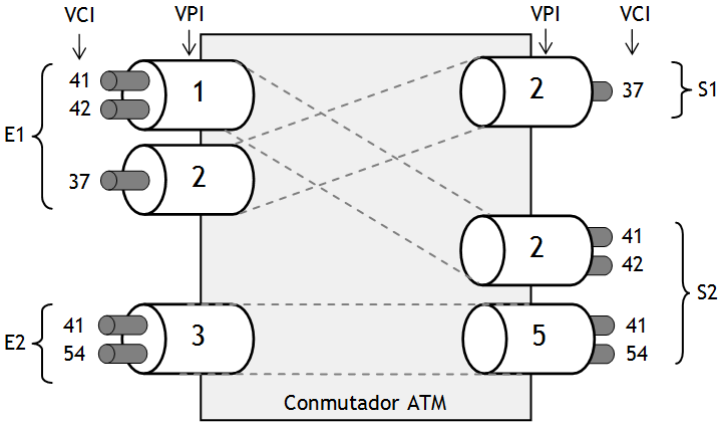

Figura 4.12: ATM: Conmutación de VPs (Repartidor digital)

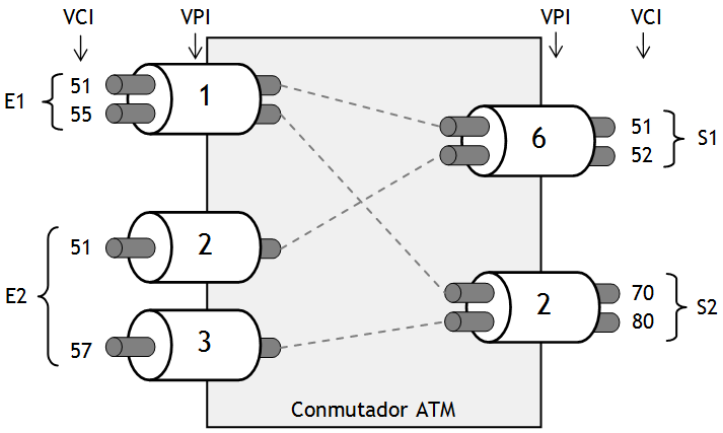

Figura 4.13: ATM: Conmutación de VCs (Conmutador)

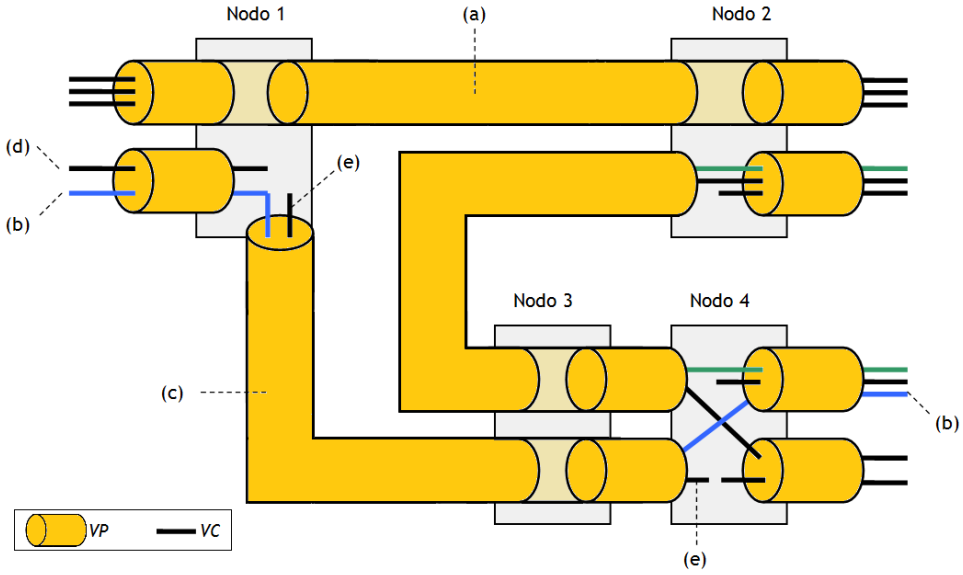

Figura 4.14: ATM: Ejemplo Conmutación de VCs y VPs

Existen una serie de ventajas inherentes al uso de dos niveles jerárquicos para conmutación.

La primera ventaja es que se permite diferenciar caminos virtuales en función de la QoS necesitada. Así, el recurso puede ser asignado sobre la base de caminos virtuales y en función de la naturaleza de la conexión solicitada, se puede garantizar un canal virtual de sobre un camino virtual específico. Esta asignación reduce la carga de trabajo en los conmutadores y permite facilitar el establecimiento o rechazo de conexiones.

La segunda ventaja consiste en la flexibilidad de mantener múltiples canales virtuales (conexiones) entre redes, utilizando un único camino virtual. Este hecho es muy útil para la infraestructura utilizada por los distintos proveedores de servicios en sus redes de agregación, situación que podemos comparar en la figura 4.15.

En la parte izquierda de la figura 4.15, cada VC lleva varios flujos de información (multiplexados por el nivel AAL), de manera que la red ATM trata cada VC por separado, mientras que en la parte derecha de la figura, los VCs de varios nodos B se agrupan en un mismo VP, lo que permite ahorrar capacidad en la red ATM hasta el RNC.

Aparte de las ventajas mencionada, debemos ser conscientes también de que la conmutación por VPs (repartición) es más rápida que la conmutación por VCs (conmutación completa), ya que únicamente se debe procesar uno

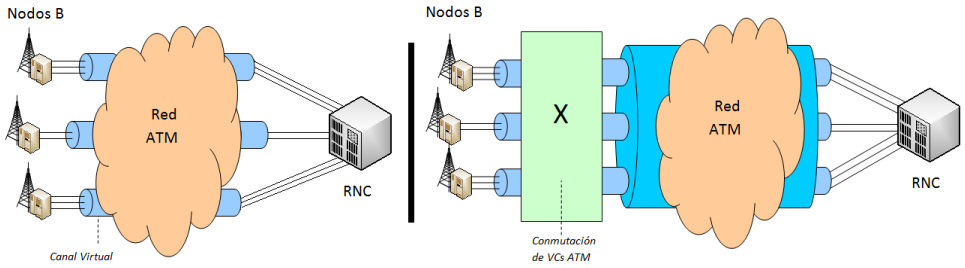

Figura 4.15: ATM: Ejemplo VC distinto para cada nodo B frente a VP compartido

de los identificadores de conexión en lugar de los dos.

Por supuesto, las conexiones, mediante VPs o VCs, pueden empezar y terminar en un usuario o en un nodo de la red, y tienen diversas aplicaciones como:

- VC o VP entre dos usuarios para interconexión de ordenadores remotos.
- VP entre nodos de la red para definir encaminamiento de VCs, separar tipos de información (de usuario, de señalización, ...).
- VC de usuario a red para señalización.

Por tanto, los conmutadores ATM realizan una conmutación por células, que se basa en buscar el camino interno de entrada/salida, traduciendo para ello las cabeceras de las células y realizando las oportunas labores de encolado de las células. Realizan también por supuesto funciones de gestión, señalización, encaminamiento y control de tráfico.

4.5.2. Formato de Célula

La estructura de una célula ATM, en concreto de su cabecera, se recoge en la figura 4.16. La estructura de cinco octetos tiene los bits en orden ascendente, de derecha a izquierda, y los octetos ascendentes, de arriba hacia abajo. La transmisión de los bits tiene lugar en orden decreciente de bits y creciente de octetos, es decir, el octavo bit del primer octeto se transmite el primero y el primer bit del quinto octeto es el último en ser transmitido.

Antes de comenzar con la descripción completa de cada uno de los campos de la cabecera, destacamos que algunos de los posibles valores de campos de cabecera se reservan para células generadas por la capa física, concretamente aquellas con VPI=VCI=0, y que son identificadas por el primer bit

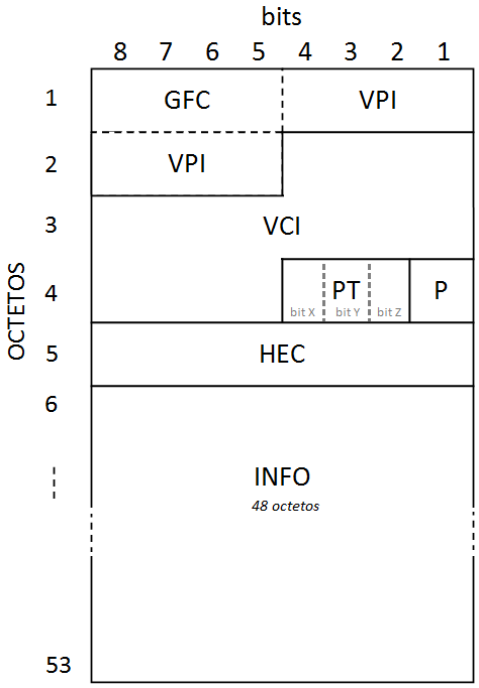

Figura 4.16: Formato de célula ATM

del cuarto octeto, que se fija a 1.

Ahora sí, pasemos a estudiar los distintos campo que componen la cabecera de una célula ATM:

- **Campo GFC (Generic Flow Control).** Campo de control de 4 bits, utilizado para realizar control de flujo entre sistemas finales y la red ATM. Este valor es utilizado únicamente por la red para limitar la cantidad de datos inyectados en ella por un sistema final. No existe control de flujo en sentido contrario.

- **Campos VPI/VCI.** En la interfaz usuario red (User Network Interface, UNI) el VPI está formado por 8 bits, que se extienden hasta 12 en las interfaces dentro de la red (Network Network Interface, NNI)[7], mientras que el identificador de canal virtual (VCI) tiene una extensión de 16 bits en cualquier caso.

  Algunos valores se reservan para labores de gestión y mantenimiento de la red, mientras que otros se reservan para funcionalidades específicas de la capa ATM. En concreto, están reservados valores de VCI

[7]Donde se utilizan los 4 bits del GFC que no tienen sentido en NNI.

de 1 a 31 para cualquier VPI. También están reservados los valores VPI=VCI=0, que indican células sin asignar. Cuando tenemos un valor de VCI nulo, cualquier combinación es inválida salvo la ya comentada con VPI también nulo. Es decir, valores admitidos de VCI para células de datos de usuario son aquellas con $VCI \geq 32$.

- **Campo PT (Payload Type).** Campo de 3 bits de extensión, denominados bits X, Y y Z utilizado para identificar el tipo de datos transportados por la célula. Los bits indican:
  - *Bit X:* si su valor es 0 indica que la célula transporta datos de usuario.
  - *Bit Y:* bit utilizado para indicar estado de congestión.
  - *Bit Z:* bit de usuario a usuario.

  La tabla 4.3 muestra los distintos valores del campo Payload Type.

XYZ	Descripción
0 0 0	Célula de datos de usuario. Sin congestión. Usuario a Usuario = 0
0 0 1	Célula de datos de usuario. Sin congestión. Usuario a Usuario = 1
0 1 0	Célula de datos de usuario. Con congestión. Usuario a Usuario = 0
0 1 1	Célula de datos de usuario. Con congestión. Usuario a Usuario = 1
1 0 0	OaM F5 célula asociada a segmento
1 0 1	OaM F5 célula asociada extremo a extremo
1 1 0	Célula de gestión de recursos VC
1 1 1	Reservado

Tabla 4.3: Valores campo Payload Type (PT)

Las posibles combinaciones del campo PT se clasifican en dos categorías. La primera se corresponde con células de datos de usuario, y son aquellas que aparecen en la tabla con el bit más significativo del campo a 0. Dentro de esta categoría, el segundo bit más significativo indica si estamos en situación de congestión o no, fijando el valor del bit a 1 y 0 respectivamente. Si un nodo recibe una célula con este bit a 1, debe iniciar procedimientos de control de congestión. Un nodo que esté en estado de congestión, debe fijar dicho bit a 1 para todos sus enlaces salientes. El bit menos significativo para una célula de datos de usuario porta indicaciones de usuario ATM a usuario ATM.

Un ejemplo de su uso se verá cuando se estudie la capa de adaptación AAL5.

La segunda categoría corresponde con células que no transportan datos de usuario. Esta categoría contiene PTs con su bit más significativo a 1. La interpretación del resto de bits es independiente de la de la anterior categoría, y son casos exclusivos tal y como se recoge en la tabla.

- **Campo CLP (Cell Loss Priority)**[8]**.** Campo de un único bit utilizado para asignar uno de los dos niveles de prioridad existentes a una célula. Células con su campo CLP a 0 tienen mayor prioridad que aquellas con su CLP a 1. En estado de congestión, las células de prioridad baja (CLP=1) están sujetas a ser descartadas antes que células de prioridad alta. Inicialmente, es el extremo origen de los datos el que fija la prioridad de las células, pudiendo ésta ser reducida (nunca aumentada) en nodos intermedios en caso de congestión.

- **Campo HEC (Header Error Control).** El último octeto de la cabecera proporciona un mecanismo de control de error, ya explicado previamente, para el resto de bits de la cabecera. Es importante recordar que este código de control no es aplicable a la parte de datos de usuario de la célula.

4.6. Capa de Adaptación

la Capa de Adaptación de ATM (ATM Adaption Layer AAL) se encarga de adaptar el servicio ATM a los distintos requisitos de las capas superiores. En el origen de la transmisión, la capa AAL toma paquetes de datos de las capas superiores, transformándolos en paquetes de datos de 48 octetos para poder ser directamente manejados en la capa ATM.

En el destino, se realiza el proceso inverso y las distintas células son reensambladas para formar un paquete de datos correspondiente a la capa superior, dando soporte por tanto extremo a extremo. Este procedimiento de segmentación en el origen y reensamblado en el destino es la tarea principal de la capa AAL.

La capa de adaptación se divide de forma general en dos subcapas, como recoge la figura 4.17:

- **Subcapa de Convergencia (CS):** interactúa directamente con el usuario y acepta datos de él. Opcionalmente añade una cabecera o trailer a los datos de usuario para entregarlos posteriormente a la subcapa segmentación y reensamblado. La subcapa de convergencia se divide a su vez en dos subcapas, denominadas Parte Común de

[8]También es común denominar a este campo simplemente como Priority (P).

la Subcapa de Convergencia (Common Part CS, CPCS) y Subcapa de Convergencia Específica de Servicio (Service Specific CS, SSCS). CPCS proporciona funcionalidad genérica común para todas las aplicaciones mientras que SSCS proporciona funcionalidad adicional para aplicaciones específicas.

- **Subcapa de Segmentación y Reensamblado (SAR):** segmenta los datos recibidos de la CS en unidades de datos más pequeñas. Puede también añadir (o no) cabeceras o colas a esas pequeñas unidades de datos para formar SAR-PDUs de 48 octetos, que forman la carga de pago de las células ATM.

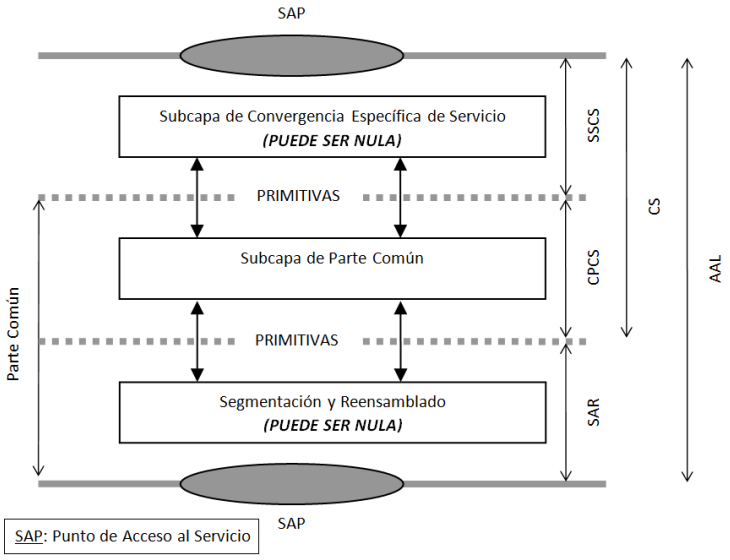

Figura 4.17: Estructura Genérica AAL

Esta arquitectura de subcapas para la AAL es totalmente genérica y varia en funcionalidad entre las distintas AALs definidas, tal y como veremos a continuación. Es decir, esta clasificación genérica no es la misma en todas las AALs. Por ejemplo, la subcapa SAR no realiza ninguna segmentación ni reensamblado en AAL2 ya que las unidades de datos provenientes de capas superiores suelen ser pequeñas y normalmente pueden encajar en una única célula. Por lo tanto, en AAL2 el uso del término subcapa SAR no es del todo correcto.

Dado que las distintas aplicaciones (usuarios de ATM) ofrecen o requieren diferentes tipos de tráfico de la red, se han definido varias capas de adaptación para poder soportar esta variedad de necesidades. Los parámetros utilizados en la definición de las distintas capas de adaptación son recursos de red como tasa de transferencia (constante o variable), retardo (constante

o variable) o naturaleza de la conexión.

Así, están definidos las capas AAL1, AAL2, AAL3/4, AAL5 y AAL0, cuyas principales características se resumen en la tabla 4.4.

Tasa	Constante	Variable	Variable
Retardo	Constante	Constante	Variable
Tipo	AAL1	AAL2	AAL5

Tabla 4.4: Tipos de AAL

AAL1 porta tráfico a tasa constante, sensible al retraso en una conexión establecida entre dos sistemas finales. AAL1 se encarga de tratar las variaciones en el retraso, establecer la conexión entre dos entidades pares y mantener los requerimientos de tiempo entre ellas. Se utiliza por tanto para emulación de circuitos y para comunicaciones vocales.

AAL2 proporciona funcionalidades para la transferencia de tráfico sensible al retraso pero con tasas de transferencia variable. Utilizado en comunicaciones vocales y también en aplicaciones de vídeo a tasa variable.

AAL3/4 proporciona transferencias de datos tanto orientadas a conexión como no orientadas a conexión, sensibles al retraso y con tasa de transmisión variable. Utilizada en tráfico de datos.

AAL5 proporciona funciones para la transferencia de ráfagas de tráfico. Es una capa de adaptación muy básica, con una funcionalidad limitada en la que únicamente destacan las labores de segmentación y reensamblado.

Únicamente estudiaremos los protocolos AAL2 (para voz) y AAL5 (para datos).

4.6.1. AAL2

AAL2 proporciona los medios para lograr una transmisión eficiente para servicios de tasa variable y que necesiten un retardo constante, por ejemplo voz con supresión de silencios o vídeo. Las características principales de AAL2 se pueden resumir en:

- Proporciona los medios para la transmisión eficiente a tasas reducidas, de paquetes de datos de longitud variable en aplicaciones sensibles a retrasos.

- Se en carga de la transferencia de tráfico sensible al retraso, tanto a tasas constante como variable.
- Proporciona técnicas para compresión de datos y supresión de silencios.
- Habilita más de una canal AAL2 en un único circuito virtual ATM, es decir, permite la multiplexión de datos provenientes de múltiples usuarios en la misma PDU, que serán transmitidos por la misma conexión ATM, por ejemplo, varias llamadas de voz codificadas a baja velocidad y con supresión de silencios o sin ella.
- Se propuso para redes de acceso UMTS basadas en ATM.

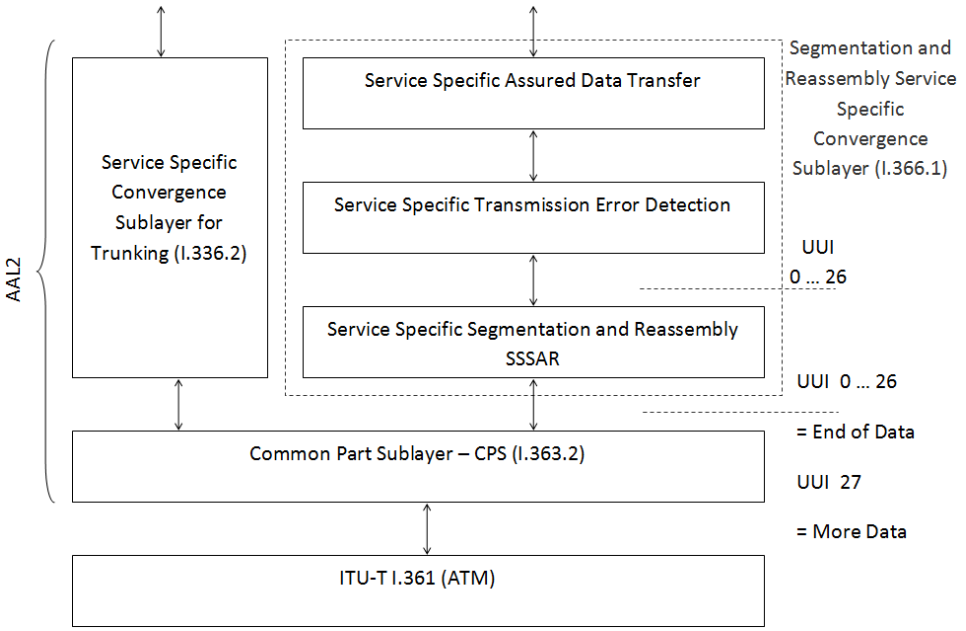

Figura 4.18: Arquitectura de Protocolos AAL2

Respecto a la estructura de subcapas de AAL2, recogida en detalle en la figura 4.18, debemos comentar que en principio en AAL2, la subcapa SAR no será necesaria, pues la subcapa CPS proporcionará unidades de datos adaptadas al tamaño de las células ATM.

No entraremos en ningún caso en el estudio de la subcapa de Convergencia Específica de Servicio (SSCF) de AAL2.

Common Part Sub-Layer (CPS)

La subcapa CPS de AAL2 proporciona capacidad para transferir CPS-SDUs desde un usuario CPS a otro usuario CPS. El usuario CPS puede ser

o bien una entidad SSCS o la entidad de capa de gestión.

CPS realiza un procedimiento en dos etapas sobre los datos recibidos del usuario CPS. En una primera etapa añade una cabecera a los datos para formar un paquete CPS. En la segunda etapa, forma CPS-PDUs de exactamente 48 octetos, que irán una a una directamente encapsuladas en la zona de carga de distintas células ATM, lo cual justifica que en AAL2 la subcapa SAR no tiene sentido. Las CPS-PDUs se forman agrupando los minipaquetes CPS provenientes de distintas fuentes de información.

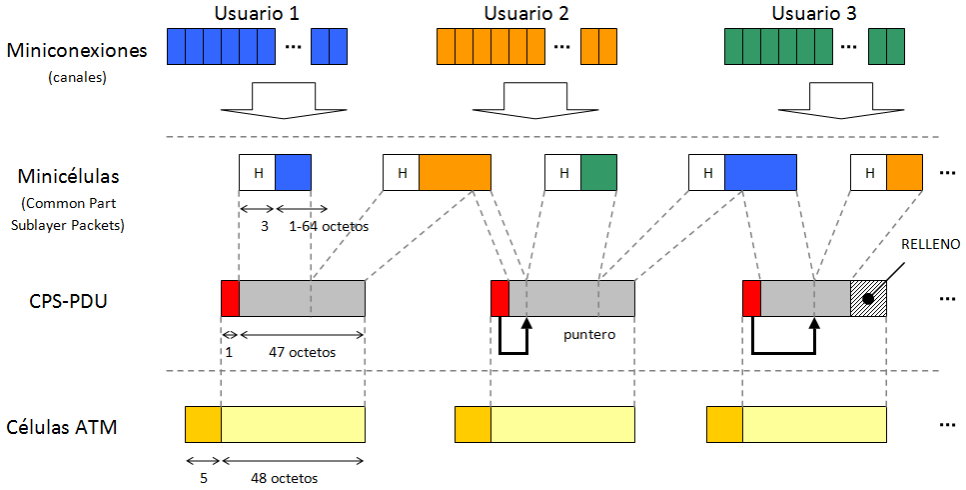

Figura 4.19: Multiplexión AAL2 (I)

El procedimiento detallado, extendido a cuatro pasos se muestra en la figura 4.19. Los pasos detallados se explican como:

- **Paso 1:** tres tramas de usuario, correspondientes a diferentes canales AAL2 llegan para ser trasmitidos.
- **Paso 2:** para cada trama de usuario, se forma un paquete CPS añadiendo una cabecera de 3 octetos y siendo los datos de un tamaño comprendido entre 1 y 64 octetos.
- **Paso 3:** los paquetes CPS se concatenan para formar una CPS-PDU de 48 octetos, que incluye al inicio una cabecera CPS-PDU de un octeto. Un paquete CPS se puede extender en múltiples CPS-PDU, utilizando las cabeceras como punteros al inicio de nuevos paquetes CPS.
- **Paso 4:** Las CPS-PDU se mapean directamente en la zona de carga de las células ATM.

Debemos destacar dos aspectos importantes. En primer lugar el uso de dos niveles de cabeceras permite distinguir claramente entre los distintos usuarios que están compartiendo la misma conexión virtual. En segundo lugar, el tiempo que AAL2 espera para despachar una CPS-PDU esta controlado por un temporizador, de modo que si no se reciben suficientes datos antes de que el contador expire, se envía la CPS-PDU con bits de relleno. Así, se garantizan los requisitos de tiempo para las aplicaciones sensibles a retraso (con un retraso máximo).

Estudiaremos ahora la estructura de un paquete CPS, concretamente los campos que componen la cabecera del mismo, estructura que se recoge en la figura 4.20.

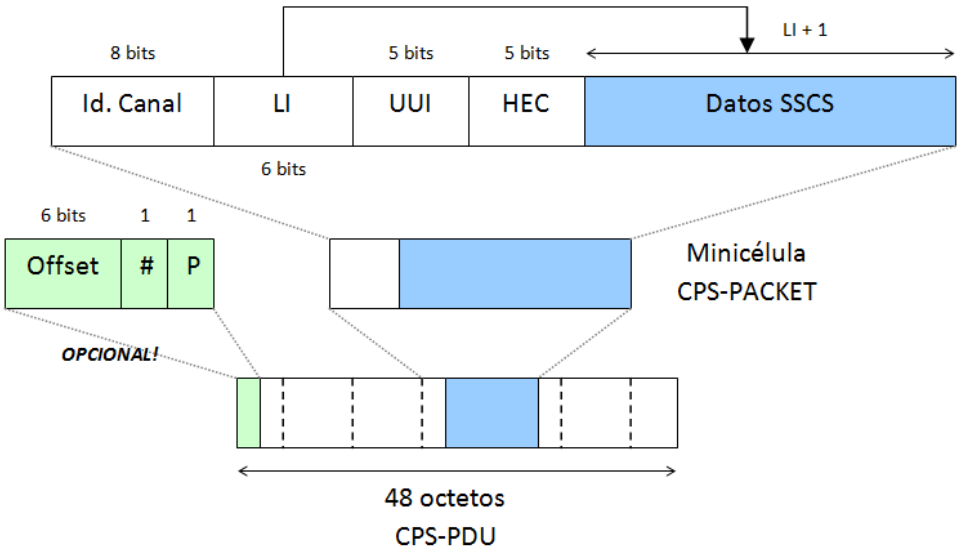

Figura 4.20: Multiplexión AAL2 (II)

- **Identificador de Canal:** octeto utilizado para identificar un canal AAL2. Se utiliza para multiplexar varios usuarios AAL2 en el mismo canal virtual ATM. Un canal AAL2 es bidireccional y debe usarse el mismo valor de identificador en ambos sentidos. El valor 0 no es utilizado y el 1 está reservado para procedimientos de gestión. Los valores de 2 a 27 se encuentran también reservados, por lo que se puede multiplexar un total de 227 usuarios, desde el 28 al 255, ambos inclusives.

- **Length Indicator (LI):** la longitud de la carga transportada por el paquete CPS se porta en este campo, de longitud 6 bits, que tiene un rango de 1 a 63, aunque también puede tomar el valor 64. La longitud

almacenada en el campo es una unidad menor que la longitud real del paquete de datos transportado. Se hace así para acomodar el valor de longitud 64 que realmente necesitaría 7 bits para ser codificado. Así, un LI de valor cero, indica una carga de datos de longitud uno, mientras que si el campo de LI es de valor todo uno, la longitud real es de 64. Por lo tanto, el tamaño del paquete completo CPS puede ser de 4 octetos (3 de cabecera más un octeto de carga) a 67 octetos (3 de cabecera más 64 de carga).

- **User to User Indication (UUI):** el identificador de canal permite diferenciar entre 227 usuarios, que pueden ser utilizados tanto por una entidad SSCS como por la entidad de la capa de gestión. Para diferenciar entre ellas se utiliza el campo UUI. Este campo tiene un doble propósito. En primer lugar se usa para transferir de forma transparente 5 bits de información entre usuarios CPS y en segundo lugar ayuda a distinguir entre dos usuarios CPS, como una entidad SSCS o la entidad de capa de gestión.
- **Header Error Control (HEC):** la subcapa CPS proporciona mecanismos de detección de errores sobre la cabecera CPS. Se utiliza un código de 5 bits, que contienen el CRC calculado para los 19 bits restantes de la cabecera.

Los paquetes CPS son transportados en el interior de las CPS-PDUs. Una CPS-PDU consta de 48 octetos, que conformarán la carga de las células ATM. La CPS-PDU tiene una cabecera de un octeto, mientras que los 47 octetos restantes son rellenados por paquetes CPS o en su ausencia, mediante bits de relleno. Cada CPS-PDU puede contener varios paquetes CPS, que son colocadas de forma consecutiva sin separación entre ellos. En caso de que el último paquete CPS no entre de forma completa, los bits faltantes serán transmitidos en la próxima CPS-PDU.

El formato de la CPS-PDU se muestra también en la figura 4.20, donde vemos que aparece un *offset* inicial de 6 bits que apunta al inicio del primer paquete CPS. El primer paquete CPS no tiene porqué empezar justo tras la cabecera, pues como hemos comentado, puede ser que se transporten bits pertenecientes a un paquete CPS que no entró completamente en la anterior CPS-PDU.

Dentro de la CPS-PDU, el final de un paquete CPS marca el comienzo del siguiente, y la longitud de los mismos se conoce accediendo al campo LI de la cabecera de cada paquete. Para diferenciar entre el comienzo de un paquete CPS y un campo de relleno, el primer octeto del paquete CPS nunca puede fijarse a valor cero. Al final de un paquete CPS, un octeto no nulo indica el comienzo de un nuevo paquete mientras que un valor de octeto

nulo indica el comienzo de un capo de relleno, lo que explica por qué no se permiten valores de identificadores de canal nulos.

El séptimo bit de la cabecera CPS-PDU se conoce como *bit de Número de Secuencia (SN o #)*. Se utiliza para numerar los flujos de CPS-PDUs. En el flujo de CPS-PDUs saliente, se fija a 1 y 0 en CPS-DPUs alternantes. Si el receptor, recibe dos CPS-PDUs consecutivas con el mismo valor de bit SN, se ha producido algún tipo de error. Como vemos, el sistema asume que la pérdida de una CPS-PDU es un hecho extraño (solo se utiliza un bit para ello). Esta asunción se deriva del hecho de que es indistinguible la pérdida de una CPS-PDU o de un numero impar de ellas. Para distinguir entre pérdidas y una cabecera errónea, y proteger el resto del campo de inicio con offset, se utiliza un bit de paridad. El octavo bit de la cabecera o *bit de Paridad (P)* se utiliza para mantener una paridad impar.

El protocolo Q.2630.1, de señalización AAL tipo 2 proporciona la capacidad de señalización para establecer, liberar y mantener conexiones punto a punto AAL tipo 2 a través de una serie de VCC ATM que transportan enlaces AAL tipo 2, es decir, proporciona señalización de canales entre entidades AAL2 por el canal 1.

En el ejemplo simplificado de la figura 4.21 se muestra como se solicitan el establecimiento y posterior liberación de un canal virtual AAL2, lo que se realiza mediante señalización que viaja por un canal AAL2 específico.

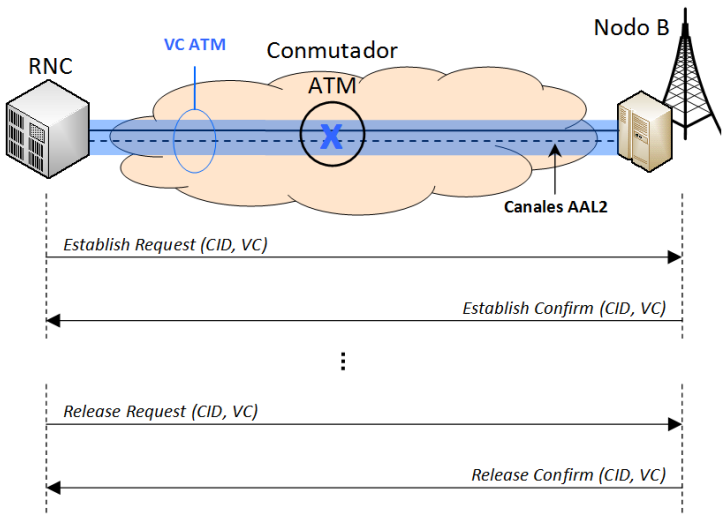

Figura 4.21: Señalización Q.2630.1 para canales AAL2

4.6.2. AAL5

AAL5 ofrece un método de transferencia de datos extremadamente simple, con una mínima sobrecarga de cabeceras. AAL5 está diseñada para trabajar con datos insensibles al retraso, y no proporciona métodos de multiplexión sobre el canal. Al igual que el resto de AALs, se divide en subcapa de convergencia (CS) y en subcapa de segmentación y reensamblado (SAR).

La **subcapa SAR** no introduce cabeceras, con lo cual es mucho más sencilla que la implementada en el resto de AALs. Esta capa simplemente trocea las SAR-SDUs en SAR-PDUs de 48 octetos, apropiadas para la carga de las células ATM. El comienzo y final de cada SAR-SDU se indica a través del bit de información usuario a usuario ATM de la cabecera de la célula. Un valor de 1 indica el fin de la SAR-PDU, mientras que un valor de 0 indica el comienzo o continuación de una SAR-PDU.

La subcapa CS tiene una parte común (CPCS) que introduce una sobrecarga de 8 octetos por mensaje, más un relleno de longitud variable. Tiene dos modos de funcionamiento, denominados modo mensaje y modo streaming. La figura 4.22 muestra el formato de las CPCS-PDU de AAL5, donde vemos que no hay cabecera, sino una cola (trailer) de 8 octetos, 4 pertenecientes a la cola y 4 correspondientes al CRC.

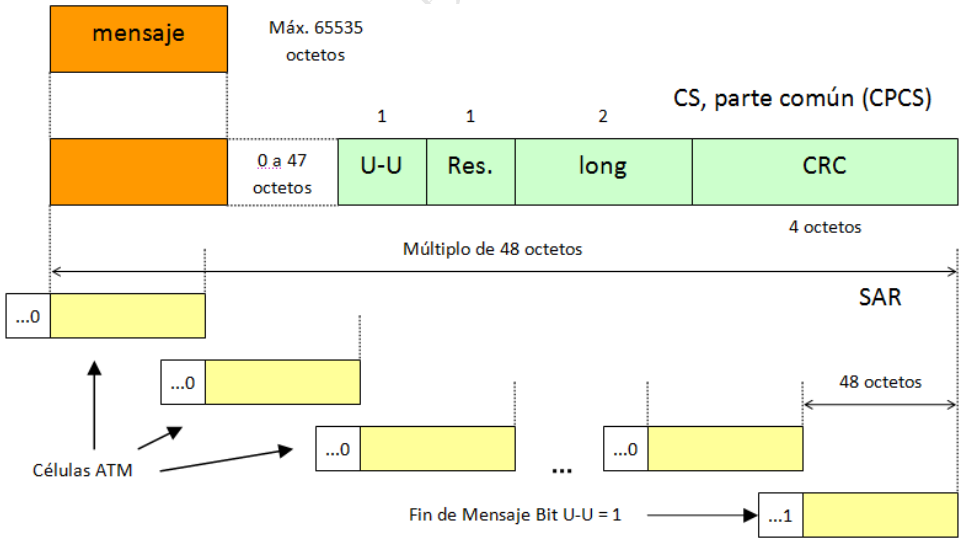

Figura 4.22: Formato AAL5 CPCS-PDU

El campo de longitud, de tamaño dos octetos, porta el número de octetos de la carga de la CPCS-PDU, con unos valores permitidos entre 1 y 65535. Un valor de longitud 0, indica una función de abortado. Existe también un

campo de indicador de parte común (CPI), utilizado únicamente para alinemamiento 64-bit de la cola. El campo de CRC de 4 octetos contiene un checksum calculado sobre toda la CPCS-PDU, incluyendo la carga, campo de relleno y los primeros cuatro octetos de la cola.

Entre la cola y la carga encontramos un campo de relleno (Padding). Se utiliza para conseguir que la longitud total de la CPCS-PDU junto con su cola, sea un múltiplo entero de 48 octetos, para poder encajar en la zona de carga de las células ATM. El número de octetos añadidos de relleno permitido va de 0 a 47. Debemos percatarnos de que no existe un campo específico en las células individuales para indicar el número de octetos útiles en la célula.

Resumen

Hemos estudiado en este apartado, algunas de las diferentes capas de adaptación que se han definido en ATM, por lo que es interesante resumir sus principales objetivos:

- **AAL1:** para flujos de tasa constante, por ejemplo, emulación de circuitos sobre ATM. No lo hemos estudiado.
- **AAL2:** más adecuado para paquetes pequeños o con requisitos de retardo. Puede multiplexar varios flujos de voz, con posibilidad de supresión de silencios, o de datos sobre la misma conexión ATM.
- **AAL5:** para tráfico de paquetes, como Frame Relay o IP sobre ATM. Es capaz de detectar paquetes incompletos o con errores.

4.7. Señalización en ATM

En este apartado, realizaremos una panorámica sobre la señalización en ATM, cuya pila de protocolos completa se recoge en la figura 4.23, donde encontramos los protocolos que que gestionan las labores de señalización en ATM. Como vemos, hemos de distinguir entre señalización en la interfaz usuario red (UNI) y en la propia red (NNI).

La **señalización en la interfaz usuario-red** viene reglamentada por la recomendación Q.2931 de la UIT-T, basada en la Q.931 de RDSI, a la que añade una serie de extensiones. Se define también por el ATM Forum la señalización UNI 4.1.

La **señalización de red** UIT-T se basa en ISUP de banda ancha (SS7) mientras que el ATM Forum define una señalización de red privada (PNNI

1.0, 1.1) que es similar a la utilizada en la interfaz usuario-red.

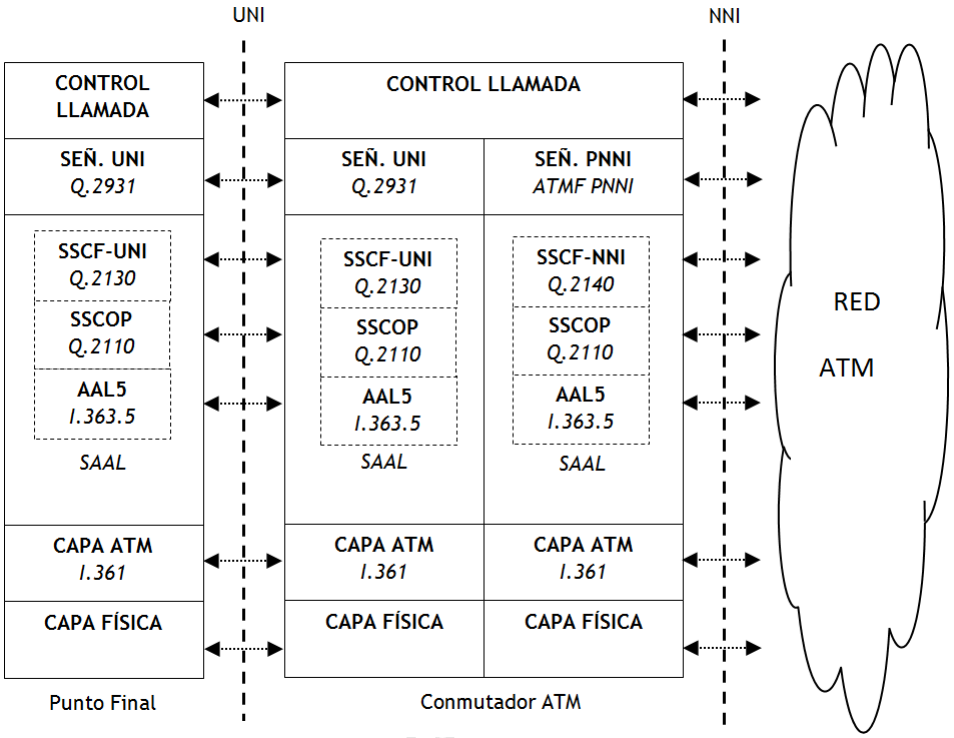

Figura 4.23: Torre de Protocolos Señalización ATM

En ATM vamos a encontrar tres tipos de conexiones:

- **Conexiones bajo demanda:** los estándares ATM proporciona soporte para una señalización elaborada, que permite el establecimiento y liberación dinámicos bajo demandan de conexiones conmutadas, son las denominadas SVC/SVP, Switched Virtual Channel/Path.

- **Conexiones permanentes «soft»:** el usuario las configura como las permanentes y dentro dela red se usa señalización para establecerlas. Si falla un enlace se restablecen automáticamente. Se denominan SPVC/SPVP, Soft Permanent Virtual Channel/Path.

- **Conexiones permanentes:** no requieren de señalización. Se configuran de antemano por otros procedimientos de gestión. Se denominan PVC/PVP, Permanent Virtual Channel/Path.

En el establecimiento de conexión, como es habitual distinguimos tres estados del proceso:

- *Antes del establecimiento:* los nodos han de tener información sobre el estado de la red, en todo lo referente a topología, direcciones, recursos, etc.

- *Durante del establecimiento:* el usuario describe su tráfico y la calidad del servicio requerida. La conexión se acepta si se encuentra un camino con recursos suficientes.

- *Tras el establecimiento:* se vigila el tráfico de la conexión.

Como vemos en la figura 4.23, la señalización UNI se sitúa encima de la capa de adaptación ATM para señalización SAAL (Signalling ATM Adaptation Layer), subcapa que puede ser interpretada como un tipo especial de AAL utilizada exclusivamente para señalización.

Al igual que las AAL convencionales, y como recoge la figura 4.24, SAAL se divide en una subcapa de convergencia (CS) y una subcapa de segmentación y reensamblado (SAR). A su vez, la CS se subdivide en la Parte Común de subcapa de convergencia (CPCS) y en la Subcapa de Convergencia Especifica de Servicio (SSCS).

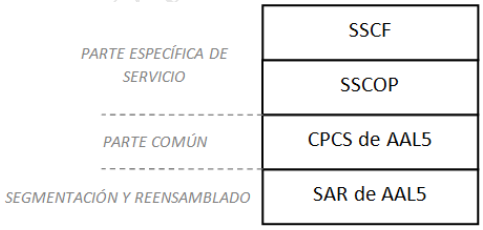

Figura 4.24: Arquitectura SAAL

Por su parte, la SSCS se subdivide en la Service Specific Connection-Oriented Part (SSCOP) y en Service-Specific Coordination Function (SSCF).

En la figura 4.23 la capas SAR y CPCS, que normalmente se implementan en hardware directamente, aparecen representadas de manera conjunta como AAL5 y sus funciones ya han sido explicadas.

El **protocolo SSCOP** es el núcleo de la subcapa SAAL y sirve para garantizar la transferencia fiable de la información de señalización. Sus características más destacadas son:

- Protocolo orientado a conexión.

- Permite control de flujo.

- Permite recuperación de errores por retransmisión selectiva.

El protocolo **SSCF (Service Specific Coordination Function)** adapta el servicio SSCOP a los diferentes protocolos de señalización usados en ATM. Controla pues el estado de los enlaces de señalización.

Por tanto, la subcapa SAAL proporciona el envío asegurado de mensajes de señalización sobre una capa ATM, no fiable de otro modo para estos propósitos. AAL5 forma parte de SAAL y por tanto, todos los nodos que transporten mensajes de señalización deben soportar AAL5. Los conmutadores intermedios también deben soportar como mínimo AAL5 para soportar el paso de mensajes de señalización por ellos. No obstante, es posible que un nodo intermedio soporte únicamente AAL5 y no otra capa de adaptación.

Es una práctica habitual referirse a la capa de señalización ATM como capa 3. Esto se debe a que se pude establecer un mapeo directo entre las funcionalidades de SAAL y las de capa 2 del modelo OSI. Así, a SAAL se le conoce como capa 2 y por extensión la capa de señalización en ATM se suele nombrar como capa 3.

4.8. Datos sobre ATM

En la figura 4.25 se recoge como las redes IP se han sustentado sobre diversas tecnologías, siendo posiblemente la más extendida o conocida las basadas en los desarrollos de la familia 802 del IETF.

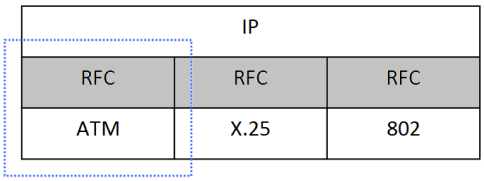

Figura 4.25: IP cásico sobre ATM

Estudiaremos en este apartado IP clásico sobre ATM, que se basa en dos aspectos principales:

- *Encapsulado de Paquetes sobre conexiones ATM:* donde estudiaremos el encapsulado multiprotocolo sobre AAL5, definido en la RFC 2684.
- *Resolución de direcciones IP a direcciones ATM:* donde estudiaremos IP y ARP[9] clásicos sobre ATM, definidos en la RFC 2225.

[9] ARP: Address Resolution Protocol.

Los encaminadores IP tratan las redes ATM como un tipo de subred más (modelo overlay), lo cual proporciona una serie de ventajas inherentes ya que los usuarios están familiarizados con este método. Así, el despliegue y la aceptación de ATM en el mundo IP serán más rápidos, teniendo en cuenta además que la administración y el control de acceso se basan en cortafuegos (firewalls) que los equipos ATM no deberían sortear.

Existen otros desarrollos de la industria para el interfuncionamiento de IP y ATM, como Multi-Protocolo sobre ATM (MPOATM) que no estudiaremos, y también aprovechamos este lugar para introducir la tecnología MPLS (Multi Protocol Label Switching), que surge como evolución o mejora sobre ATM para soportar redes IP y que estudiaremos en el último apartado de este capítulo.

Con modelo clásico de IP sobre ATM, entendemos el tratamiento de un host adaptador ATM como interfaz de red para la torre de protocolos IP, operando en un paradigma basado en LAN. En particular, este modelo clásico viene caracterizado por los siguientes factores:

- Una subred IP es utilizada por muchos hosts y routers. Cada VC conecta directamente dos entidades IP dentro de la misma subred lógica IP (Logical IP Subnetwork LIS).
- Las direcciones IP son resueltas a direcciones ATM mediante el uso del servicio ATMARP dentro de su LIS.
- Se utiliza el mecanismo de encapsulado de paquetes IP LLC/SNAP (Logical Link Control/Subnetwork Attachment Point).
- Se define la Unidad Máxima de Transmisión (MTU), que se utilizará para todos las VCs en una misma LIS.
- La arquitectura de direccionamiento extremo a extremo permanece intacta.

El modelo clásico sugiere dos posibles áreas de aplicaciones para el despliegue de ATM. El uso principal sería para reemplazar a las tecnologías tradicionales empleadas en LAN, como ethernet, mientras que en el segundo escenario se utilizaría ATM para interconectar routers.

4.8.1. Encapsulado Multiprotocolo sobre AAL5

En la encapsulación multiprotocolo sobre AAL5, RFC 2684, se definen dos métodos para transportar tráfico multiprotocolo sobre AAL5. El primer método, denominado encapsulación LLC, permite que paquetes pertenecientes a diferentes protocolos puedan ser multiplexados sobre una misma

conexión VC, con una cabecera añadida al paquete. El segundo método, denominado Multiplexado VC, realiza una multiplexación de capa más alta implícitamente por la conexión ATM, es decir, un sólo tipo de paquetes por cada conexión (VC).

- **Encapsulado LLC.** Los paquetes pertenecientes a múltiples protocolos se multiplexan sobre un mismo VC. La necesidad de multiplexión surge cuando una fuente necesita usar la misma conexión VC para transportar paquetes de varias aplicaciones hacia el mismo destino. Una cabecera en cada PDU identifica el protocolo que está siendo transportado en la trama AAL5.

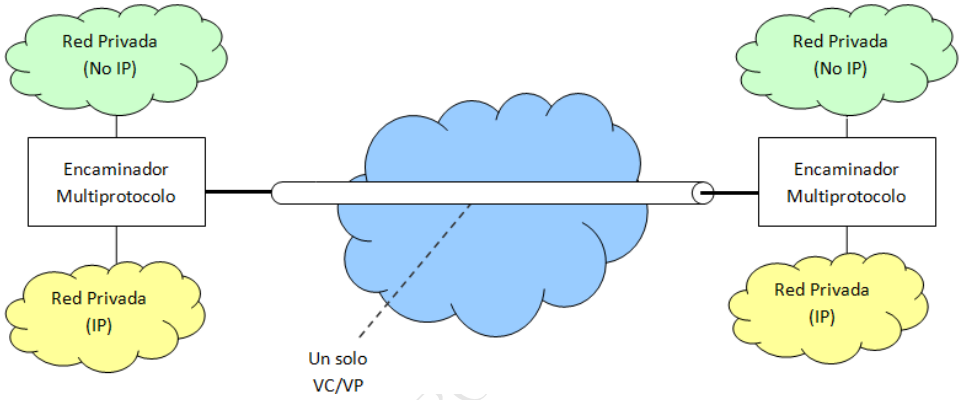

Figura 4.26: IPoATM: Encapsulado en LLC/SNAP

Sin entrar en una descripción detallada, la figura 4.27 recoge los formatos de la cabecera utilizada en el encapsulado LLC/SNAP. Se permite una MTU (Maximum Transmission Unit) de 9180 octetos, aunque se permite llegar al máximo de 65536 octetos, soportado por AAL.

- **Encapsulado por Multiplexado VC.** El protocolo de los paquetes es implícitamente detectado por la conexión VC existente entre los dos equipos ATM. Esto es, cada protocolo es transportado sobre una conexión VC independiente, por lo que la conexión identifica el protocolo. El protocolo transportado es configurado de forma manual o dinámica durante la fase de establecimiento del canal virtual. Así, no hay necesidad de añadir una cabecera para identificar el protocolo, aunque como contrapartida implica un aumento de carga al tener que establecer y liberar numerosas conexiones VCs.

4.8.2. Resolución de direcciones

IP clásico sobre ATM define una entidad lógica llamada Subred Lógica IP (LIS). Una LIS consta de hosts ATM adjuntos y routers, configurados de

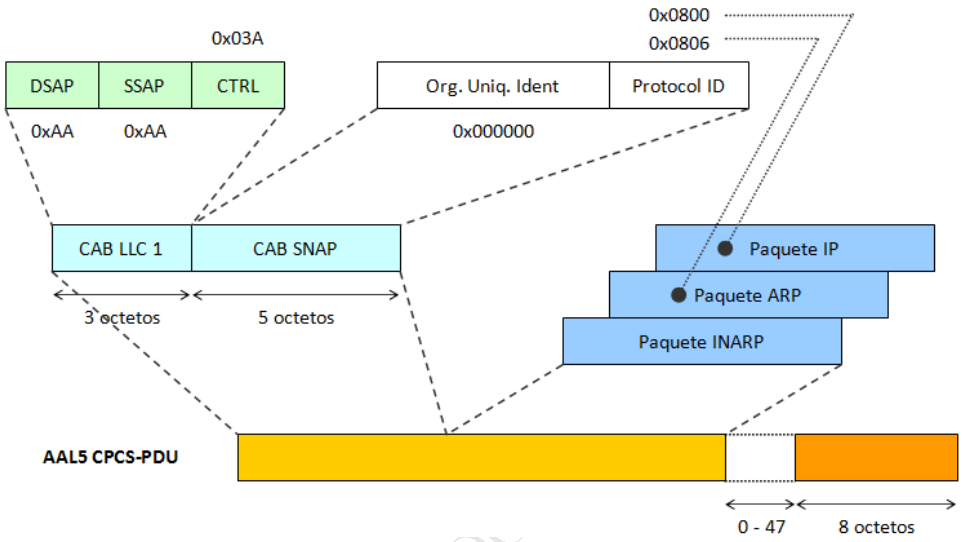

Figura 4.27: IPoATM: Formato cabeceras LLC/SNAP

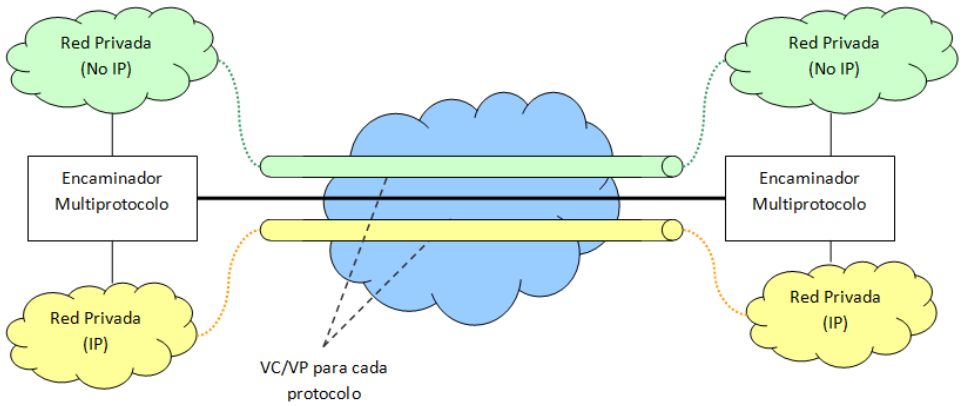

Figura 4.28: IPoATM: Encapsulado sobre Canal Virtual

manera similar a una subred IP convencional. Los requerimientos específicos para hosts/routers en una LIS incluyen:

- Todos los miembros de la LIS tienen el mismo número de red/subred IP y máscara.
- Todos los miembros de la LIS están conectados directamente a la red ATM.
- Todos los miembros de la LIS tienen un mecanismo para resolver direcciones IP a direcciones ATM mediante servicios ATMARP y viceversa, mediante servicios IN-ATMARP, cuando utilizan una conexión ATM SVC.
- Todos los miembros de la LIS tienen un mecanismo para resolver VCs a direcciones IP mediante IN-ATMARP, cuando utilizan una conexión ATM PVC.
- Todos los miembros de la LIS son capaces de comunicar mediante ATM con el resto de miembros de la misma LIS.

Cada LIS en una red ATM opera y se comunica de manera independiente de otras LIS dentro de la red ATM. El alcance del servicio ATMARP está restringido dentro de la LIS. Los nodos que pertenecen a diferentes LIS pueden comunicarse mediante routers.

Un nodo que desee comunicarse con otro nodo en una LIS necesita conocer la dirección ATM correspondiente a la dirección IP del nodo destino. Para lograr esta correspondencia, la RFC 2225 define el servicio ATMARP. El servicio ATMARP es similar al Address Resolution Protocol (ARP) definido para medios basados en difusión, como Ethernet o Token Ring. El método exacto a seguir depende si se están utilizando SVCs o PVCs.

En un entorno con SVC, se utiliza un servidor ATMARP para la resolución de direcciones. Dicho servidor mantiene una base de datos centralizada de direcciones IP y sus correspondientes direcciones ATM de todos los nodos que pertenecen a una LIS. Esta base de datos es consultada por todos los nodos ATM cuando necesitan resolver una dirección ATM.

En el momento de inicialización, marcado como instante [1] en la figura 4.29 un nodo cliente en la LIS establece una conexión con el servidor ATMARP. La dirección del servidor ATMARP está preconfigurada en el nodo. Seguidamente el servidor pregunta al nuevo cliente sus direcciones IP y ATM. El servidor utiliza esta información para mantener actualizada la base de datos para atender futuras consultas ATMARP.

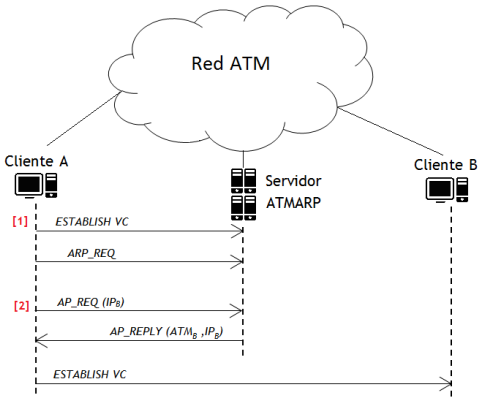

Figura 4.29: IPoATM: Resolución de direcciones

Suponiendo que el cliente quiera conectarse con otro nodo, instante [2], pregunta al servidor y obtiene la dirección ATM correspondiente a la dirección IP del nodo al que desea conectar, pudiendo establecer entonces la conexión con el nodo deseado.

En un entorno con PVC, un nodo no tiene la capacidad de establecer una conexión con el servidor ATMARP y no puede usar ATMARP, por lo que en este caso se utiliza IN-ATMARP, o ATMARP inverso. El protocolo ATMARP inverso, definido en la RFC 2390, proporciona un mecanismo para que un nodo conozca la dirección IP del nodo destino, correspondiente a una conexión PVC abierta. Utilizando el mecanismo ARP inverso, un nodo puede conocer todas las direcciones IP alcanzables por él. Este mecanismo es una opción ligeramente mejor que establecer una configuración estática de todas las IPs alcanzables.

En cualquier caso, existen una serie de limitaciones en la resolución de direcciones sobre ATM, que pasamos a enumerar:

- No hay multicast.
- No permite enviar datos hasta que la conexión ATM se ha establecido.
- No permite conexiones directas entre subredes lógicas.
- No hay soporte de calidad de servicio.
- Cuello de botella en los elementos de interconexión.

IP clásico sobre ATM tiene limitaciones en términos de envío de datos cuando los nodos pertenecen a LIS diferentes. Así, cuando un nodo perteneciente a una LIS quiere enviar información a otro nodo en otra LIS, necesita

conocer la relación entre la dirección ATM y la dirección IP de dicho nodo destino. Para proporcionar esta relación, el IETF proporciona el protocolo de resolución de salto siguiente, o Next Hop Resolution Protocol (NHRP), definido en la RFC 2332 y del que se recoge un ejemplo en la figura 4.30.

En el protocolo NHRP se distinguen las entidades Clientes y los NHS o Next Hop Servers. Sin entrar en detalle, el protocolo NHRP suele ser iniciado por un nodo, S por ejemplo, que quiere enviar un paquete a otro nodo, por ejemplo D, que pertenece a otra LIS. Para hacerlo, S necesita la dirección ATM de D (S ya posee la dirección IP de D, que ha sido proporcionada por la capa IP). Así, el nodo S comprueba primero su caché local por si la existiera una relación ya conocida entre las direcciones IP y ATM de D. En caso positivo, se utilizaría la dirección ATM para establecer una conexión VC, si no estuviera ya establecida, y se enviaría el paquete.

En caso contrario se inicia el protocolo NHRP, realizando una petición NHRP al NHS. El NHS busca en su propia caché por la existencia de ese mapeo o relación entre la IP y la dirección ATM de D. Si el NHS conoce la información, envía la respuesta al nodo S y en caso contrario, el NHS inicia otra petición NHRP hacia otro NHS. Este procedimiento se va repitiendo hasta alcanzar al NHS que sirve al nodo D y que sí conoce la correspondencia entre las direcciones IP y ATM. Este NHS responde al anterior, y la respuesta va viajando de vuelta por los mismos NHS que tuvieron que realizar consulta NHRP hasta llegar la respuesta al nodo S y entonces se utilizaría la dirección ATM para establecer una conexión VC y se enviaría el paquete.

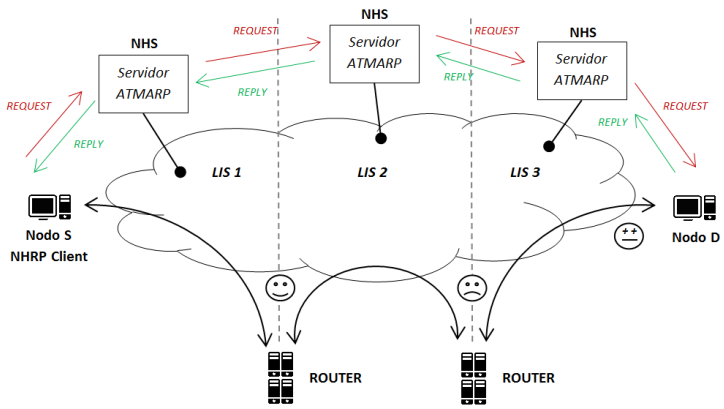

Figura 4.30: IPoATM: Ejemplo de encaminamiento con varias LIS

Existe otro enfoque o solución a este problema, que es el que nosotros utilizaremos, y que también se recoge en la figura 4.30. Cuando un cliente

quiere conectar con un cliente que se encuentra en otra LIS, lo hace enviando sus paquetes IP a través de un encaminador, realizando el encaminamiento totalmente en IP. Por tanto, en cada salto, puede ser necesario establecer nuevas conexiones ATM en cada LIS entre los encaminadores, hasta llegar al encaminador que esté sirviendo a la LIS del cliente destino. Así los paquetes IP atravesarán diferentes conexiones ATM y diferentes encaminadores.

4.9. Fundamentos de control de tráfico

Se ha comentado en numerosas ocasiones, la capacidad de las redes ATM para ofrecer diferentes Quality of Service (QoS). Pero, *¿cuáles son los parámetros que definen la QoS? ¿Cómo se define la calidad del servicio en ATM? ¿Todos los usuarios de ATM necesitan la misma calidad de servicio?*

Trataremos de responder a éstas y similares cuestiones en este apartado del capítulo. Para ello, en primer lugar estudiaremos dos conjuntos de parámetros que nos ayuden en estas tareas.

El primer conjunto es el llamado **parámetros de tráfico**, utilizados para obtener medidas cuantitativas de las características del tráfico de datos. El segundo conjunto son los **parámetros de calidad del servicio**, parámetros que cuantifican la calidad con la que la red está transportado tráfico de usuario, siempre desde una perspectiva propia a la red.

Conocidos todos los descriptores, se realiza una clasificación de los servicios ATM en seis categorías. Estas categorías de servicio esencialmente relacionan las características del tráfico y los requerimientos de QoS que serán necesarios obtener de la red para poder soportar dichos servicios.

Es importante tener siempre presente el orden de magnitud habitual en conexiones de datos ATM. Una conexión ATM, desde su fase de establecimiento hasta la de liberación puede ser medida en el orden de minutos. Durante todo ese tiempo, y debido a la naturaleza del tráfico se producirán ráfagas de datos del orden de fracciones de segundo. Las ráfagas por supuesto están formadas por la transmisión de células, cuyo duración es del orden de microsegundos (μs). Estas relaciones temporales quedan reflejadas en la figura 4.31.

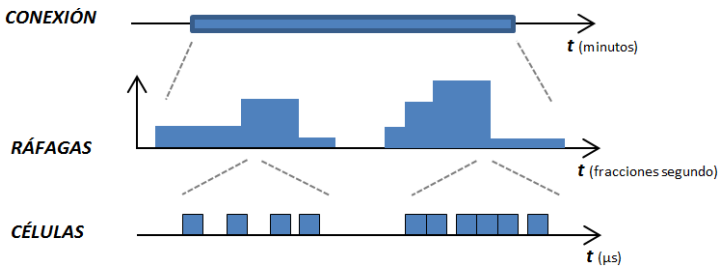

Figura 4.31: Flujo de Células ATM

4.9.1. Parámetros de tráfico

En ATM, se definen varios parámetros de tráfico. Algunos de ellos se agrupan juntos para formar los descriptores de origen de tráfico. Como sugiere su nombre, estos indicadores son un conjunto de indicadores de tráfico asociados a una fuente u origen de tráfico ATM. Los principales parámetros de tráfico son:

- **Tasa de Pico (Peak Cell Rate, PCR):** es la tasa máxima [b/s] a la que un usuario se le permite inyectar datos en la red. Específicamente, el PCR define un límite superior para el tráfico que puede ser enviado por una fuente de datos ATM. Su inverso nos da el valor mínimo de tiempo entre llegada de datos.

- **Máxima Longitud de Ráfaga (Maximum Burst Size, MBS):** cantidad de datos [células] que una fuente ATM puede enviar a su pico de tasa de células. Específicamente, es el número de células que se pueden enviar la tasa PCR. Conocidas PCR y MBS, la duración máxima de ráfaga viene determinada por $T_{MBS} = MBS/PCR$

- **Tasa Sostenible (Sustainable Cell Rate, SCR):** es la medida a largo término de la media de tráfico de usuario [b/s]. Específicamente es un límite superior de la media a largo plazo de las células transmitidas en una conexión.

- **Tolerancia de Ráfaga (burst Tolerance, BT):** es una medida del intervalo entre ráfagas consecutivas en las que las células se envían a PCR. En otras palabras, BT es el tiempo [s] tras el que una fuente ATM puede enviar de nuevo datos a su tasa máxima PCR, sin violar a largo plazo el término SCR.

- **Mínima Tasa de Célula(Minimum Cell Rate, MCR):** este parámetro está definido para aplicaciones de baja prioridad. Específicamente es la tasa mínima de células [b/s] que la red puede ofrecer a una conexión. Este valor puede ser incluso nulo.

- **Máximo Tamaño de Trama (Maximum Frame Size, MFS):** este parámetro especifica el tamaño máximo de AAL PDU ([bits]), para la categoría de servicio de Tasa de transferencia garantizada (Guaranted Frame Rate).

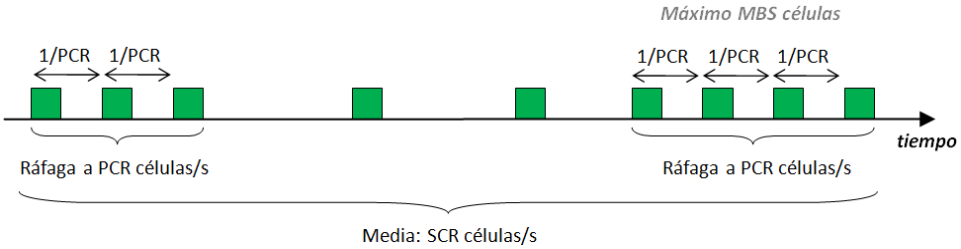

Figura 4.32: Parámetros de Tráfico

El ejemplo siguiente pone de manifiesto el uso y la información proporcionada por estos parámetros.

Un proceso de toma de medidas genera un paquete de 150 octetos cada 20 ms. Las medidas se envían por una conexión ATM con AAL5. El intervalo entre células del mismo paquete es 1 ms. Calcular los parámetros de tráfico de la conexión.

Dentro de un paquete, se transmite una célula cada 0,0001 s, por lo tanto:

$$PCR = 1000\,células/s = 1000 \times 53 \times 8\,/s = 424\,Kbit/s \qquad (4.1)$$

Para el cálculo del MBS vemos la capacidad de usuario por célula, teniendo:

$$150\,octetos/48\,octetos = 3,125 \Longrightarrow MBS = 4\,células \qquad (4.2)$$

En media, se transmiten

$$SCR = 4\,células/0,02s = 200\,células/s = 84,8\,Kbit/s \qquad (4.3)$$

4.9.2. Parámetros de Calidad de Servicio (QoS)

En ATM, los parámetros de calidad del servicio normalmente se denominan Calidad del Servicio (QoS). La recomendación ATMF TM 4.1, de ATM Forum, especifica 6 parámetros de QoS. Dependiendo de la capacidad de la red y los requerimientos de las conexiones individuales, una red puede ofrecer uno o más parámetros. Los seis parámetros definidos son:

- Probabilidad de Pérdida de Células (Cell Loss Ratio, CLR).
- Retardo de tránsito máximo (Maximum Cell Transfer Delay, max CTD).
- Variación del retardo pico a pico (Peak to peak Cell Dellay Variation, CDV)
- Tasa de Error de Células (Cell Error Rate, CER).
- Tasa de fallo de inserción de célula (Cell Mis-insertion Ratio, CMR).
- Tasa de bloques de células con errores severos (Severely Errored Cell Block Ratio, SECBR).

Comentar que los tres primeros parámetros son negociables con la red, mientras que los tres últimos no lo son. Negociable implica que la resolución de un valor concreto para uno de esos parámetros pueda ser fijado por el usuario o no. No obstante, la red puede decidir si el valor negociado por el usuario es aceptado o no.

La figura 4.33 recoge como se interrelacionan dichos parámetros.

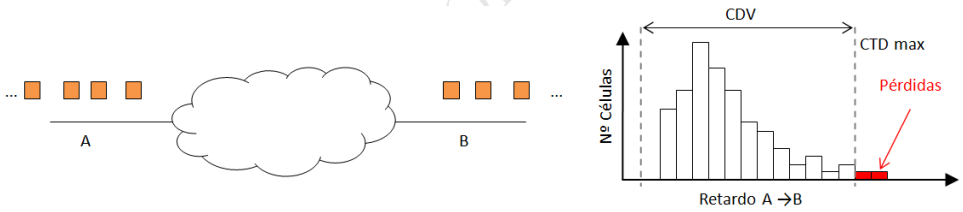

Figura 4.33: Parámetros de QoS

4.9.3. Tipos de conexiones ATM

Dependiendo de un número de atributos, los servicios ATM se clasifican en las siguientes seis categorías:

1. **CBR:** Constant Bit Rate.
2. **rt-VBR:** Real Time Variable Bit Rate.
3. **nrt-VBR:** Non Real Time Variable Bit Rate.
4. **UBR:** Unspecified Bit Rate.
5. **ABR:** Available Bit Rate

6. **GFR:** Guaranted Frame Rate.

Como decimos, esta clasificación se basa en uno o más de los siguientes atributos:

- *Sensibles al tiempo:* algunas de estas categorías requieren límites estrictos para el retraso o para la variación del retraso, como por ejemplo aplicaciones de voz o vídeo. Esta es la razón de por qué los parámetros CTD y CDV se especifican para estas categorías. CBR y rt-VBR son ejemplos de categorías de servicios sensibles al tiempo.
- *Naturaleza del Tráfico:* algunas aplicaciones requieren de tasas fijas de datos (voz) mientras que para otras es indiferente (datos). para estas últimas es preferible compartir el ancho de banda de manera estadística entre un cierto número de aplicaciones. Categorías de servicio que se acomodan a estas aplicaciones son nrt-VBR, ABR, UBR o GFR. Dependiendo de la categoría del servicio, se especifican unos u otros parámetros. Por ejemplo, para nrt-VBR se especifica SCR y para ABR se especifica MCR.
- *Aprovisionamiento:* para alcanzar los requerimientos de algunas aplicaciones, la red debe reservar ciertos recursos. Dicho aprovisionamiento puede implicar costes de mantenimiento más altos. Desde otro punto de vista, la red puede ofrecer ancho de banda excedente a menor precio, como por ejemplo en UBR. UBR es útil para aplicaciones de baja prioridad que pueden asumir retrasos excesivos e incluso pérdida de células.

Sin entrar en mayor detalle, la tabla 4.5 recoge las principales diferencias de cada categoría de servicio, listando características de cada categoría respecto a su sensibilidad al tiempo, prioridad e incluso respecto a descriptores de tráfico y de servicio.

4.10. MPLS. Conmutación de etiquetas multiprotocolo

Multi Protocol Label Switching (MPLS), traducido como Conmutación de Etiquetas Multiprotocolo, es un nuevo desarrollo de la industria, estandarizado por el IETF. A pesar de su nombre, la realidad es que MPLS se ha utilizado de manera casi exclusiva para soportar el protocolo de internet IP, énfasis que se debe principalmente al gran éxito de Internet en los últimos años.

Mientras que IP es un protocolo no orientado a conexión que es capaz de trabajar en redes de datos sin requerimientos de QoS, ATM es popular

Servicio	**Parámetros Trafico**	**Naturaleza Trafico**	**Parámetros QoS**	**Sensibilidad Tiempo**	**Aplicaciones**
CBR	PCR, CDVT	Estable	maxCTD, CDV, CLR	Sí	Voz, vídeo sin compresión
rt-VBR	PCR, CDVT, SCR, MBS	Ráfagas	maxCTD, CDV	Sí	Voz, vídeo comprimido
nrt-VBR	PCVR, CDVT, SCR, MBS	Ráfagas	CLR	No	Datos, transferencias bancarias, multimedia, e-mail
UBR	PCR, CDVT, SCR, MBS	Ráfagas	N/A	No	E-mail, FTP
ABR	PCR, CDVT, MCR	Ráfagas	CLR bajo	No	E-mai, FTP
GFR	PCR, CDVT, MCR, MBS, MFS	Ráfagas	CLR bajo	No	E-mail, FTP

Tabla 4.5: Categorías de Servicio ATM

por proporcionar servicios de red que sí requieran de ciertos mínimos en parámetros de QoS. MPLS puede ser descrito como una aproximación entre IP y ATM, que fusiona la flexibilidad de los protocolos de encaminamiento de IP con la velocidad de los conmutadores ATM, para lograr conmutación rápida de paquetes en redes IP.

Se puede entender que el objetivo de MPLS es acelerar la conmutación, integrando encaminamiento en capa de red (no sólo IP) con la conmutación en capa de subred (enlace).

Los requerimientos para MPLS han estado siempre relacionados con las deficiencias históricamente observadas en el protocolo IP, entre las que destacamos:

- **Mecanismo de reenvío eficiente:** la complejidad de los algoritmos que los routers IP implementan se está convirtiendo en un cuello de botella, debido al continuo aumento de tráfico en las redes actuales. Los routers IP implementan un algoritmo **longest-match prefix**, para determinar el próximo salto de un paquete. Este es un algoritmo intensivo, que se repite en cada nodo para cada paquete hasta alcanzar el destino, por lo que se hace necesario un método de reenvío más eficiente.
- **Soporte para ingeniería del tráfico y encaminamiento explícito:** la ingeniería del tráfico es la disciplina que trata de obtener un uso óptimo de los enlaces existentes en una red. Esto requiere de balanceo de cargas en los enlaces para evitar que unos terminen sin uso mientras otros están congestionados. Un concepto relacionado es el de encaminamiento explícito, donde un nodo puede especificar de forma explícita el camino a seguir para alcanzar el destino, en lugar de realizar una decisión de salto al siguiente nodo en cada nodo. Desgraciadamente, IP no tiene mecanismos para dar soporte de forma elegante a estos conceptos.
- **Soporte para QoS:** el tráfico IP ha sido tradicionalmente diseñado para proporcionar un servicio *best-effort.* Sin embargo, los usuarios cada vez son más demandantes en términos de QoS y las redes IP tradicionales no tienen medios para proporcionar garantías de QoS.

MPLS fue desarrollado para solventar éstas y otras carencias (distribución de etiquetas propietarias, multidifusión, múltiples protocolos en capa de subred, escalabilidad, ...) de las redes IP clásicas.

Para estudiar y entender MPLS, hemos de repasar una serie de conceptos previos. En primer lugar vamos a establecer las diferencias entre un encaminador (router) y un conmutador (switch).

- **Encaminador - Router:** Un router, también conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante puentes), y que por tanto tienen prefijos de red distintos.

  El funcionamiento básico de un encaminador consiste en almacenar un paquete y reenviarlo a otro encaminador o al host final. Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de enrutamiento.

  Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

  - *Reenvío de paquetes (Forwarding):* cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado, almacenado en la tabla de información de reenvío (Forwading Information Base, FIB) o comúnmente tabla de encaminamiento. Una característica importante de los routers es que no difunden tráfico broadcast.
  - *Enrutamiento de paquetes (Routing):* cuando cambia la información de encaminamiento, almacenada en la tabla conocida como base de Información de encaminamiento (Routing Information Base, RIB) el router mediante el uso de algoritmos de enrutamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor, actualizando la tabla de encaminamiento

  Por tanto, debemos distinguir entre reenvío y enrutamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla FIB, mientras que por enrutamiento se entiende el proceso de hacer esa tabla, a partir de la información del entorno que se va almacenando en la tabla RIB. Cuando esta tabla cambia, se ejecutan los algoritmos para actualizar la FIB.

- **Conmutador - Switch:** Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

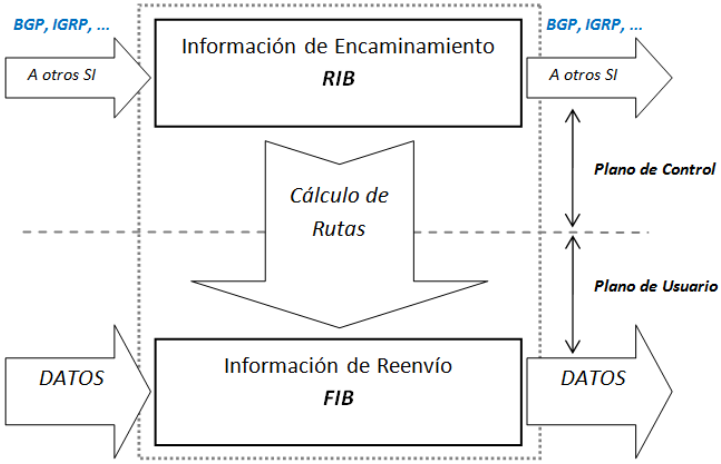

Figura 4.34: Funcionamiento de un encaminador

Así, en un entorno clásico, los encaminadores buscan en la FIB el prefijo coincidente más largo, repitiéndose el proceso de búsqueda/asignación en cada salto, mientras el paquete atraviesa una red de encaminadores. Por su parte, los conmutadores buscan en su tabla una coincidencia total para reenviar el paquete.

MPLS se diseñó para evitar este proceso salto a salto de clasificación y reenvío. En una red MPLS, formada por encaminadores/conmutadores LSR (Label Switching Router) la clasificación de un paquete en una clase de equivalencia para reenvío (Forwarding Equivalence Class, FEC) se realiza únicamente en el punto de ingreso en la red MPLS. Es decir, la clasificación del paquete se realiza únicamente en el momento de su ingreso en el dominio MPLS, asignándosele en este proceso una etiqueta (Label) al paquete. El resto de nodos, por los que pase el paquete, únicamente realizan una consulta a una tabla de etiquetas para conmutar el paquete hacia su destino.

En gran medida, el concepto de etiquetas y tablas de etiquetas en MPLS es similar al concepto de VPI/VCI y tablas de traducciones VPI/VCI en ATM. Del mismo modo que los protocolos de señalización de ATM trabajan para rellenar las tablas de traducción en todos los conmutadores ATM, MPLS requiere de un protocolo para rellenar sus tablas de etiquetas en todos los encaminadores MPLs dentro de un dominio. Este protocolo se conoce como Protocolo de Distribución de Etiquetas (Label Distribution Protocolo, LDP)[10].

Por tanto, trataremos ahora de reagrupar una serie de conceptos que

[10]IETF ha definido el Resource Reservation Protocolo (RSVP) con la misma función.

hemos de tener en cuenta para el estudio en detalle del funcionamiento de una red MPLS.

- **Label Switching Router, LSR:** podemos definir los LSR como routers (típicamente IP) que implementan los procedimientos de distribución de etiquetas y pueden reenviar paquetes usando las etiquetas como información. Existen distintos tipos de LSR, pero nos centraremos en una clasificación sencilla con dos tipos de LSR:
  - *LSR Normal*: nodo LSR en el interior de una red MPLS.
  - *LSR Frontera:* nodo LSR que limita con el exterior de la red IP. Estos nodos realizan la transición entre el enrutado en el dominio IP normal y el enrutado en el dominio MPLS. Es decir son los encargados de imponer las etiquetas o de removerlas de los paquetes IP. Un nodo LSR que tenga al menos un vecino no MPLS es considerado un LSR frontera.

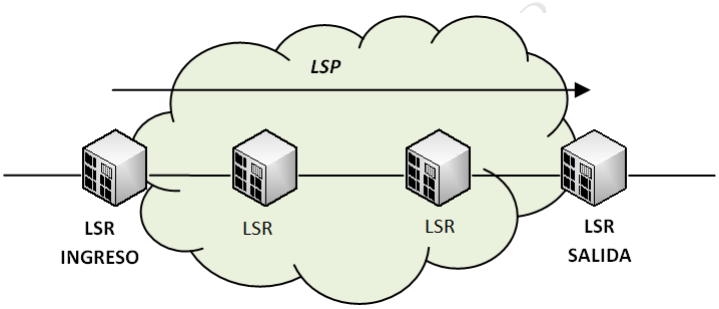

Figura 4.35: Red MPLS

- **Forwarding Equivalence Class, FEC:** clase de equivalencia de reenvío o conjunto de datagramas que se reenvían de la misma forma, es decir, que se les puede asignar la misma etiqueta. Normalmente es una partición de la FIB, es decir, se corresponde con una subred IP, pero también puede realizarse una clase de equivalencia para tráfico con alguna característica determinada, como por ejemplo para distinguir tráfico multimedia del resto de tráfico hacia una subred IP. Por tanto, se corresponde con un subconjunto de paquetes IP que son tratados de la misma manera por un router. Podemos decir que en el routing convencional, cada paquete está asociado a un nuevo FEC en cada salto. En MPLS esta operación sólo se realiza la primera vez que el paquete entra en la red.
- **Etiqueta:** identificador de FEC con significado local entre dos nodos MPLS. Tienen una longitud fija.
- **Flujo:** conjunto de datagramas de un origen a un destino.

- **Flujo Agregado:** la agregación es el proceso de asociar una sola etiqueta con un conjunto de FECs. Así varios flujos compartirán ruta, o se verán como un único flujo entre un origen y un destino, que puede ser interno o parcial en la red MPLS.

- **Label Switching Path, LSP:** senda conmutada o secuencia de etiquetas que determinan una ruta unidireccional entre un origen y un destino.

Es importante destacar que en los routers LSR sigue siendo necesario el uso de los protocolos de encaminamiento IP, para generar la base de conocimiento sobre la que generar posteriormente la tabla de encaminamiento de etiquetas o **Label Forwarding Information Base (LFIB)**, tal y como se recoge en la figura 4.36.

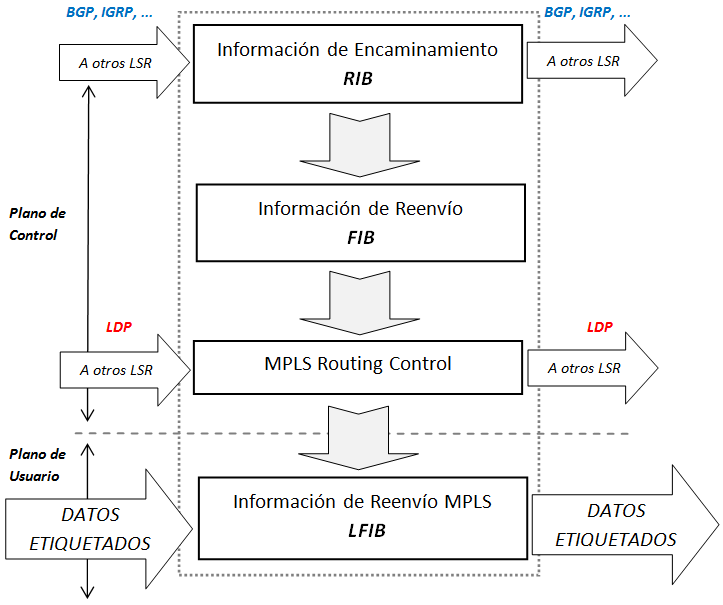

Figura 4.36: Funcionamiento de un LSR

Se utiliza la LFIB para propagar paquetes etiquetados a través de la red MPLS, de manera similar a como se hace en ATM con los identificadores VPI/VCI.

4.10.1. Funcionamiento Básico de MPLS

En la figura 4.37 se recoge un ejemplo de funcionamiento básico en una red MPLS, para dos paquetes que entran en dicha red (paquetes A y B).

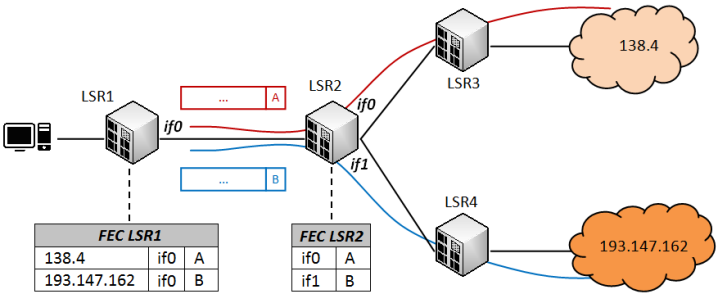

Figura 4.37: Ejemplo funcionamiento básico MPLS

El router LSR2 interconecta dos subredes IP distintas y genera para cada una de ellas una clase de equivalencia, es decir, les asigna una etiqueta a cada una de ellas (A y B). Posteriormente, transmite a su nodo vecino esta información. Así, cuando se recibe un datagrama en el LSR de ingreso a la red MPLS, es decir a LSR1, se realiza una búsqueda IP tradicional, pero asignando al paquete finalmente la etiqueta correspondiente a esa FEC y se envía el datagrama ya etiquetado a la red MPLS. Al llegar a LSR2, se realiza la conmutación de los paquetes, únicamente consultando su tabla de etiquetas, y en este caso s extrae la etiqueta para poder entregar a la subred destino el paquete original no etiquetado.

En cada salto, como veremos más adelante, es posible realizar operaciones sobre el etiquetado del paquete.

Una etiqueta MPLS es un campo de 32 bits, que sigue la estructura recogida en la figura 4.38. Los primeros 20 bits son el valor de la etiqueta, que por tanto tienen a priori un rango de valores entre $[0,2^{20-1}]$=[0,1.048.575]. No obstante, los 15 primeros bits están exentos de uso normal. Los bits 20 a 22 componen el campo **EXP**, correspondiente a 3 bits denominados experimentales en la recomendación, utilizados únicamente para motivos de QoS. El bit 23, se conoce como el bit de fondo de pila (**Bottom of Stack, BoS**), y su valor es siempre cero, a no ser, que ciertamente sea el último elemento de la pila de etiquetas, tomando para indicarlo el valor uno. La pila en este caso es el conjunto de etiquetas que encontramos encabezando el paquete de datos que se mueve por la red MPLS. Los bits 24 a 31 componen el campo de tiempo de vida (**Time To Live, TTL**), campo que tiene exactamente el mismo significado que en IP, es decir, es un contador que va decreciendo una unidad en cada salto, de modo que si el contador llega a cero, el paquete se descarta.

Queremos hacer hincapié nuevamente en que las etiquetas pueden ser apilables, es decir, un LSR puede necesitar más de una etiqueta para en-

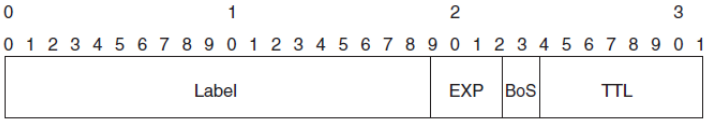

Figura 4.38: Etiqueta MPLS

caminar el paquete en la red[11], de modo que las etiquetas se apilan en la cabecera del paquete, teniendo todas el bit BoS a cero, menos la última que lo llevará a uno.

Pero, **¿dónde colocamos la etiqueta MPLS?** El encapsulado general viene recogido en la norma RFC 3032, donde se establece que la etiqueta MPLS debe situarse entre la cabecera de capa 2 y el paquete de capa 3 transportado[12], como recoge la figura 4.39.

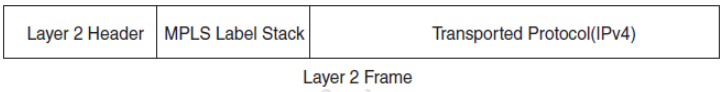

Figura 4.39: Ubicación etiqueta MPLS

El protocolo transportado puede ser en teoría cualquiera, pero nosotros lo estudiaremos únicamente con IPv4. Pueden ser transportados incluso protocolos de nivel 2 como Frame Relay, PPP, HDLC, ATM y Ethernet.

Una vez que la pila de etiquetas MPLS es insertada entre la cabecera de capa 2 y la carga de datos de capa 3, el router que la envia debe tener algun medio para indicar al router receptor que el paquete que está siendo transmitido no es un datagrama IP puro, sino un datagrama etiquetado MPLS. Para ello, se definieron nuevos tipos de protocolo sobre la capa 2 como:

- En entornos LAN los paquetes etiquetados que portan paquetes IP unicast o multicast utilizan un *ethertype* con valores 0x8847 y 0x8848. Estos valores del campo ethertype de la trama ethernet se pueden utilizar directamente en medios ethernet (Fast Ethernet y Gigabit Ethernet) así como parte de la cabecera SNAP en otras tecnologías LAN, como Token Ring o FDDI.
- En enlaces punto a punto utilizando encapsulado PPP se introdujo un nuevo protocolo denominado MPLS Control Protocol (MPLSCP). Los

[11] Como en MPLS VPN.

[12] Por su situación y también porque es difícil encuadrar MPLS en el modelo OSI, suele decirse que es un protocolo de capa 2.5

paquetes MPLS se marcan con un campo de protocolo PPP de valor 0x8281.

- Paquetes MPLS transmitidos a través de Frame Relay son marcados con un identificador DLCI.
- Paquetes MPLS transmitidos en una red ATM se encapsulan con una cabecera SNAP que utiliza un ethertype con los mismos valores que en entornos LAN (0x8847 y 0x8848).

No obstante, aparte del encapsulado general, las etiquetas MPLS se pueden portar mediante el uso de otras capas, como por ejemplo, utilizando la cabecera del datagrama en IPv6, o los identificadores VCI/VPI en ATM, ... Es decir, utilizando protocolos de nivel 3, que tengan capacidad para identificar flujos.

Una vez estudiado el mecanismo básico de funcionamiento en una red MPLS estudiaremos los principales procedimientos que se implementan en MPLS para el tratamiento de etiquetas.

4.10.2. Tratamiento de Etiquetas

Estudiaremos a continuación las principales tareas relacionadas con la gestión de etiquetas, y por tanto de encaminamiento, en una red MPLS. Las tareas que estudiaremos son la *asignación, distribución, fusión o agregación de flujos, operaciones y conservación de etiquetas.*

Asignación

La asignación de etiquetas es la acción que asocia una etiqueta a un flujo. Es un proceso local a un LSR, es decir, es el propio conmutador en el que decide la asignación.

La asignación se realiza en sentido contrario al flujo, y la puede llevar a cabo:

- *El nodo siguiente:* que es el que va a usar la etiqueta como índice de la tabla de envío.
- *El nodo siguiente bajo demanda:* situación en la que en nodo anterior pide una etiqueta para una FEC.

Esta última situación se da cuando el nodo anterior manda una serie de paquetes iguales y el posterior no le pide que les asigne una etiqueta,

entonces el anterior puede solicitar que se haga.

Los dos métodos de asignación anteriores pueden coexistir en la red, pero no entre nodos vecinos, independientemente del mecanismo de distribución de etiquetas utilizado, aspecto que estudiaremos a continuación.

Cerraremos esta sección discutiendo sobre el alcance y la unicidad de las etiquetas. Lo haremos iniciando la discusión con un ejemplo que nos ayude a comprender los conceptos y utilizaremos la idea ya introducida de nodos previos y siguientes, relativos a la asignación de etiquetas.

Un LSR dado Rd (nodo siguiente) puede asociar la etiqueta L con el FEC F, y distribuir ese enlace al punto Ru1 (nodo previo). Rd puede también asociar la etiqueta L con el FEC F, y distribuir ese enlace con el punto Ru2 (nodo previo)[13].

Un LSR dado Rd puede asociar la etiqueta L con el FEC F1, y distribuir ese enlace al punto Ru1. Rd puede también asociar la etiqueta L con el FEC F2, y distribuir ese enlace con el punto Ru2.

Si y sólo si, Rd puede decir, al recibir un paquete cuya etiqueta en la cima sea L, si fue puesta por Ru1 o por Ru2, entonces la arquitectura no requiere que F1 = F2.

En estos casos, podemos decir que el espacio de etiquetas que Rd está empleando para las etiquetas que distribuye en Ru1 es diferente al de Ru2. En general, Rd sólo puede decir si fue Ru1 o Ru2 el que puso esa etiqueta en concreto si se dan estas condiciones:

- Ru1 y Ru2 son los únicos puntos de distribución de etiquetas a los que Rd distribuyó la etiqueta L.
- Ru1 y Ru2 están conectados directamente a Rd vía un interfaces punto a punto independientes.

Por lo tanto, la unicidad del espacio de etiquetas puede garantizarse mediante:

- **Espacio de etiquetas con unicidad por interfaz:** cuando estas dos condiciones se dan, un LSR podrá emplear etiquetas que posean alcance por interfaz, es decir, que sean sólo únicas por interfaz.

[13]La notación utilizada se corresponde con Rd (Router Downstream) y Ru (Router Upstream), habitual también para referirse a los nodos siguiente y previo respectivamente.

- **Espacio de etiquetas con unicidad por LSR:** cuando no se dan estas dos condiciones, las etiquetas deberán ser únicas sobre el LSR que las ha asignado.

Distribución

Las etiquetas son locales para cada par de nodos adyacentes. Las etiquetas no tienen un significado global a través de la red. Para que los nodos adyacentes se pongan de acuerdo, en la etiqueta que se utilizará para cada paquete, necesitan alguna forma de comunicación entre ellos, de lo contrario, los nodos no sabrán por donde reenviar los distintos paquetes. Por lo tanto, se necesita un protocolo de distribución de etiquetas.

Existen dos protocolos para la distribución de etiquetas:

- **Protocolo de Distribución de Etiquetas (Label Distribution Protocol, LDP):** definido en la RFC 3036, es un protocolo de encaminamiento, que permite el establecimiento de vecindades, es decir, el descubrimiento de vecinos y el establecimiento de sesión. Permite así mismo el envío de notificaciones y por supuesto, la distribución de etiquetas.

  Las vecindades se establecen porque el protocolo permite el descubrimiento de vecinos y el establecimiento de sesiones entre ellos. La relación de vecindad es jerárquica, así se realizan los descubrimientos mediante el intercambio de paquetes UDP, envío de *HOLA UDP/IP-multicast* para vecinos directamente conectados y envío de *HOLA UDP/IPunicast* para vecinos no directamente conectados. Para mantener las sesiones entre vecinos, que permiten el envío de recuerdos periódicos y el intercambio de pares etiquetas/FEC, el vecino con la IP activa más alta inicia una sesión TCP. Estos procesos se recogen en el ejemplo de la figura 4.40.

  Dos LSRs que emplean el protocolo LDP para intercambiar información de asociación etiqueta / FEC son llamados pares LDP con respecto a esa información , manteniéndose entre ellos una sesión LDP. Una sesión LDP permite a cada par aprender la información de las etiquetas del otro. El protocolo es bidireccional.

  Existen cuatro categorías de mensajes :

  - *Mensajes de descubrimiento:* empleados para anunciar y mantener la presencia de un LSR en la red.

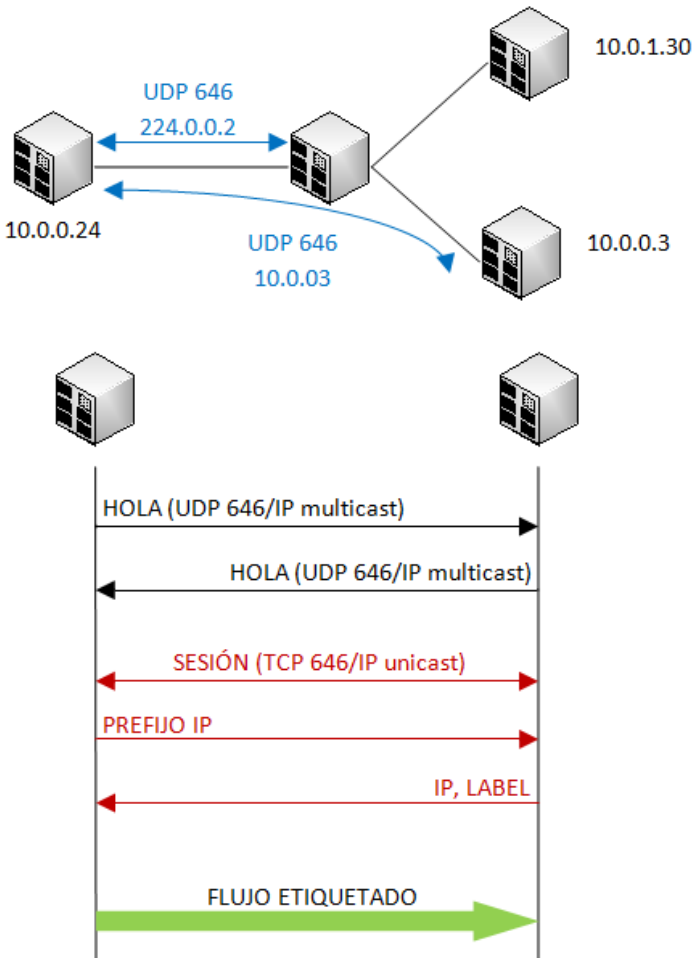

Figura 4.40: Establecimiento de vecindades en MPLS

- *Mensajes de sesión:* empleados para establece, mantener y finalizar las sesiones entre los pares.
- *Mensajes de anuncio:* empleados para crear, cambiar y borrar asociaciones de etiquetas con FECs.
- *Mensajes de notificación:* empleados para da información de aviso o de error.

Los mensajes de descubrimiento anuncian la presencia de un LSR en la red, estos se realizan enviando el mensaje HELLO periódicamente. Éste es transmitido como un paquete UDP por el puerto LDP en la dirección multicast del grupo todos los routers de esta subred. Cuando un LSR desea establecer una sesión con otro LSR, aprendido gracias al mensaje HELLO, empleará el procedimiento de inicialización LDP sobre TCP. Si se lleva a cabo de forma correcta el procedimiento de inicialización LDP, los dos LSRs son ya pares LDP, y pueden intercambiar mensajes de anuncio.

Cuándo pedir cierta etiqueta, o anunciarla a un par, será una decisión local a cada LSR. En general, el LSR pide una etiqueta a su vecino cuando la necesita, y la anuncia cuando desea que el vecino la comience a utilizar.

El funcionamiento correcto del protocolo LDP requiere una recepción fiable y ordenada de mensajes. Para ello, se emplea el protocolo TCP para mensajes de sesión, de anuncio y de notificación. Es decir, para todo el proceso, excepto para los mensajes de descubrimiento, que viajan sobre UDP.

- **Protocolos tradicionales:** consiste en utilizar protocolos conocidos como OSPF, BGP, RSUP, modificándolos para que puedan transportar nuevos elementos de información.

Utilizando cualquiera de estos dos protocolos, encontramos dos filosofías a la hora de realizar la distribución de etiquetas:

- **Distribución independiente:** un LSR decide que reconoce una FEC y le asigna una etiqueta. Una vez asignada, la distribuye a los LSR vecinos, tal y como se hace en el encaminamiento IP. No existe comunicación de etiquetas más allá de los nodos vecinos.
- **Distribución ordenada:** la asignación la hace sólo el último nodo de una FEC mientras que la distribución se hace por cualquier nodo que ya tenga una etiqueta para esa FEC (distribución hacia atrás). Esta forma de proceder equivale al establecimiento de una conexión.

De esta forma podemos estar seguros que se ha establecido un sendero de etiquetas entre origen y destino.

En el ejemplo de distribución de etiquetas recogido en la figura 4.41 vemos como 8 nodos LSR intercambian información de encaminamiento y actualizan sus tablas de etiquetas.

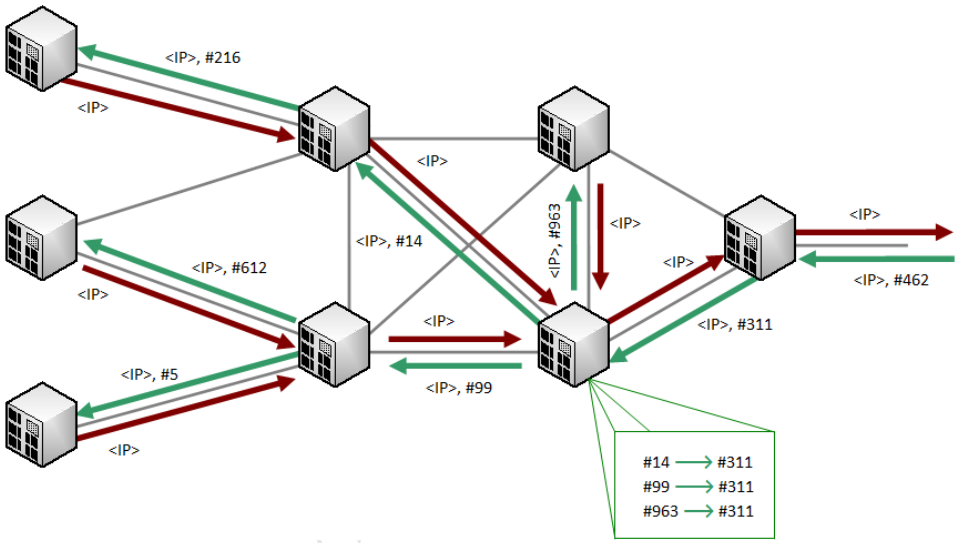

Figura 4.41: Ejemplo distribución etiquetas MPLS

Fusión de flujos

La fusión de flujos o agregación es el procedimiento por el que se asigna una etiqueta a un conjunto de FECs de forma que se constituye una nueva FEC. La principal ventaja de la agregación es la reducción en el número de etiquetas necesarias y del número de mensajes de control necesarios para la distribución de estas etiquetas.

La granularidad se clasifica en grados:

- **Granularidad Gruesa:** la fusión viene determinada por el LSR de salida, así todas las rutas hacia ese LSR llevan la misma etiqueta.
- **Granularidad Intermedia:** basándose en el prefijo IP, asignación de etiqueta basada en topología, de forma que para cada entrada de la tabla de encaminamiento hay una etiqueta.
- **Granularidad Fina:** en función de la aplicación, la fusión se realiza atendiendo a IPorigen, IPdestino, puerto origen y puerto destino. las

etiquetas se asignan por cada proceso de aplicación, de forma que los paquetes de dos aplicaciones pueden seguir rutas distintas en la red, algo que no se podía hacer con IP convencional.

MPLS permite realizar la agregación/segregación de forma automática. Según la distribución de etiquetas hay varias formas de agregación/segregación:

- **Distribución Ordenada:** se propaga la granularidad hacia atrás.
- **Distribución Independiente:** en la agregación el nodo previo usa más etiquetas para las mismas FECs. Se permite propagar el fundido hacia atrás. Para la segregación, el nodo previo usa menos etiquetas para las mismas FECs. Entonces el nodo previo puede adoptar el ramificado o bien mantener la granularidad.

Para conseguir la escalabilidad que requiere MPLS se permite que las etiquetas sean apilables (LIFO). Aplicar una etiqueta es equivalente a agregar un flujo, lo que de manera implícita nos permite definir *jerarquías* en la red. De esta forma, permitimos que un flujo esté contenido dentro de otro. En la decisión de encaminamiento en cada salto sólo se considera la etiqueta más reciente.

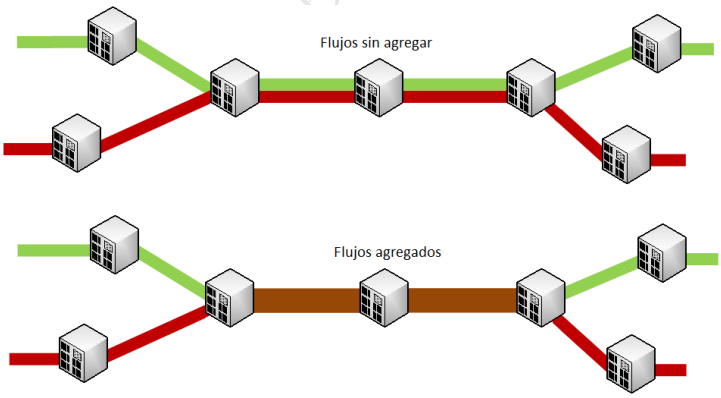

Figura 4.42: Jerarquías MPLS

En la figura 4.42 se muestra en la parte superior una representación de varios flujo sin agregar mientras que en la parte inferior se mostraría el comportamiento agregando dichos flujos.

Así pues, la pila de etiquetas define una jerarquía MPLS que puede coincidir o no con la jerarquía de encaminamiento.

Un nuevo nivel de apilado permite diferenciar flujos pertenecientes a un flujo agregado y simplificar la operación al segregar, pero también hace jerárquica la relación de vecindad, es decir, que no es imprescindible la adyacencia y se propaga la pila de etiquetas.

Operaciones

Se define una tabla de operaciones (Next Hop Label Forwarding Entry, NHLFE) donde se guardan las etiquetas. Para cada etiqueta entrante (o FEC si la pila de etiquetas está vacía) se almacena en la tabla los siguientes elementos:

- Siguiente salto, o siguientes.
- Encapsulación o encapsulaciones de nivel 2 a utilizar.
- Codificación de la pila de etiquetas (dónde va la etiqueta dentro de la trama).
- Operación en la pila entrante. Se realiza una única operación en cada salto la sobre la pila de etiquetas del paquete entrante.

Se definen cuatro posibles operaciones a realizar sobre la pila de etiquetas:

- **SWAP:** intercambia el valor dela etiqueta más externa.
- **POP:** quita una etiqueta, es decir, segrega un flujo.
- **PUSH:** añade una etiqueta sobre la anterior, es decir, agrega un flujo.
- **SWAP+PUSH:** se cambia el valor y posteriormente se añade uno nuevo.

Gracias al uso de las operaciones, definimos un **sendero de etiquetas** como una secuencia de LSRs para una FEC, que empieza en el LSR frontera de entrada que hace un PUSH (aplica etiqueta al paquete IP convencional), continúa con los LSRs que hacen SWAP, el penúltimo puede hacer POP y que acaba en el LSR frontera de salida, que encamina basándose en una etiqueta de otro nivel inferior o por un procedimiento no MPLS.

Los senderos de una FEC forman un árbol con raíz en el LSR frontera de salida de la red MPLS.

Existen algunas etiquetas reservadas:

- **Etiqueta 0:** IPv4 Explicit Null Label, fuerza POP y uso de dirección IP. Debe ser única.

- **Etiqueta 1:** Router Alert Label, fuerza procesado local y propaga la etiqueta. Nunca debe ser la última.
- **Etiqueta 2:** IPv6 Explicit Null, fuerza POP y uso de dirección IPv6. Debe ser única.
- **Etiqueta 3:** Implicit Null Label, no viaja nunca en el paquete, forzando el POP en el nodo previo.
- **Etiquetas 4-16:** Reservados.

La etiqueta nula implícita (etiqueta 3) se utiliza para soporte del POP en el penúltimo LSR, como vemos en el ejemplo de la figura 4.43.

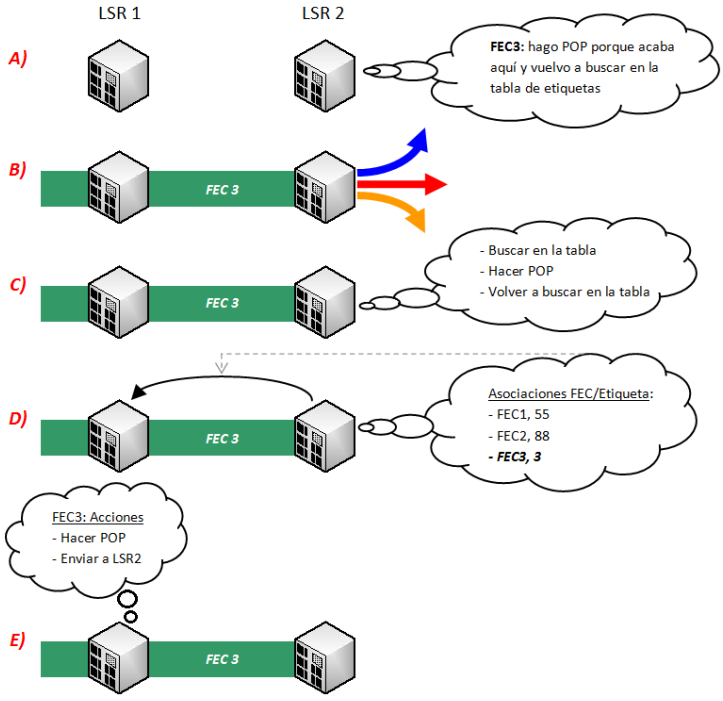

Figura 4.43: Uso de Implicit Null Label

Al usarla, forzamos el POP en el nodo previo, imaginemos que al LSR llegan tres flujos agregados que llegan tal cual al posterior. Con este mecanismo se puede conseguir que el encaminador anterior mande ese tráfico ya agregado.

Conservación de Etiquetas

La topología de red está sujeta a cambios que pueden provocar que cambien las rutas cuando cae algún enlace. Estos cambios en la topología deben

reflejarse en el espacio de etiquetas. En MPLS se implementan dos estrategias para asegurar la consistencia y protegerse frente a estos cambios en las topologías de red:

- **Estrategia Liberal:** el LSR que asigna la etiqueta la comunica a todos los vecinos, aunque no sean el salto previo para esa FEC. Los vecinos conservan esa información (FEC,Etiqueta), de forma que si se requiere que ese flujo vaya por ese nodo vecino, por ejemplo debido a un cambio de topología de red, no hay necesidad de iniciar el proceso de asignación de etiqueta.
- **Estrategia Conservadora:** sólo se mantienen las etiquetas recibidas correspondientes a las FECs para las que el emisor es el siguiente salto. Ésto supone que si cambia el encaminamiento habría que hacer una nueva asignación de etiquetas.

La estrategia liberal gasta más etiquetas, pero es más rápida a la hora de adaptarse a cambios en la topología de red.

4.10.3. Aspectos avanzados MPLS

Una vez estudiados los mecanismos más básicos relacionados con la gestión de etiquetas para el funcionamiento de las redes MPLS, pasaremos a describir de manera resumida otros aspectos algo más avanzados que se soportan en las redes MPLS tales como: *prevención y detección de bucles, soporte para encaminamiento explícito, soporte multiprotocolo, soporte multicast y la protección local y restauración.*

Prevención y detección de Bucles MPLS

El campo tiempo de vida (**Time To Live, TTL**) de las etiquetas MPLS tiene exactamente el mismo significado que el campo TTL en IP. Se utiliza para aliviar el efecto de los bucles debidos a cambios de topología en la red, en los que los nodos tienen temporalmente una visión distinta de la red. El uso específico de estos campos depende del protocolo.

En IP los saltos MPLS deben contar como saltos IP. Para ello en el ingreso del paquete IP en el segmento MPLS se le asigna al campo TTL de la etiqueta MPLS un valor menor o igual que el valor del campo TTL del paquete IP, decrementándose en cada salto en nodos intermedios.

Al salir del segmento MPLS al campo TTL IP se le asigna un,valor menor o igual que el valor del campo TTL de MPLS.

Dado que utilizamos dos valores de campos TTL, en principio es posible detectar bucles en los que intervenga una segmento de red MPLS y otra

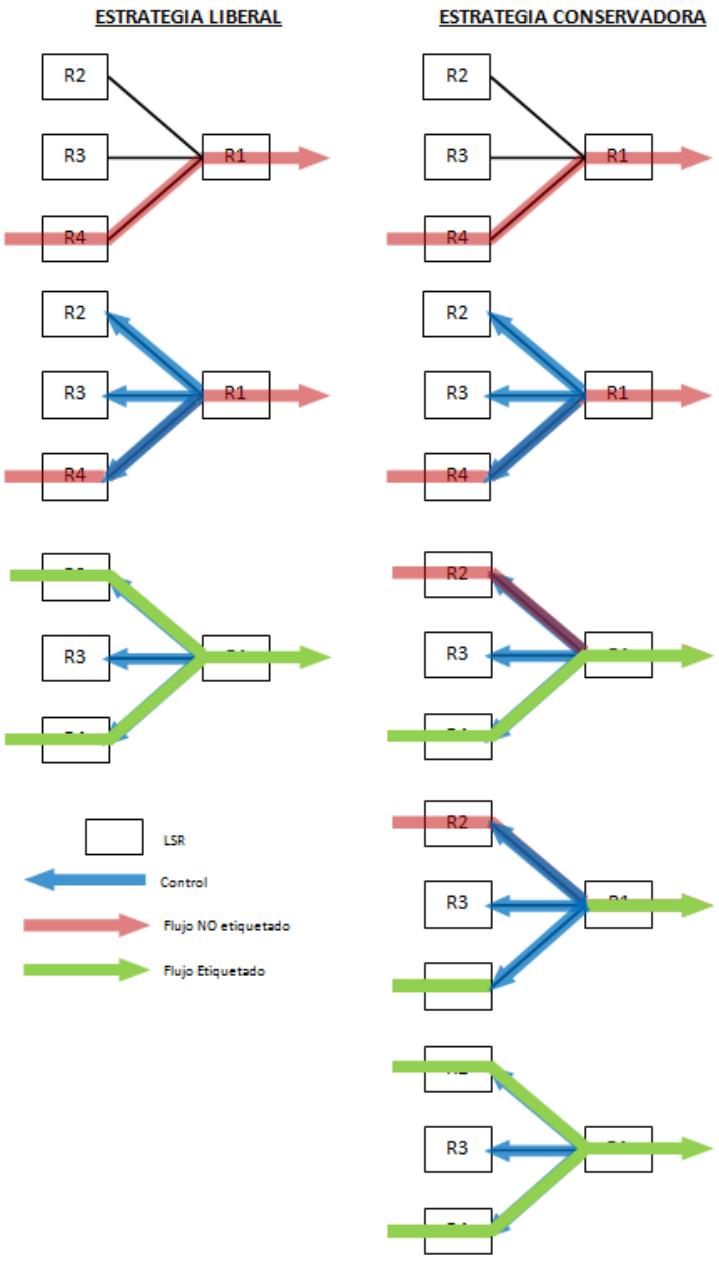

Figura 4.44: Ejemplo de conservación de etiquetas MPLS (I)

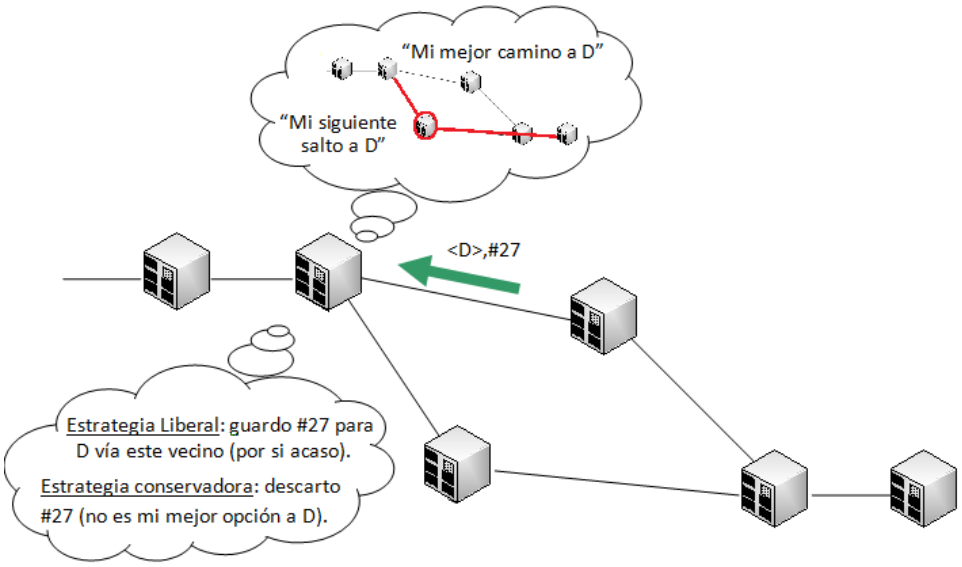

Figura 4.45: Ejemplo de conservación de etiquetas MPLS(II)

segmento IP.

Los bucles pueden aparecer tanto en nivel 3 (para nosotros IP exclusivamente) como en MPLS. Para mitigar el efecto de los mismos, tenemos como hemos dicho sus respectivos campos TTL, tanto en nivel 3 (IP) como en MPLS. Sin embargo, podemos tener problemas en segmentos no TTL, tales como segmentos de red MPLS que no utilicen el etiquetado convencional, o directamente no sorporten el campo TTL o bien si se están utilizando las cabeceras de la capa ATM AAL5 para codificar las etiquetas (campos VPI/VCI), con los paquetes etiquetados siendo reenviados por switches ATM por lo que la capa de enlace de datos no tiene campo TTL.

En la lucha contra los efectos de los bucles se definen dos tareas, la detección y la prevención.

- **Prevención de bucles:** es opcional y se realiza mediante la distribución ordenada.

- **Detección de bucles:** es obligatoria y se puede realizar mediante la distribución independiente o mediante distribución ordenada. La idea general es que cada LSR mantenga su lista de LSRs para los LSPs propagándose a la vez la lista de LSD-ID (label Switching Database-ID).

Soporte para Encaminamiento Explícito

El camino más corto entre dos nodos según la métrica normal IGP es el que tiene menor número de saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización de un camino alternativo, aunque tenga un número mayor de saltos.

MPLS es una herramienta efectiva para dar soporte al encaminamiento explícito en grandes backbones, ya que en el encaminamiento explícito es el origen el que decide la ruta que va a seguir el paquete, y para ello se puede establecer una FEC específica que predefine una senda conmutada (LSP).

Hay varios niveles para lograr el encaminamiento explícito:

- **Salto a salto:** el LSR únicamente determina el siguiente salto.
- **Estricto:** el LSR de entrada determina el LSP.
- **Laxo:** el LSR de entrada determina algunos LSRs.

Todas estas funciones se soportan en MPLS gracias al etiquetado. La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM[14] por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

Soporte Multiprotocolo

Es la determinación del protocolo, tras la última etiqueta. La determinación del protocolo de capa superior se realiza de manera implícita, ya sea utilizando etiquetas reservadas para cada protocolo o con etiquetas reservadas a familias de protocolos, teniendo en cuenta que dentro de cada familia pueda diferenciarse el protocolo específico en la cabecera del mismo, por ejemplo la encapsulación LLC-SNAP.

La restricción se aplica a todas las etiquetas de la pila.

Soporte Multicast

Para dar soporte a tráfico multicast en MPLS se permite que el LSP puede ser multipunto, simplemente indicando varios ineterfaces de salida para una etiqueta correspondiente a una FEC.

Si el LSR pertenece a un árbol multicast:

[14] recordemos que ATM si soportar explícitamente QoS

- Asocia etiqueta a ese árbol.
- Propaga la etiqueta árbol arriba (LDP, PIM, ...).
- Indica en la tabla los interfaces de salida.

Para poder soportar multicast se exige coordinación en LAN, es decir, sigue siendo necesario un protocolo de gestión de grupos multicast, que posteriormente será traducido en las distintas FEC.

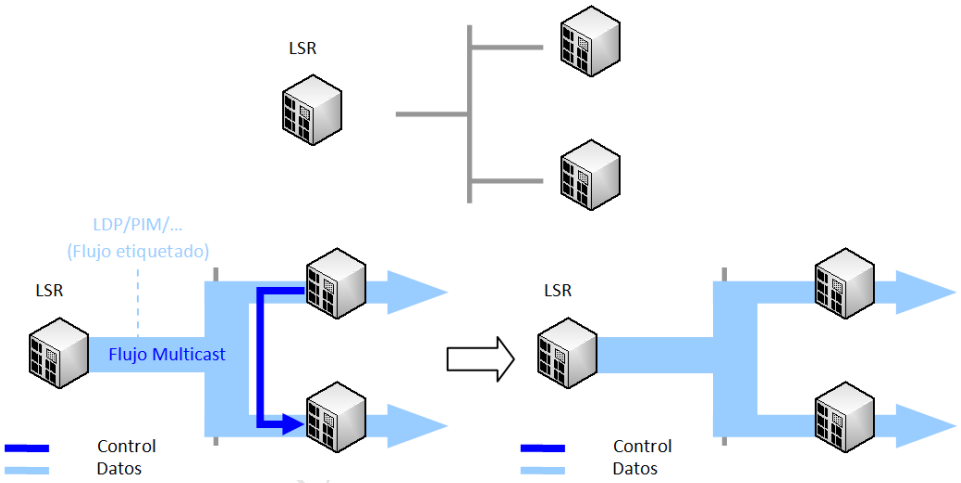

Figura 4.46: Soporte Multicast en MPLS

Protección Local y Restauración

La denominada **protección local** o (*Fast Reroute*) son una serie de mecanismos incorporados en MPLS cuyo objetivo principal es lograr una recuperación lo más rápida posible (del orden de decenas de mili segundos) ante fallos, tratando de compensar y evitar las recuperaciones de varios segundos de duración que se producen en entornos de IP convencionales.

Si falla un enlace o nodo, el LSP protegido se pasa por un LSP de reserva, de modo que logramos puentear el fallo. Un LSP protegido puede tener asignados varios LSPs de reserva sólo para él (*Detours LSPs*) o bien existe otra filosofía en la que varios LSPs protegidos comparten un mismo LSP de reserva (*Bypass LSP*).

Cuando se produce el fallo, se avisa al LSR origen con el mensaje PATHERR (path error) que puede restaurar el LSP extremo a extremo.

Para soportar la protección local se utilizan unas extensiones adicionales a la señalización RSVP: campos FAST_REROUTE y DETOUR.

En el ejemplo recogido en la figura 4.47 vemos como se pueden establecer más de un desvío por cada LSP protegido, en este caso, el LSP definido por $A \rightarrow C \rightarrow E \rightarrow F$ está protegido por:

- $A \rightarrow B \rightarrow E$.
- $C \rightarrow B \rightarrow D \rightarrow F$.
- $E \rightarrow D \rightarrow F$.

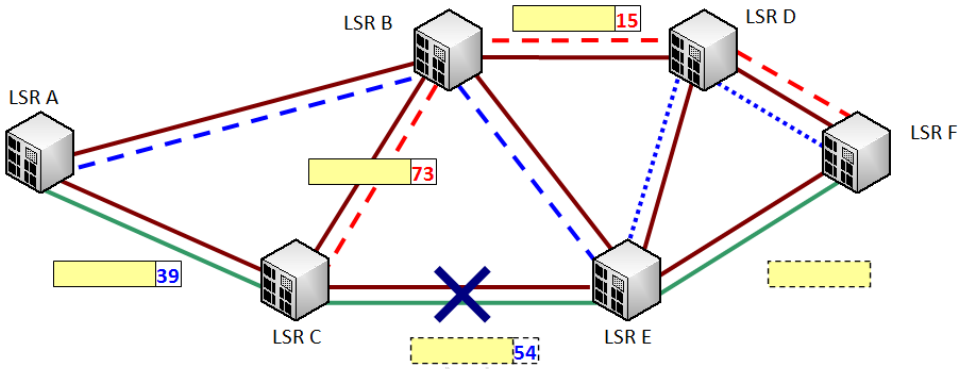

Figura 4.47: Ejemplo Fast Reroute MPLS

C sustituye la etiqueta del LSP protegido por la etiqueta asignada al desvío LSP que parte de C y avisa a A de la situación.

La **restauración extremo a extremo** se produce cuando ante un fallo en un LSP, el LSR origen puede asignar el troncal de tráfico a otro LSP. Esta restauración puede estar preestablecida o bien establecerse sobre la marcha, en función del atributo Resistencia del Troncal. En todo caso, este mecanismo de protección es más lento que la protección local.

Cerramos el tema estudiando un ejemplo donde se aplica el sistema de restauración extremo a extremo, para proteger un LSP, recogido en la figura 4.48.

La secuencia de eventos en el ejemplo de la figura es la siguiente:

- C detecta el fallo por plazo de *HOLA* o bien por aviso del nivel inferior.
- C utiliza el LSP de reserva preestablecido y avisa al origen A.
- El encaminamiento informa del nuevo estado.

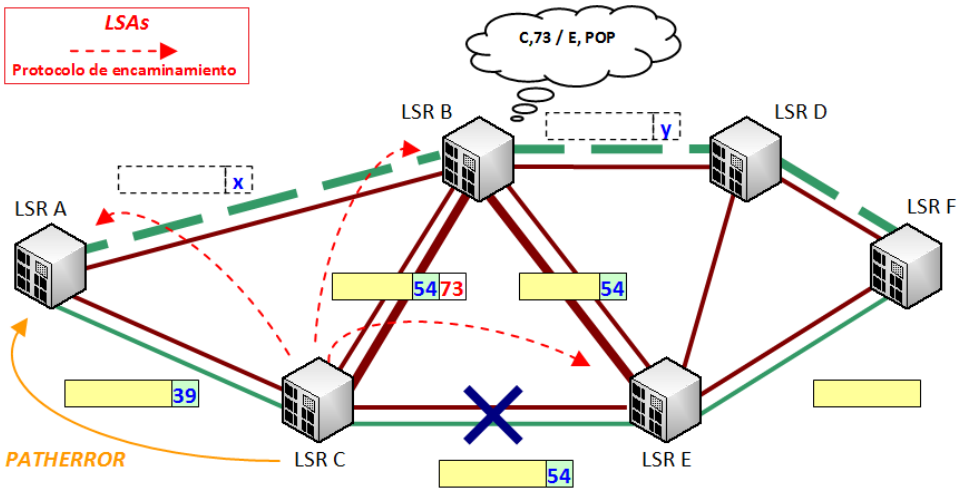

Figura 4.48: Ejemplo de protección local y restauración MPLS

- A calcula un nuevo LSP entre entre A y F, concretamente $A \rightarrow B \rightarrow D \rightarrow F$.

Capítulo 5

Redes de Nueva Generación [1]

5.1. Introducción

Las operadoras actuales se encuentran luchando en un mercado que evoluciona continuamente en su formato. De las evoluciones sufridas en estas últimas décadas hasta encontrarnos en la situación actual, podríamos extraer las siguientes conclusiones:

- El tráfico tradicional asociado a circuitos proporciona unos ingresos cada vez menores, debido a que su crecimiento está estancado y a que la competencia es creciente, ofreciéndose cada vez precios más bajos, lo que conlleva a menores márgenes de beneficios.
- Por otro lado, las demandas sobre las operadores crecen y lo hacen en varios sentidos. Crecen las demandas de los usuarios, que reclaman cada vez nuevos servicios y a menores precios, y crecen también las demandas de los accionistas, que únicamente pretenden aumentar sus beneficios.
- Para poder satisfacer todas estas demandas la tecnología clásica ha llegado a su límite, donde la evolución de los conmutadores de circuitos tradicionales es totalmente inviable, pues la velocidad y las necesidades en QoS actuales no justifican su precio ni su arquitectura, sin tener en cuenta que el soporte de nuevos servicios, principalmente los asociados a contenido multimedia, son de difícil implementación.

Por lo tanto, se hace necesario un nuevos paradigma de explotación de redes, concepto que se ha englobado en el término Redes de Nueva Generación (New Generation Networks, NGN), definido por la UIT-T como: *a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in*

[1] Este capítulo está basado en los trabajos [6], [5] y [**?**].

which service-related functions are independent from underlying transport-related technologies. It offers unfettered access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users[2]*.*

Es decir, a grosso modo las características generales de una red de nueva generación son:

- *Conmutación de Paquetes:* IP, ATM, MPLS.
- *Separación de funciones:* transporte, llamada, servicio: los servicios han de estar separados del transporte, esto es, la provisión de los servicios es independiente de la red por la que se transmiten, lo que además permite que su evolución no esté ligada a la de la infraestructura de red.
- *Interfaces abiertos entre transporte, control y aplicaciones:* la arquitectura de red y su organización funcional deben ser tales que presenten interfaces abiertas en las que mediante pasarelas se permita la operación de nuevos servicios.
- Debe existir capacidad de *interoperabilidad/interconexión* con las redes tradicionales, muy específicamente con la red telefónica de pares de cobre.
- Se debe permitir la *movilidad del usuario.*

Por tanto, la NGN es una arquitectura de red para las operadoras, es decir, los clientes no tienen por qué notarla sino a través de nuevos servicios. Las distintas operadoras en todo el mundo han utilizado dos estrategias en su evolución hacia las NGNs:

- *Evolución gradual:* exprimiendo equipos existentes y por tanto conllevando un menor coste para la operadora.
- *Evolución inmediata:* a un coste mayor pero sin riesgo de falta de soporte.

Telecom Italia, the former PTT[3] *in Italy, announced that a significant portion of its domestic long distance and international voice traffic is now using IP for transport. (03/october/2006).*

Todo este proceso evolutivo en las redes de telecomunicación ha necesitado de un marco de referencia normalizado para llevarse a cabo. Algunos de los agentes involucrados en el establecimiento de dicho marco han sido:

[2] `http://www.itu.int/UIT-T/ngn/files/NGN_FG-book_I.pdf`
[3] PTT: Provider of Telecommunications Training.

- *UIT-T:* definió el marco de referencia, es decir, estableció los objetivos a largo plazo.
- *3GPP:* ha desarrollado el IMS (IP Media System) y junto con el IETF trabajaron para garantizar que los nuevos protocolos encajan con los requisitos del 3GPP (servicio móvil).
- *Open Mobile Alliance, OMA:* esta definiendo servicios basándose en el IMS.
- *ETSI TISPAN:* están definiendo las NGN basándose en el IMS. Trabajando con 3GPP para definir interfaces fijos para el IMS y realimentando a la UIT-T y definidiendo una NGN de primera generación implementable.

En este nuevo ámbito normalizado, ahora sí se pueden recoger de manera más específica las **características fundamentales de una NGN**, recogidas en la recomendación Y-2001[4] de la UIT-T:

- **Transporte basado en conmutación de paquetes multiservicio:** utilizando multiplexación estadística se busca conseguir un aprovechamiento óptimo de la red. Se puede utilizar tecnologías IP o ATM, aunque debido a su ubicuidad IP suele ser el preferido.
- **Separación de las funciones de control:** en capacidad de la portadora, control de la sesión o la llamada, y servicio o aplicación.
- **Desacoplo entre la provisión del servicio y la red de transporte:** la provisión de interfaces normalizados busca conseguir un desarrollo y despliegue rápido de servicios. Además un servicio no se vera limitado por el tipo de red que lo proporciona pudiendo evolucionar de manera independiente tanto los servicios proporcionados como las tecnologías de transporte, como por ejemplo en los servicios de mensajería, disponibles tanto en red fija, red móvil, PDA con WLAN, smartphone, etc.

Es importante destacar que el beneficiario directo es el operador, ya que con las NGN las operadoras buscan *conseguir menores costes de operación y por tanto mayores márgenes de beneficio.*

Por último, la UIT-T define también una serie de **requisitos a cumplir** por las NGN. Los principales requisitos son:

- **Interfuncionamiento con redes heredadas:** GSM, RTC, RDSI, Frame Relay, ... Este requisito justifica también el uso de interfaces

[4]De recomendada lectura como introducción a este capítulo.

abiertas. Así, mediante el uso de pasarelas (Gateways, GW) para el interfuncionamiento entre operadores de redes NGN y otras redes. Un ejemplo claro que estudiaremos en este tema es el interfuncionamiento en red telefónica, donde la señalización usa SS7 y la voz es codificada en PCM mientras que en IP la voz se transporta codificada (G.723,G.729,...) y la señalización es SIP o bien H.323, por lo que serán necesarias pasarelas tanto para la voz digitalizada (medios) como para la señalización.

- **Soporte de movilidad generalizada** que se aplicará en diferentes ámbitos:
  - *Gestión de identidad:* de usuario, de dispositivo, localización, presencia, autentificación, registro, ...
  - *Gestión dinámica de sesión:* control de sesión/llamada, ancho de banda y QoS por sesión, tarificación, etc.
  - *Gestión de movilidad:* heredada de GSM/UMTS incluye aspectos como suscripción a servicios, invocación, itinerancia, movilidad de usuario, ...

  Es decir, el concepto de movilidad generalizada se define como la capacidad del usuario u otras entidades móviles de comunicar y acceder a servicios independientemente de los cambios de ubicación o del entorno técnico. El grado de disponibilidad de servicio puede depender de varios factores, incluidas las capacidades de la red de acceso, los acuerdos de nivel de servicio (si los hubiese) entre la red propia del usuario y la red visitada, etc. El término movilidad incluye la capacidad de telecomunicación con o sin continuidad de servicio.

- **Numeración, nombrado y direccionamiento:** dado que una NGN está compuesta de multitud de redes heterogéneas, accesos heterogéneos y terminales heterogéneos, los usuarios individuales deben ser identificados por nombres o números, como por ejemplo E-164, URL, nombres únicos, identificadores SIP, etc., ofreciendo siempre la NGN la portabilidad de identificador de usuario. Se debe utilizar un sistema fiable para la resolución de nombres/números que sea capaz de traducir un nombre/número dado en una dirección IP. Dicho sistema debe ser fiable, íntegro, seguro y respecto a la independencia de organizaciones.

5.2. Fundamentos de Transmisión de Voz en Redes de Paquetes

La voz se genera cuando el aire es empujado desde los pulmones, pasando por las cuerdas vocales a lo largo del tracto vocal. Las vibraciones básicas se

producen en las cuerdas vocales, pero el sonido es alterado por la disposición del tracto vocal, es decir, por la posición de la lengua o la forma de la boca.

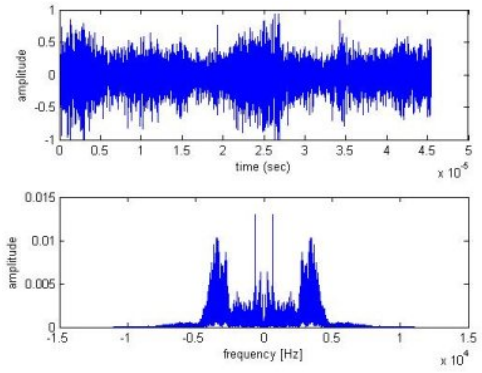

Figura 5.1: Muestra vocal y espectro de frecuencia

Sin entrar en mayor detalle, el tracto vocal se puede considerar un filtro de tecnologías de codificación. Es posible encontrar numerosos trabajos donde se modela el tracto vocal como un filtro.

En la figura 5.2 se recoge el modelo básico de funcionamiento de un transmisor de voz típico, donde vemos como el modelo se reduce a la realización de dos procesos, en primer lugar se produce una **codificación** de las muestras vocales, que posteriormente son **empaquetadas** de manera que puedan ser susceptibles de ser transmitidas en una red IP.

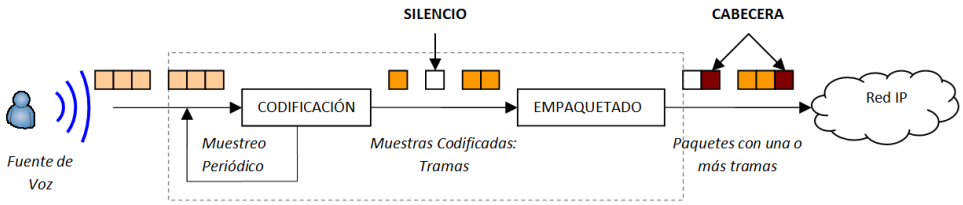

Figura 5.2: Transmisor típico VOIP

El estudio exhaustivo de los elementos que componente este sistema cae fuera del alcance del texto, pero sí es interesante estudiar unas ciertas características existentes en la voz humana que deben ser tenidas en cuenta a la hora de utilizar una red de conmutación de paquetes, es decir IP, para el soporte de comunicaciones vocales.

Para una correcta explotación se pretende lograr la máxima calidad con el menor consumo de recursos por parte de la red. Para ello, existe una cualidad importante que se puede aprovechar durante la codificación de la voz

humana y es la **intermitencia** de la misma.

Al ser la voz una actividad intermitente se logran mejores resultados utilizando técnicas de **Detección de Actividad Vocal (Voice Activity Detection, VAD)** junto con la inserción de tramas de descripción de silencios (SID). Así, la detección de actividad vocal permite la supresión de silencios tanto en las pausas naturales del habla, al respirar entre frases por ejemplo, o bien cuando habla el otro interlocutor de la conversación.

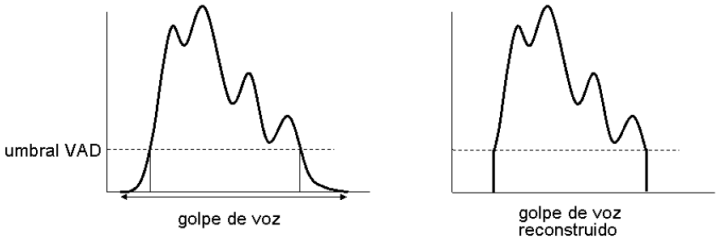

Figura 5.3: Detección de Actividad Vocal

Como se muestra en la figura 5.3, la VAD no es perfecta y presenta una serie de problemas que afectan a la calidad de la conversación, típicamente la existencia de recortes al inicio y fin de cada palabra o fonema además de poder provocar una respuesta lenta o mal ajuste.

Otro aspecto importante en una conversación digital, en la analógica no es necesaria, es la **generación de ruido de confort (Confort Noise Generation, CNG)**, pues el cerebro asocia la ausencia de ruido con un corte en la comunicación, por lo que la adición de un cierto nivel de ruido es más agradable para el interlocutor.

Para implementar dicho ruido existen distintas posibilidades, como transportar el ruido con la misma fidelidad que el hablante o generar un ruido blanco en el destino, ya sea con el nivel de potencia correspondiente al origen o bien con un nivel de potencia independiente.

El proceso de **codificación de voz** se realiza:

- *Ráfaga:* generación periódica de tramas activas, de aproximadamente 10 a 70 octetos de tamaño.

- *Silencios:* descripción grosera, es decir de nivel de potencia, del ruido de fondo, actualizada cuando convenga, en tramas cortas, de 1 o 2 octetos, para la generación de ruido de confort.

El retardo de codificación, que en algunos casos puede ser de decenas de milisegundos, se suma a otras componentes de retardo.

Recogemos en la tabla 5.1 los codecs más utilizados junto con su régimen binario final.

Nombre	**Siglas**	**Recomendación**	**Rb (Kb/s)**
Pulse Code Modulation	PCM	G.711	64/56/48
Adaptive Differential PCM	ADPCM	G.726	40/32/24/16
Linar Predictive Coding	LPC	G.723.1	6,4/5,3
		G.728 LD-CELP	16/12,8/9,6
		G.729 CS-ACELP	12/8/6,4
		iLBC	15,2/13,33

Tabla 5.1: Codecs Vocales

El proceso de **empaquetado** consiste en la adición de una cabecera de transporte adecuada. Para no sobrecargar la red es habitual que un mismo paquete IP sea compartido por hasta N_{fpp} tramas de codec. Por lo tanto, la cabecera es muy grande comparada con una trama de codec y encontramos límites en el sistema, motivados por el retardo (por el eco) y la temporización (por la marca de tiempo).

Por supuesto, el sistema carece de sentido sin el interlocutor complementario, por lo que es necesario incluir el esquema básico de funcionamiento del receptor típico en VOIP, recogido en la figura 5.4. El receptor garantiza la correcta reproducción de la muestra adecuada en el instante procedente.

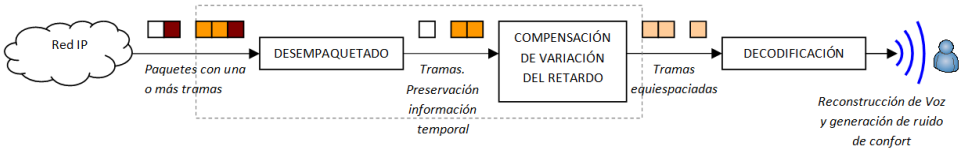

Figura 5.4: Receptor Típico VOIP

Para ello, el proceso es inverso al realizado por el transmisor, debiendo realizar el receptor tres procesos en cascada, empezando por desempaquetado de los paquetes IP, una vez tenga las tramas deberá realizar una compensación de la variación del retardo y finalmente una decodificación de las tramas para lograr la reconstrucción de la voz y la generación del ruido de confort.

Es bien conocido, que en una red IP disponemos de dos protocolos básí-

cos de transporte de datos: *User Datagram Protocol (UDP)* y *Transmission Control Protocol (TCP)*, y que en general y sin entrar en detalle[5], se utiliza TCP cuando se necesita una conexión fiable y UDP cuando se prefiere simplicidad por encima de la fiabilidad.

Debido a la naturaleza sensible al retraso del tráfico vocal, se utiliza UDP/IP para el transporte de voz, usando un número de puerto que identifica las aplicaciones en el sistema final, ya que las posibles retransmisiones que existen en TCP no son en absoluto deseables en un sistema VOIP.

Para sistemas en tiempo real sensibles al retraso, como es VOIP, el IETF adoptó el protocolo **Real-Time Transport Protocol (RTP)**, definido en la RFC 3550 y caracterizado por ser un protocolo no fiable y que no garantiza secuencia, y que normalmente usa UDP. Sus principales funciones son la detección de pérdidas, identificación de carga útil y la recuperación de temporización.

Por lo tanto, tal y como se recoge en la figura 5.5, la cabecera del sistema de transporte de voz sobre VOIP está formado por RTP/UDP/IP en el plano de usuario.

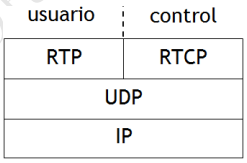

Figura 5.5: Torre de Protocolos Básica VOIP

Además, en el plano de control VOIP utiliza el protocolo **RTP Control Protocol (RTCP)**, definido también en la RFC 3550, que proporciona información de control asociada al flujo de datos de voz que viaja en el flujo RTP. Es decir, RTCP no transporta ningún dato de voz por sí mismo, sino que transporta información de control para lograr una realimentación de la calidad de la conversación, esto es QoS, por ejemplo limitando el flujo o usando un codec de compresión más baja.

A continuación estudiaremos más en detalle estos protocolos.

5.2.1. RTP: Real-Time Transport Protocol

RTP proporciona un servicio de entrega de datos extremo a extremo para datos con características de tiempo real, como audio y vídeo interactivo.

[5]Ver Anexo E para ampliar

Estos servicios incluyen la identificación del tipo de carga, secuenciación, timestamping y monitoreo de la entrega, aunque no garantiza la entrega en secuencia.

RTP suele implementarse sobre UDP para hacer uso de sus servicios de multiplexación y suma de comprobación, aunque RTP se puede usar con otros protocolos adecuados subyacentes de la capa de red. RTP soporta transferencia de datos a múltiples destinos a través de distribución multicast.

Antes de continuar veremos una serie de conceptos que son importantes en RTP:

- **Sesión:** se define una sesión como una asociación lógica entre dos interlocutores RTP. Un interlocutor RTP está definido por la tupla (IP, PuertoRTP, PuertoRTCP).
- **Sistema Final:** fuente o sumidero del flujo. En una conversación de voz, los sistemas finales son simultáneamente fuentes y sumideros de flujos.
- **Mezclador/Traductor:** equipo intermedio como por ejemplo un puente de conferencia, traductor de codec, etc.
- **Fuente de Sincronización (SSRC):** fuente de un flujo RTP. Todos los paquetes con la misma SSRC llevan el mismo origen de secuencia y tiempos. No se ve afectado por los traductores.
- **Fuente Contribuyente (CSRC):** identifica las fuentes que contribuyen a un flujo RTP a la salida del mezclador.

Veamos a continuación el formato de la cabecera RTP, recogido en la figura 5.6.

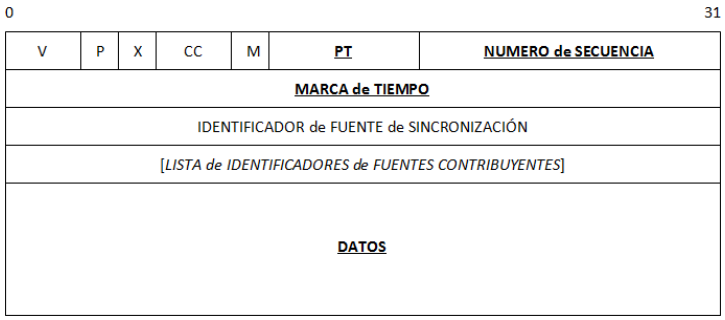

Figura 5.6: Formato Cabecera RTP

Donde los campos de la cabecera son:

- **Número de versión de RTP (V - versión number):** 2 bits. La versión definida por la especificación actual es 2.
- **Relleno (P - Padding):** 1 bit. Si el bit del relleno está activado, hay uno o más octetos al final del paquete que no es parte de la carga útil. El último octetos del paquete indica el número de octetos de relleno. El relleno es usado por algunos algoritmos de cifrado.
- **Bit de extensión (X - Extensión):** 1 bit. Si el bit de extensión está activado, entonces el encabezado fijo es seguido por una extensión del encabezado. Este mecanismo de la extensión posibilita implementaciones para añadir información al encabezado RTP.
- **Conteo CSRC (CC):** 4 bits. El número de identificadores CSRC que sigue el encabezado fijo. Si la cuenta CSRC es cero, entonces la fuente de sincronización es la fuente de la carga útil.
- **Bit Marcador (M - Marker):** 1 bit. Un bit de marcador definido por el perfil particular de media.
- **Tipo de Carga útil (PT - Payload Type):** 7 bits. Un índice en una tabla de perfiles de media que describe el formato de carga útil, recogido en la figura 5.7, donde se indica codec, bits por muestra, frecuencia de muestreo y tasa de tramas. También existe perfiles reservados para vídeo.
- **Número de Secuencia:** 16 bits. Un único número de paquete que identifica la posición de este en la secuencia de paquetes. El número del paquete es incrementado en uno para cada paquete enviado.
- **Marca de tiempo:** 32 bits. Refleja el instante de muestreo del primer octeto en la carga útil. Varios paquetes consecutivos pueden tener el mismo sellado si son lógicamente generados en el mismo tiempo - por ejemplo, si son todos parte del mismo frame de vídeo.
- **Identificador de Fuente de Sincronización (SSRC)**: 32 bits. Identifica la fuente de sincronización. Si la cuenta CSRC es cero, entonces la fuente de carga útil es la fuente de sincronización. Si la cuenta CSRC es distinta a cero, entonces el SSRC identifica el mixer(mezclador).
- **Lista identificadores de fuentes contribuyentes (CSRC):** 32 bits cada uno. Identifica las fuentes contribuyentes para la carga útil. El número de fuentes contribuyentes está indicado por el campo de la cuenta CSRC; Allí puede haber más de 16 fuentes contribuyentes. Si hay fuentes contribuyentes múltiples, entonces la carga útil son los datos mezclados de esas fuentes.

PT	encoding name	media type	clock rate (Hz)	channels
0	PCMU	A	8,000	1
1	reserved	A		
2	reserved	A		
3	GSM	A	8,000	1
4	G723	A	8,000	1
5	DVI4	A	8,000	1
6	DVI4	A	16,000	1
7	LPC	A	8,000	1
8	PCMA	A	8,000	1
9	G722	A	8,000	1
10	L16	A	44,100	2
11	L16	A	44,100	1
12	QCELP	A	8,000	1
13	CN	A	8,000	1
14	MPA	A	90,000	(see text)
15	G728	A	8,000	1
16	DVI4	A	11,025	1
17	DVI4	A	22,050	1
18	G729	A	8,000	1
19	reserved	A		
20	unassigned	A		
21	unassigned	A		
22	unassigned	A		
23	unassigned	A		
dyn	G726-40	A	8,000	1
dyn	G726-32	A	8,000	1
dyn	G726-24	A	8,000	1
dyn	G726-16	A	8,000	1
dyn	G729D	A	8,000	1
dyn	G729E	A	8,000	1
dyn	GSM-EFR	A	8,000	1
dyn	L8	A	var.	var.
dyn	RED	A		(see text)
dyn	VDVI	A	var.	1

Figura 5.7: Perfiles Pay Load Type RTP para Audio

- **EH:** Opcional. El tamaño de este dato debe ser CC x 32 en bits.
- **Datos:** El tamaño de los datos debe ser de X x((EHL+1) x 32) donde EHL es la longitud de la extensión del la cabecera en unidades de 32 bits.

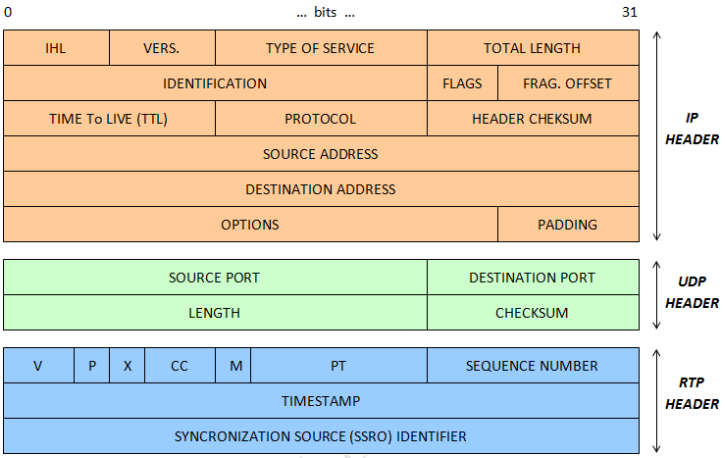

Figura 5.8: Formato Cabecera RTP/UDP/IP

5.2.2. RTCP: Real-Time Transport Control Protocol

Como ya hemos comentado, **RTP Control Protocol (RTCP)**, definido también en la RFC 3550, proporciona información de control asociada al flujo de datos de voz que viaja en el flujo RTP. Es decir, RTCP no transporta ningún dato de voz por sí mismo, sino que transporta información de control para lograr una realimentación de la calidad de la conversación.

RTCP realiza su tarea en tres áreas o bloques específicos:

- **Monitorización:** aplicación que recibe los paquetes RTCP generados por los interlocutores RTP de una sesión.
- **Realización de Informes:** proporciona una realimentación de la calidad enviada por receptores RTP. Para ello se contabilizan:
  - Número de paquetes perdidos.
  - Número de paquetes enviados.
  - Número de octetos enviados.
  - Fluctuación del retardo.

- **Identificador permanente de fuente RTP (CNAME):** es muy importante establecer la diferencia entre el identificador de fuente de sincronización de RTP, el SSRC y el CNAME del RTCP. Por ejemplo, un stream de audio y vídeo procedentes del mismo emisor utilizan diferentes SSRC, puesto que en el caso contrario se podrían dar colisiones de identificadores SSRC. Para solucionar este problema, RTCP utiliza el concepto de nombre canónico (CNAME) que se asigna al emisor. Este CNAME es asociado a varios valores SSRC. Así se garantiza que streams que no tienen el mismo SSRC se puedan sincronizar y ordenar correctamente.

5.2.3. Aspectos de Calidad en el Servicio Telefónico

La calidad del servicio es un concepto subjetivo relacionado con la satisfacción de las expectativas del usuario, y no se debe confundir en ningún caso con las prestaciones de la red, como retardo, pérdidas, ... Un ejemplo de valoración de calidad de servicio conocido por todos se recoge en la figura 5.9.

Figura 5.9: Skype Quality Feedback

Es fundamental disponer de un método de realimentación que permita conocer la calidad del servicio ofrecido, teniendo en cuenta demás que el usuario puede modificar sus expectativas respecto a la calidad de la conversación esperada en función del servicio que utiliza (telefonía celular, VOIP, RTC, ...).

La calidad del servicio está afectada por múltiples variables que dependen de múltiples factores, entre ellos:

- *La red:* pérdidas, retardos, variación del retardo, ... afectan a la percepción de la calidad de la llamada por parte del usuario.

- *El terminal y los codecs:* igualmente afectan ecos, retardos, cortes, distorsión, ruido, ...
- *Otros:* facilidad de uso, rapidez de establecimiento, fiabilidad, momento en el que aparecen las molestias, ...

La pregunta ahora es **¿cómo medimos la calidad?**

La UIT-T ha definido distintos estándares que estudiaremos a continuación para poder calibrar la calidad de una conversación. Estudiaremos los estándares *P.800, G.107, P.862 y el P.563.* El estándar P.800 es un modelo que nos da la calidad de la conversación a posteriori y es utilizado como referencia al dar un valor de calidad medible en un parámetro final, denominado *MOS o Mean Opinion Score.* El resto de estándares son lo que se denominan métodos predictivos, utilizados para estimar o planificar la calidad de una red en base a distintos parámetros para finalmente estimar o predecir un valor de calidad que es traducible al valor MOS.

UIT-T P.800: Medida de la Calidad

Para medir la calidad de una conversación la UIT-T optó por definir una medida natural, realizada por medio de encuestas, tratando de eliminar la variabilidad interpersonal.

Para ello, utilizó el **Mean Opinion Score (MOS)**, un test que ha sido utilizado durante décadas en redes de telefonía para obtener o estimar la calidad de la red, siempre desde el punto de vista del usuario. Históricamente, MOS era una medida subjetiva donde los usuarios debían mantener una conversación en una sala bajo unas condiciones acústicas controladas, para posteriormente valorar la calidad de la conversación mantenida.

Actualmente se somete a los usuarios participantes a pruebas de diverso tipo (test conversacional (MOS-CQ) o test de audio (MOS-LQ)) tratando de estimar calidades absolutas y relativas. Realizando el promedio de las opiniones de todos los usuarios, se obtiene el valor final de MOS. Las valoraciones que los usuarios pueden dar a la conversación varían entre 5 (máxima calidad) y 1 (mínima calidad), baremo completo recogido a continuación y que no por casualidad coincide con la numeración de estrellas representada en la figura 5.9.

- 5. Excelente.
- 4. Buena.
- 3. Aceptable.

- 2. Regular.
- 1. Mala.

Hemos visto como vamos a valorar la calidad final de una conversación, pero **¿qué factores influyen en la calidad de la señal?** Recogemos a continuación los efectos típicos sufridos en una conversación telefónica que afectan y merman la percepción de la calidad por parte del usuario:

- *Bajo volumen.*
- *Variación del ruido:* en ausencia de CNG la falta de ruido se asimila al corte y en presencia de CNG la diferencia de nivel de ruido es desagradable al usuario.
- *Eco:* se puede producir por fenómenos eléctricos (en las bobinas híbridas si existen segmentos analógicos a dos hilos) o por fenómenos acústicos, producidos por el terminal.
- *Distorsión de la voz:* se puede producir por una mala codificación o por pérdidas elevadas de muestras.
- *Recortes:* por respuesta lenta o mal ajuste del VAD.
- *Alteración del ritmo del discurso:* por retardo elevado o bien por la existencia de un retardo diferente en ambos sentidos.

El **retardo** afecta tanto a la *interactividad* de la conversación, la UIT-T define un límite de interactividad de entre 250 y 300 ms para el retardo de ida y vuelta en la recomendación G.114, como al *eco*, de modo que retardos superiores a 25 ms requieren control de eco.

En una red VOIP encontramos diferentes contribuciones al retardo, recogidas en la figura 5.10.

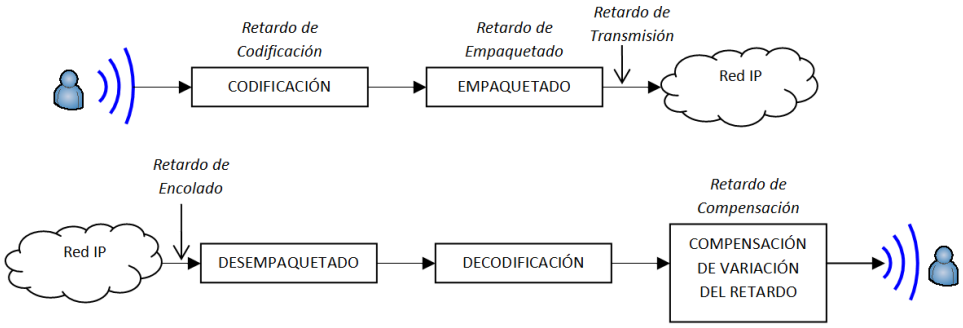

Figura 5.10: Contribuciones al Retardo

- *Retardo de Codificación:* producido en el sistema de muestreo y codificación de la voz. Se considera constante ya que el codificador de debe generar muestras a una tasa constante.
- *Retardo de Empaquetado:* introducido en el proceso de generación de los paquetes IP que contendrán las muestras de voz digitalizada, silencios, nivel de ruido, etc. Puede suponerse constante.
- *Retardo de Transmisión:* dependerá de la tasa binaria de acceso a la red. Típicamente constante.
- *Retardo de Propagación y encolado:* retardo variable producido al atravesar la red IP.
- *Retardo de Compensación:* introducido en el receptor para compensar la variación de retardo producida en la propagación y encolado.

El **eco** se ve afectado por la atenuación y el retardo. VOIP es una red digital de paquetes y por tanto tiene la ventaja de la inexistencia de atenuación y eco eléctrico, por ser una red digital, pero el retardo puede ser notable y variable, al ser una red de paquetes, y por tanto producir eco. Por lo tanto, para controlar el eco se utilizan canceladores de eco en todos los accesos a RTC.

El **retardo** sabemos que es variable[6] en una red de paquetes, pero la tasa de generación de tramas del codec es constante, así como el resto de retardos introducidos en el sistema, por lo tanto es necesaria una cola de espera en el receptor para ecualizar las muestras. Esto produce varios efectos inmediatos:

- A mayor cola, mayor retraso.
- Si se desborda, se descartan tramas del codec.
- Si se vacía el receptor únicamente escucha el ruido de confort.

Las **pérdidas** (o un retardo excesivo) pueden producirse por congestión en la red o por desbordamiento en la cola de compensación de variaciones del retardo, afectando a la distorsión de la voz.

Una vez vistos los factores que afectan a la calidad de la conversación y como medirla, es posible comparar los distintos resultados de calidades obtenidas utilizando diferentes codecs y sistemas de mejora de la calidad del servicio telefónico. La figura 5.11 recoge algunos resultados con los principales codecs utilizados.

[6] Jitter: retardo variable.

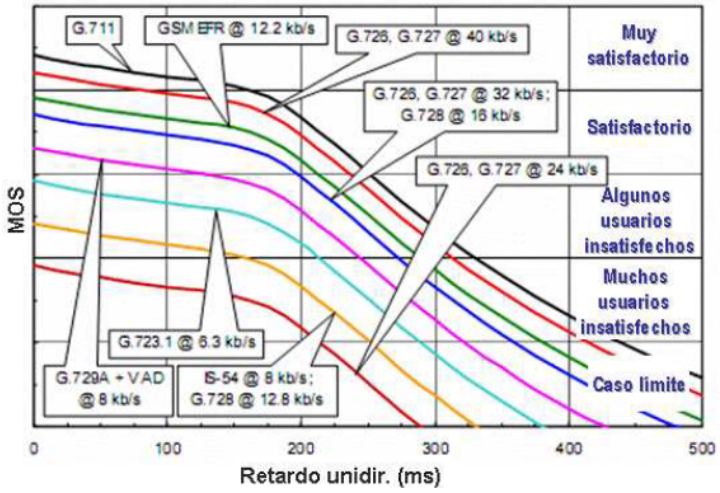

Figura 5.11: Comparativa Mean Opinion Square (MOS) en diferentes Codecs

Del estudio de la propia figura 5.11 es posible extraer una serie de **conclusiones** importantes:

- *Más recursos no implican más calidad.*
- *Con recursos dados hay varias calidades posibles.*
- *Hay calidades inalcanzables.*

Hemos introducido hasta este punto los principales aspectos que afectan a la calidad del servicio telefónico, como compensarlos y como medir a posteriori la calidad del servicio telefónico ofrecido. Es evidente, que en las fases iniciales de planificación de un servicio es necesario utilizar un método predictivo, que nos permita estimar la calidad que ofrecerá nuestro nuevo despliegue.

Para ello, la UIT-T ha definido unos **Métodos Predictivos**, con las siguientes propiedades deseables:

- Que prediga el resultado de la P.800, es decir, que sus resultados sean trasladables a un valor MOS.
- Que no requiera de participación humana.
- Que no requiera disponer de la red y por lo tanto proporcione información útil al planificador de la red.
- Que pueda automatizarse.

Por tanto, los métodos predictivos predicen la calidad a partir de parámetros mesurables tanto de la red (pérdidas, retardo y su fluctuación, como de los terminales (eco, retardo, distorsión, tipo de codec).

Existen dos categorías de clasificación de métodos predictivos:

- Paramétrico / Psicoacústicos.
- Activos / Pasivos.

Pasamos a continuación a estudiar tres métodos predictivos: *G.107, P.862 y el P.563.*

G.107: El Modelo E

El modelo E (UIT-T Rec. G.107) es una herramienta de planificación de transmisión que proporciona una predicción de la calidad de voz esperada, según la percepción de un usuario de teléfono normal, para una conexión telefónica completa extremo a extremo, es decir, de boca a oído, en condiciones normales de conversación.

El modelo E tiene en cuenta una amplia gama de alteraciones de telefonía, en particular, el deterioro debido a codificación a bajas tasa binaria, retardos, así como deficiencias clásicas de telefonía como pérdidas, ruido y eco.

Se puede aplicar para evaluar la calidad de voz de los escenarios de líneas fijas e inalámbricas, basadas en conmutación de circuitos y la tecnología de conmutación de paquetes.

Es un modelo paramétrico para la planificación, pero que puede ser usado también para evaluación pasiva. Predice un resultado, factor R [0,100], que es traducible a MOS, como vemos en la figura 5.12[7].

En cualquier caso se recomienda no utilizar sistemas con un parámetro R menor de 50.

Para el cálculo del parámetro R se toma como punto una **hipótesis aditiva**, en la que se considera que los factores de degradación son directamente aditivos en el dominio psicológico (percepción del usuario). Así, la calidad percibida resulta de la suma algebraica de una serie de degradaciones que incluyen distorsión de la cuantificación, ecos, retardo, distorsión adicional en codecs de baja tasa, expectativas del usuario, etc.

[7] La obtención de esta gráfica puede consultarse en el anexo B de la Rec. G.107

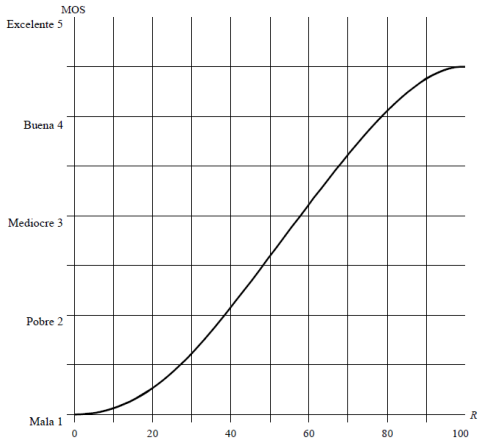

Figura 5.12: MOS en función del factor de determinación de índices R

Parámetro R	**Calidad**	**Satisfacción Usuario**	**Equ. MOS**
$90 \leq R \leq 100$	Best	Very satisfied	5
$80 \leq R \leq 90$	High	Satisfied	4
$70 \leq R \leq 80$	Medium	Some users dissatisfied	3
$60 \leq R \leq 70$	Low	Manny users dissatisfied	2
$50 \leq R \leq 60$	Poor	Nearly all users dissatisfied	1

Tabla 5.2: Modelo E: definición de categorías de calidad de transmisión de conversación

En una primera etapa, el resultado de cualquier cálculo con el modelo E en una primera etapa es un factor de determinación de transmisión R, que combina todos los parámetros de transmisión pertinentes para la conexión considerada. Este factor de determinación de índice R está constituido por:

$$R = R_o - I_s - I_d - I_e + A \tag{5.1}$$

- *Factor R_o:* representa en principio la relación señal/ruido básica que incluye fuentes de ruido como ruido de circuito y ruido ambiente.
- *Factor I_s:* es una combinación de todas las degradaciones que aparecen de forma más o menos simultánea con la señal vocal, como efectos locales, distorsión de cuantificación, ...
- *Factor I_d:* representa las degradaciones producidas por el retardo y el factor de degradación de equipo, es decir efectos de retardo y eco.
- *Factor I_e:* representa las degradaciones producidas por codecs de velocidad binaria baja y pérdidas de paquetes.
- *Factor de expectativa A:* permite compensar los factores de degradación cuando existan otras ventajas de acceso para el usuario, como el acceso móvil o por satélite.

El modelo E puede ser utilizado de forma pasiva, tal y como se recoge en la figura 5.13.

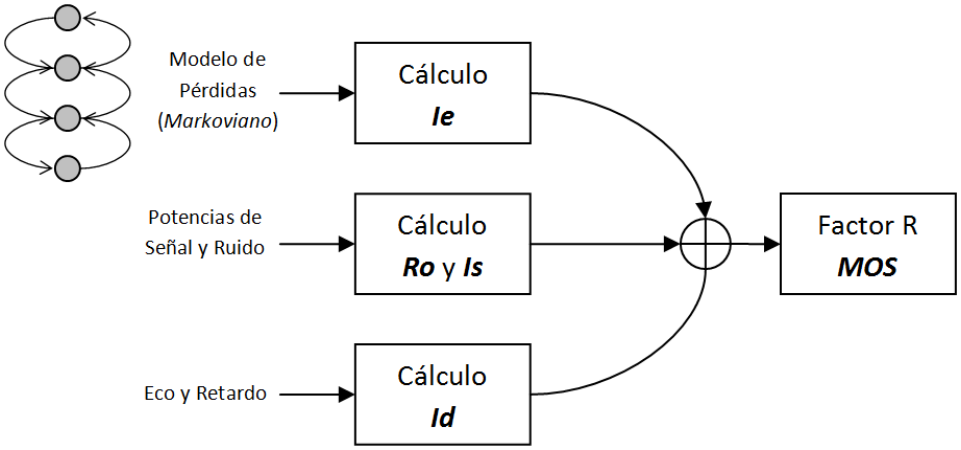

Figura 5.13: Modelo E: uso pasivo

El modelo E admite un cálculo simplificado para una aproximación del parámetro R. Dicho calculo se realiza con la ecuación:

$$R = 93,2 - I_d - I_e \tag{5.2}$$

Donde el parámetro I_d es el límite de retardo en la red y el parámetro I_e es la degradación por pérdida de paquetes en la red según el codec utilizado. La gráfica 5.14 recoge la estimación del parámetro R en función del codec y del TELR (Talker Echo Loudness Rating).

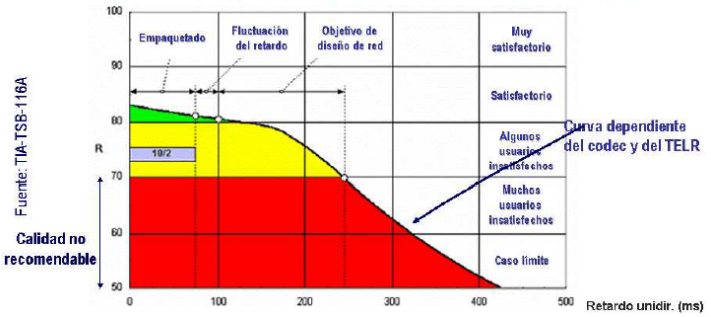

Figura 5.14: MOS en función del factor de determinación de índices R

El modelo E está bastante extendido[8], sin embargo presenta una serie de carencias que es conveniente conocer:

- La hipótesis aditiva se sabe errónea.
- Respecto a los parámetros utilizados, I_e, I_d, I_s, sus valores son suministrados por fórmulas diseñadas por la ITU, sin embargo se obtienen pocos valores de algunos parámetros y a menudo erróneos.
- No contempla degradaciones que varíen con el tiempo.
- Utiliza un modelo de pérdida de paquetes simplista (Bernouilli, Markoviano de 2 estados o Markoviano de 4 estados).

P.862: Perceptual Evaluation of Speech Quality

La recomendación P.862 describe exhaustivamente el método de *evaluación de la calidad vocal por percepción* (Perceptual Evaluation of Speech Quality, PESQ). Es el resultado de varios años de trabajos de desarrollo y es aplicable no sólo a los codecs vocales sino también a las mediciones de extremo a extremo. Es una evolución de otros modelos anteriores como el UIT-T P.861 Perceptual Speech Quality Measure (PSQM) y Perceptual Analysis Measuremente System (PAMS).

Es un método para evaluación de calidad para telefonía en banda vocal y en un único sentido, utilizando para ello el envío de muestras de referencia.

[8]Una implementación del modelo la encontramos en `http://www.itu.int/UIT-T/studygroups/com12/emodelv1/index.htm`

Tiene una extensión para codecs de banda ancha.

Modela la percepción humana, midiendo la distorsión sufrida por muestras de voz al atravesar el sistema y, si es posible, traduce el resultado a MOS. Su esquema básico de funcionamiento se recoge en la figura 5.15, donde vemos como utiliza muestras vocales antes de entrar al sistema y después de atravesar el mismo para poder generar el modelo psicoacústico.

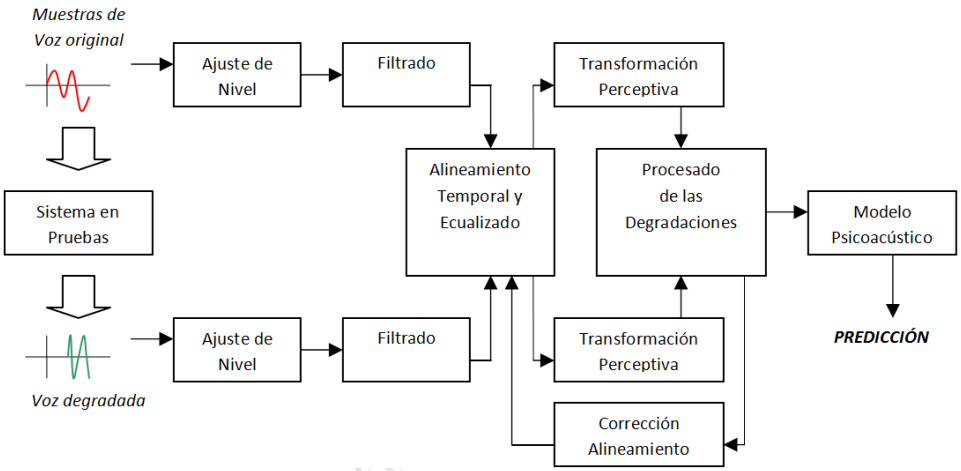

Figura 5.15: Esquema Funcionamiento Modelo P.862

Respecto a este modelo debemos tener en cuenta las siguientes conclusiones:

- Es un método de evaluación unidireccional, que no contempla retardo, eco o bajo volumen, únicamente valora la calidad de escucha.
- Es intrusivo: utiliza material vocal procedente de 8 hombres y 8 mujeres, en 7 idiomas y usando 4 codecs (AMR/G.729/G.723.1/iLBC).
- No es válido para planificación, pues requiere acceso al sistema, pero sí es válido para evaluar la calidad del sistema (Service Level Agreements, SLA) ofrecida por los operadores a los usuarios.

P.563: Medida de calidad vocal en un extremo

El algoritmo P.563 es aplicable para la predicción de la calidad vocal sin una señal de referencia independiente. Por ese motivo, este método se recomienda para la evaluación no intrusiva de la calidad vocal y para la supervisión y evaluación con la red en funcionamiento, empleando en el extremo lejano de una conexión telefónica fuentes de señal vocal desconocidas.

Utiliza un doble modelo de análisis estadístico, uno del mecanismo de producción de voz humana y otro del mecanismo de percepción auditivo.

El esquema básico de funcionamiento se recoge en la figura 5.16.

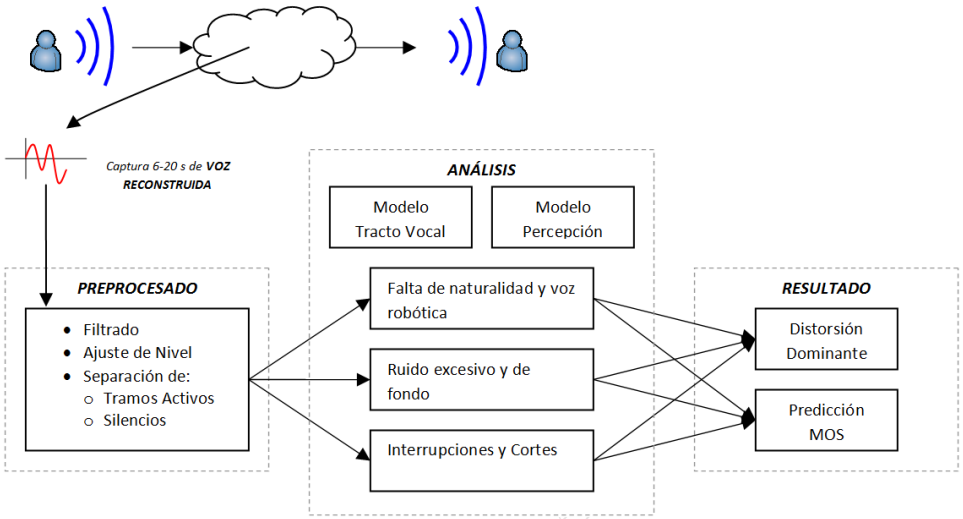

Figura 5.16: Esquema Funcionamiento Modelo P.563

Debemos tener en cuenta que únicamente es válido para monitorización de calidad y que presenta los siguientes inconvenientes:

- Válido sólo para telefonía en banda vocal (muestreo a 8 KHz).
- Codecs G.7XX y CELP con valores de régimen binario mayores de 4 Kb/s.
- Válido sólo para pruebas de escucha.

Conclusiones

A lo largo de esta sección hemos estudiado **factores de calidad del servicio telefónico** localizados *en los terminales* (codec, PLC, retado de empaquetado) y *en la red* (pérdidas y retardos variables en una red IP). Hemos estudiado también que existen dos enfoques para **medir la QoS**, un método utilizando *encuestas* y el otro método utilizando *métodos predictivos* (P.862, G.107, P.563), cuyas principales características se resumen en la tabla 5.3.

También hemos estudiado como **controlar la QoS**, tanto en los *terminales* (con la selección de adecuada de los distintos parámetros de configuración) como *en la red IP* (mejora de prestaciones con reserva de recursos,

G.107	Paramétrico	No intrusivo	Sin Señal de referencia
P.862	Psicoacústico	Intrusivo	Con Señal de referencia
P.563	Psicoacústico	No intrusivo	Sin Señal de referencia

Tabla 5.3: Características principales modelos predictivos

ingeniería de tráfico, ...)

Por último, no debemos olvidar que es necesario tener siempre una **red controlada**, ya sea por *sobredimensionamiento* o con *reserva de recursos*, teniendo en cuenta que *más recursos disponibles no implica más calidad*, ya que depende de la percepción del usuario y de los propios terminales utilizados.

5.3. Transmisión de Señalización de Circuitos en Redes de Paquetes

En este capítulo introducimos la arquitectura de red de nueva generación y realizaremos una descripción detallada de los protocolos de transporte de señalización (Signaling Transport, SIGTRAN) utilizados entre los elementos fundamentales de la arquitectura de red de nueva generación.

Una vez estudiado la arquitectura de red de las NGN, se pasara a estudiar las arquitecturas normalizadas SIP y MEGACO. No entraremos en el estudio de H.323.

5.3.1. SIGTRAN: Interfuncionamiento con Q.931/CSS7

Hemos comprobado que una red IP controlada puede ser tan fiable como la de señalización, con una serie de ventajas añadidas, como proporcionar encaminamiento dinámico, siendo más barata, flexible y fácil de configurar.

También hemos comprobado que la voz puede transportarse sobre IP y sabiendo que la señalización hace tiempo que utiliza una red digital de paquetes separada (SS7), parece lógico preguntarse **¿por qué no transportar también la señalización sobre una red IP?**

5.3.2. Arquitectura SIGTRAN

El grupo de trabajo SIGTRAN del IETF definió la arquitectura y requerimientos de rendimiento para transporte de señalización mediante redes

de paquetes en la RFC 2719. La arquitectura incluía el concepto de reconstrucción de la conmutación de circuitos tradicional utilizando una serie de elementos de red (MGC, MG, y SG), separando los planos de señalización y de control de medios.

SIGTRAN se caracteriza por:

- Ofrecer transporte transparente de protocolos de señalización para redes de conmutación de circuitos, basados en mensajes (Q.931, MTP3, partes de usuario SS7) y en cualquier punto (RDSI, RTC, PLMN[9]).
- Soportar primitivas normalizadas en la interfaz con la aplicación de red de conmutación de circuitos que esté siendo transportada.
- Complementar el protocolo de transporte IP con funciones diseñadas para satisfacer los requisitos de transporte de la señalización de conmutación de circuitos.

La RFC 2719 propone una **arquitectura de referencia**, donde se definen:

- Requisitos funcionales y marco de referencia.
- Relaciones entre entidades físicas y funcionales que intercambian información de señalización.
- Interfaces donde se puede usar SIGTRAN.
- Requisitos funcionales y de comportamiento que se aplican a los protocolos de señalización de redes de conmutación de circuitos, como por ejemplo control de flujo, entrega en secuencia, etc.
- Métodos de encapsulado.
- Protocolos extremo a extremo.
- Escenarios de señalización donde usar SIGTRAN.

En SIGTRAN se define pues una **Arquitectura de Red Integrada (Integrated Network Architecture, INA)**, recogidas en las figuras 5.17 y 5.18, donde vemos como se accede a la red SIGTRAN por diferentes elementos en cada caso.

Pasamos ahora a describir los distintos elementos que componen una red SIGTRAN:

[9]PLMN: Public Land Mobile Network.

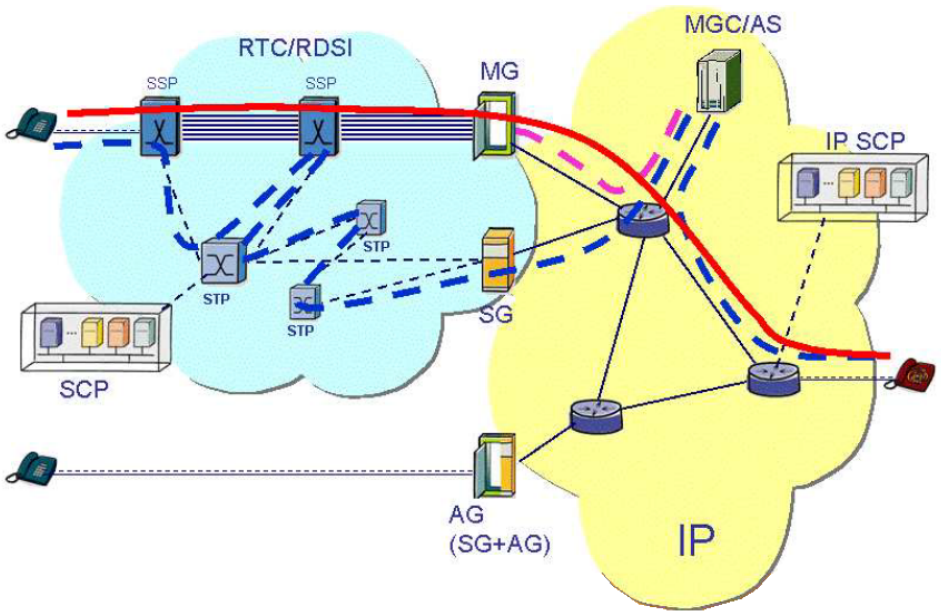

Figura 5.17: SIGTRAN: Arquitectura de Red Integrada (Acceso por MG y SG)

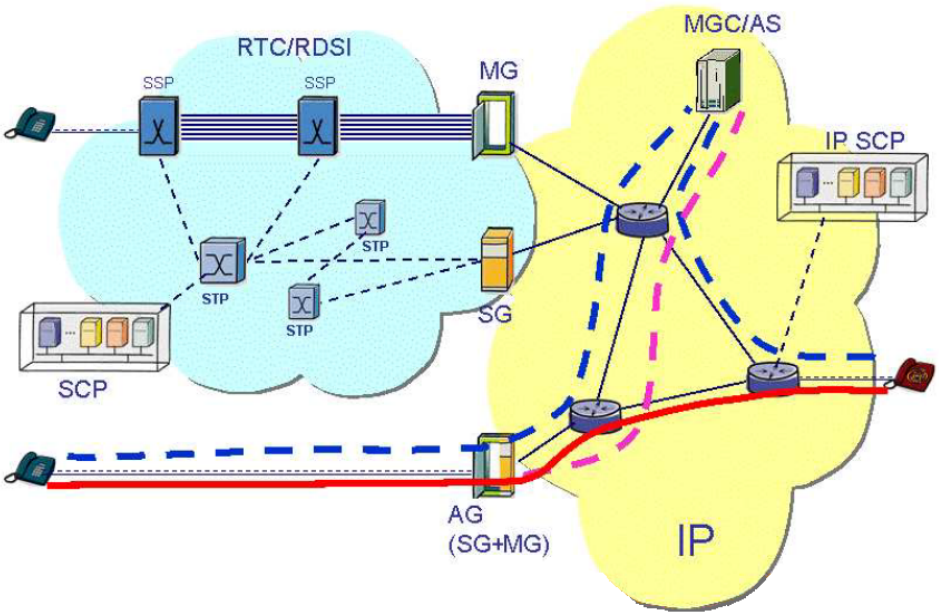

Figura 5.18: SIGTRAN: Arquitectura de Red Integrada (Acceso por AG)

- **MG - Media Gateway.** Pasarela de Medios. Termina los flujos de medios (voz, etc.) de la red de conmutación de circuitos. Convierte en paquetes el flujo procedente de la SCN y entrega el tráfico a la red de paquetes para transportarlo a su destino, realizando por supuesto la función inversa hacia la SCN.
- **SG - Signaling Gateway.** Pasarela de Señalización. Agente de señalización que recibe y envía señalización propia de la SCN en la frontera de la red IP. Retransmite, traduce o termina parcialmente la señalización de la SCN.
- **AG - Access Gateway:** pasarela de acceso completa. Es la unión en un único elemento de la la pasarela de medios y la pasarela de señalización, es decir: AG = MG + SG.
- **MGC - Media Gateway Controller.** Controladora de Pasarela de Medios. Maneja el registro y la gestión de los recursos de la MG. Autoriza el uso de recursos según políticas locales.
- **AS - Application Server.** Terminación de SCN. Posible punto de origen o terminación para aplicaciones de protocolo de SCN (ISUP, Q.931, etc.). Controla el acceso desde la red IP hacia/desde la SCN.
- **IPSCP - IP Service Control Point.** Punto de Control de Servicio IP. Pertenece a la red IP pero es direccionable desde la red SS7.
- **IPSEP - IP Signaling End Point.** Punto de finalización de señalización IP, es decir, es un nodo SS7 equipado con una conexión de red IP.

Vemos en las figuras también, como SIGTRAN permite la coexistencia de terminales IP. Algunas entidades físicas pueden estar agrupadas en algún caso, como por ejemplo:

- MGU - MG Unit.
- SGU - SG Unit.
- MGCU - MGC Unit.

En estos escenarios es frecuente encontrar algunos elementos de red SS7 ya estudiados, como por ejemplo SEP (Signaling End Point) o STP (Signaling Transfer Point).

¿Dónde aparece SIGTRAN? SIGTRAN se utiliza para transportar señalización, por lo tanto, encontraremos SIGTRAN entre las siguientes entidades:

- SG - MGC.
- MG - MGC.
- MGC - MGC.
- SG - SG (cuando conectan SEPs o STPs en una SCN[10]).

Por lo tanto SIGTRAN tiene su **alcance** bien definido, siendo su función el *transporte transparente de señalización.* Quedan fuera de su ámbito funciones como:

- Definición de protocolos de SCN.
- Interfuncionamiento de señalización, por ejemplo, conversión de CAS a protocolos de señalización de mensajes.
- Especificación de funciones que tienen lugar en las pasarelas, como la determinación de la dirección IP destino para la señalización o los procedimientos para valorar el rendimiento de la sesión de transporte.
- Interfuncionamiento o intermediación en la pasarela de señalización, que es transparente a la función de transporte.

SIGTRAN propone una **arquitectura de protocolos**, recogida en la figura 5.19, basada en transporte IP.

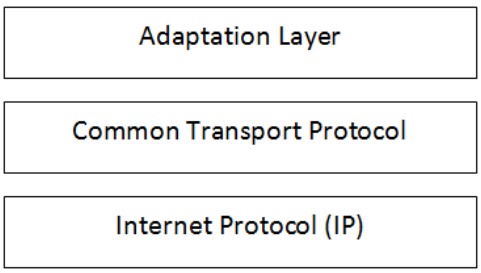

Figura 5.19: Torre de Protocolos Conceptual SIGTRAN

- **Capa de Adaptación (User Adaption, UA):** es específica para cada protocolo de señalización de conmutación de circuitos (Switched Circuit), soportando sus primitivas específicas.
- **Protocolo de Transporte de Señalización Común:** conjunto común de funciones de transporte fiables para el transporte de señalización.

[10]SCN: Switched Circuit Network.

Se definió un nuevo protocolo SCTP (Stream Control Transport Protocol) ya que el uso de TCP o UDP no se adaptaba correctamente al tráfico de señalización. SCTP no obstante es un protocolo de transporte genérico que puede usarse en otras aplicaciones.

- **Protocolo IP (IPv4/IPv6):** como red de transporte.

5.3.3. El protocolo SCTP

El grupo de trabajo SIGTRAN definió el protocolo de transmisión de control de flujo SCTP (Stream Control Transmission Protocol) en la RFC 2960.

SCTP es un protocolo de transporte fiable de propósito general, diseñado para el transporte de información sensible al retraso, y por tanto, adecuado para el transporte de señalización.

El diseño de SCTP surge para tratar de resolver las inconveniencias de TCP para ciertos tipos de aplicaciones, principalmente aquellas sensibles al retardo o con requerimientos en tiempo real, ya que TCP presenta ciertas características, como:

- TCP proporciona un único flujo de octetos, con garantía de secuencialidad, por lo que es ideal para entrega de largas cadenas de datos sin estructurar, como por ejemplo en aplicaciones P2P.
- Es sensible a los retardos originados en la red, pérdidas de octetos, mensajes o alteración de la secuencia, reteniendo todos los datos hasta que se recupera al modo de funcionamiento normal.
- Excesiva duración de los temporizadores, definidos en términos de muchos segundos.

Es interesante destacar no obstante, que en una red sin pérdidas TCP y SCTP deben ofrecer un rendimiento equivalente.

SCTP presenta las siguientes características:

- Protocolo orientado a conexión, punto a punto, proporcionando un intercambio de datos entre dos puntos definidos.
- Temporizadores más cortos que en TCP.
- Transporte fiable de datos de usuario, es decir implementa detección de errores y pérdidas de secuencia, que es capaz de recuperar.

- Velocidad adaptativa, por lo que es capaz de responder en situaciones de congestión moderando la tasa de transmisión.
- Soporta multiubicación (multihoming), de modo que cada extremo SCTP puede tener varias direcciones IP a las que se puede encaminar de manera independiente a las demás.
- Procedimientos de inicialización basados en cookies, por lo que previene ataques de denegación de servicio (Deny of Service, DoS).
- Orientado a flujo de mensajes, no a flujo de octetos. Define para ello tramas estructuradas de datos.
- Soporta empaquetado (bundling). Un mensaje SCTP puede contener múltiples pedazos y cada pedazo puede contener un mensaje de señalización.
- Soporta fragmentación, en la que un mensaje de señalización puede trocearse en varios mensajes SCTP.
- Soporta múltiples flujos simultáneos y cada flujo se entrega en secuencia independientemente de los demás.

Las dos últimas características, además de las mejoras de seguridad hacen más conveniente SCTP que TCP para transportar señalización. Introduciremos ahora una serie de conceptos que son básicos en el uso del protocolo SCTP.

- **Terminación SCTP:** emisor/receptor de paquetes SCTP. Se identifica por una o más direcciones IP y un único número de puerto.
- **Asociación:** relación entre dos terminaciones SCTP. Puede entenderse como una conexión.
- **Paquetes y Pedazos:** unidad enviada de emisor a receptor. Un paquete puede constar de varios pedazos.
- **Pedazos:** fragmento de datos que portan información de usuario (tipo 0) o bien información para el control de SCTP (otros tipos).
- **Flujos:** canal lógico unidireccional y ordenado entre terminaciones dentro de una asociación.

Estudiaremos ahora algo más en detalle algunas de las características propias de SCTP.

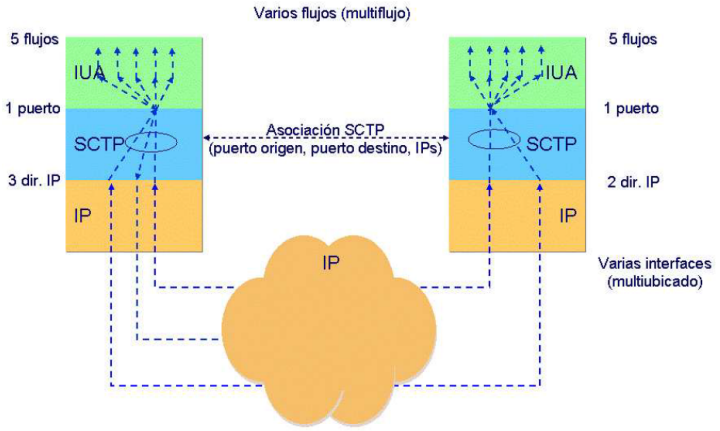

Figura 5.20: Ejemplo de escenario SCTP con 2 direcciones IP y 3 flujos

Separación de Flujos

SCTP utiliza flujos independientes para minimizar el impacto en el rendimiento ocasionado por la pérdida de paquetes si comparamos con el uso de TCP en el que únicamente se mantiene un flujo para toda la señalización. Así, en el ejemplo mostrado en la figura 5.21, al perder un paquete en TCP, se bloquearía la recepción de los siguientes hasta que el sistema se recuperase de la pérdida del paquete, es decir, volviera a enviarlo y a recibirlo correctamente.

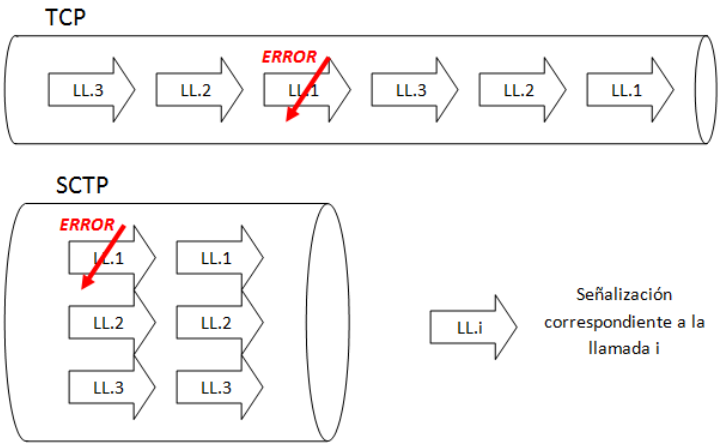

Figura 5.21: Separación de flujos en SCTP

SCTP permite mantener múltiples flujos, cada uno de ellos asociados a una aplicación o recurso particular, con lo que la pérdida de un paquete perteneciente a un flujo no afecta a los restantes flujos de señalización de las demás llamadas.

Formato de un mensaje SCTP

Como se recoge en la figura 5.22, los mensajes SCTP constan de una cabecera común, donde se incluyen los puertos origen y destino, una etiqueta de verificación asignada en el establecimiento de la asociación y un checksum de comprobación (CRC-32/Adler 32). Tras esta cabecera encontramos los distintos pedazos que componen el mensaje, encabezados cada uno de ellos por un campo que indica el tipo de pedazo, una serie de banderas (que dependen del tipo de pedazo) y finalmente la longitud del mismo.

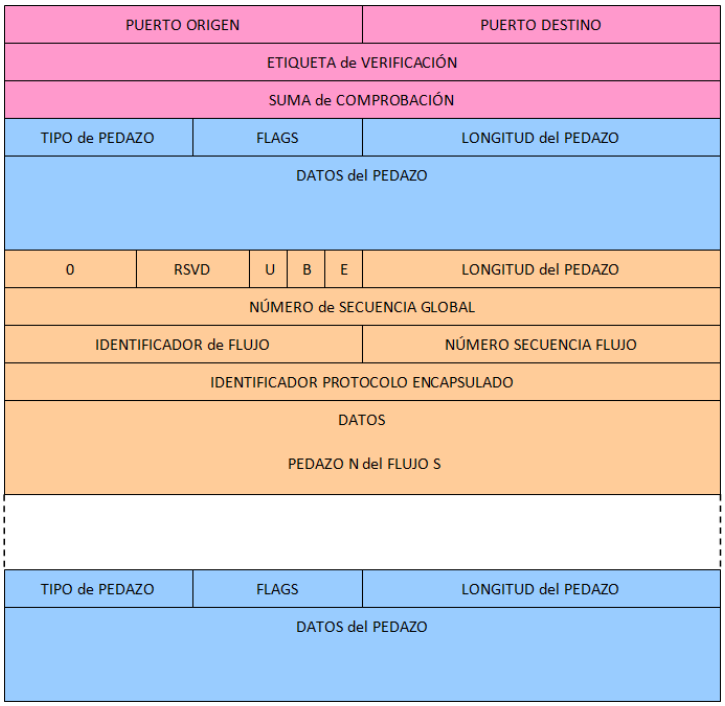

Figura 5.22: Formato de mensaje SCTP

Los pedazos los vamos a distinguir en dos grandes grupos, aquellos de tipo 0, que portan datos de usuario y por otro lado el resto de tipos de pedazos. Los indicadores de tipos de pedazo se recogen en la tabla 5.4. Las banderas de los pedazos tipo 0 son:

- *TSN:* Transmission Sequence Number.
- *U:* Unordered bit.
- *B:* Beginning fragment bit.

- *E:* ending fragment bit.

El campo *número de secuencia global* del pedazo es independiente de los de los flujos, que se asiente independientemente, haya o no salto en la secuencia. Posteriormente se encuentran el *identificador del flujo*, cuyo uso es dependiente del usuario y el *número de secuencia dentro del flujo*, usado para ordenar en recepción. Por último encontramos los *datos de usuario* (en el tipo 0) y los posibles *demás pedazos* que viajen en el mensaje SCTP, tal y como recoge la tabla 5.4.

Identificador	**Tipo de Pedazo**	**Short name**
0	Payload Data	DATA
1	Initiation	INIT
2	Initiation Acknowledge	INIT ACK
3	Selective Acknowledge	SACK
4	Heartbeat Request	HEARTBEAT
5	Heartbeat Acknowledge	HEARTBEAT ACK
6	Abort	ABORT
7	Shutdown	SHUTDOWN
8	Shutdown Acknowledge	SHUTDOWN ACK
9	Operational Error	ERROR
10	State Cookie	COOKIE ECHO
11	Cookie Acknowledge	COOKIE ACK
14	Shutdown Complete	SHUTDOWN COMPLETE

Tabla 5.4: SCTP: Tipos de Pedazos

Se admiten además una serie de parámetros opcionales, recogidos en la tabla 5.5.

ID Valor	**Parámetro Opcional**
5	IPv4 Address
6	IPv6 Address
9	Cookie Preservative
11	Host Name address
12	Supported Address Type

Tabla 5.5: SCTP: Parámetros opcionales

Control de Congestión

El control de congestión en SCTP se basa en el uso de una serie de parámetros:

- **Asentimientos Selectivos (SACK):** describen completamente el estado del receptor, indicando número de secuencia asentido, pedazos duplicados, pedazos que faltan, ...
- **Temporizador de Retransmisión (RTO):** calculado dinámicamente, es un temporizador básico, en el momento que vence, se retransmite.
- **Ventana de congestión (cwnd):** es ajustada por el emisor, de modo que s el número de octetos sin asentir alcanza este valor se suspende el envío de nuevos datos.
- **Ventana de Recepción (rwnd):** es anunciada por el receptor, así si el receptor indica que no dispone de sitio (aún no habiendo alcanzado la ventana de congestión), se suspende el envío de nuevos datos.
- **Umbral de Arranque Lento (slow start thresold):** marca el cambio de fase de arranque lento a fase de elusión de la congestión.
- **Unidad Máxima de Transmission (MTU):** tamaño en octetos de la unidad de datos más grande que puede ser enviada.

Todos estos parámetros, salvo rwnd (por asociación) son por ubicación IP del interlocutor (por destino).

Ahora bien, el control de congestión se realiza en tres fases, jugando con los parámetros anteriores:

- **Fase de Arranque Lento (slow-start):** al inicio o tras inactividad prolongada se utiliza el algoritmo 1 de control para maximizar la tasa sin causar congestión.

  Es decir, el algoritmo básicamente va incrementando cwnd en MTU. por cada SACK recibido hasta que se supera el umbral y se pasa a la fase de Elusión de Congestión.

- **Fase de Elusión de Congestión:** se realiza un aumento más cuidadoso, es decir lento, de la ventana de congestión. Si se agota cwnd se aumenta tal que $cwnd \leq cwnd + MTU$, cada RTT segundos. Si no se agota no se aumenta (¿para qué si no se usa?).

  Básicamente, en la fase de elusión de congestión se incrementa cwnd en MTU cada RTT segundos.

Algoritmo 1 Fase de arranque Lento

INICIO: $cwnd \leq 2 \times MTU$ y Fija Umbral Arbitrario
while $cwnd \leq UmbralArbitrario$ **do**
  Permanecemos En Arranque Lento
  if $cwnd > 0$ **then**
    Transmitir.
  end if
  if RTO **then**
    $cwnd \leq MTU$
  end if
  if SACK **then**
    $cwnd \leq cwnd + min(MTU, octetosasentidos)$
  end if
end while
Salimos de Arranque Lento

- **Fase de Control de Congestión:** se realizan dos posibles acciones:
  - En caso de pérdidas (4 SACK indicando un salto en TSN) se calcula el umbral como $umbral = max(cwnd/2, 2 \times MTU)$ y se asigna *cwnd=umbral.*
  - En caso de expiración de RTO (no se reciben SACKs) se calcula el umbral como $umbral = max(cwnd/2, 2 \times MTU)$ como antes, pero se asigna *cwnd=MTU.*

  Básicamente se reduce cwnd a la mitad o a MTU.

Como notas finales, destacar que se realiza un control de congestión independiente por cada ubicación de la asociación, es decir, una ubicación puede estar en arranque lento y otra en elusión de congestión, por ejemplo. El control de congestión no se aplica a los flujos individuales.

Establecimiento y Liberación de la Asociación

El establecimiento de la asociación en SCTP (figura 5.23) se realiza a cuatro bandas para evitar ataques de Denegación de Servicio (DoS) como ocurre en TCP. El estado de la asociación lo guarda el llamante o la red, pero nunca el llamado.

En el mensaje de INIT ACK se intercambia información como otras direcciones IP para configuraciones multiubicación, números de flujos, etiqueta de verificación, tiempo de validez de la cookie y firma digital de la misma, necesarias para el establecimiento de la asociación.

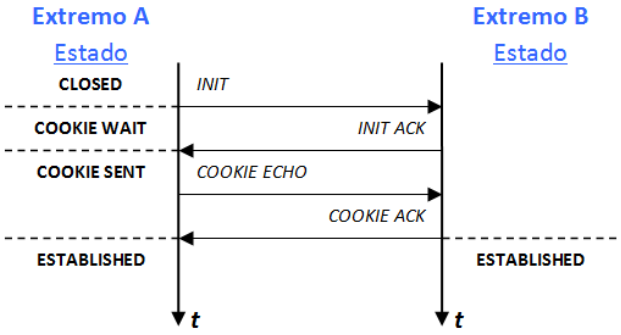

Figura 5.23: Establecimiento asociación SCTP

La liberación o cierre de la asociación (figura 5.24) se realiza con tres mensajes, para evitar sesiones pendientes de cierre como ocurre en TCP.

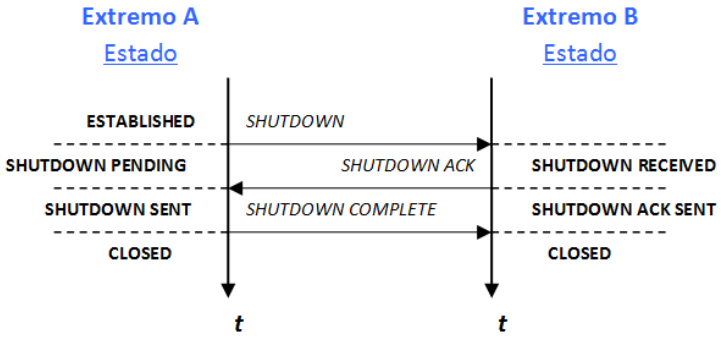

Figura 5.24: Liberacion asociación SCTP

5.3.4. Los agentes de usuario: IUA, M2UA, M3UA, SUA, V5UA

Las capas de adaptación de usuarios (*User Adaptation, UA*) encapsulan diferentes protocolos de señalización de redes de conmutación de circuitos, para su transporte sobre una red IP utilizando SCTP. Mientras que cada capa de adaptación es diferente en términos de encapsulación, debido a las diferencias en los propios protocolos de señalización, sí que presentan una serie de características comunes entre todas ellas:

- Soporte para el transporte de las capas altas de los protocolos de señalización sobre un transporte fiable basado en IP.
- Proporcionar la misma clase de servicio ofrecido en la interfaz equivalente de PSTN, es decir, debe ofrecer la misma impresión a los usuarios del servicio. Por ejemplo, M2UA soporta la misma interfaz que soporta MTP2.

- Deben ser transparentes, de modo que el usuario no debe darse cuenta de que la capa de adaptación ha reemplazado al protocolo original, o visto de otro modo, MTP3 no debe notar diferencia alguna entre usar M2UA o MTP2.
- Eliminar tanto como sea posible las capas bajas de SS7.
- Soporte para la gestión de asociaciones SCTP.
- Soporte para el informe asíncrono de cambios de estado a la capa de gestión.

Actualmente hay definidas siete capas de adaptación, que se denominan de acuerdo al servicio que sustituyen. De las siete capas estudiaremos únicamente cinco de ellas, recogidas en las figuras 5.25 y 5.26 que ofrecen una visión panorámica de las torres de protocolos utilizadas para la adaptación de la señalización SS7, es decir del plano de control, así como de los planos de control de dispositivo, a una red de transmisión IP.

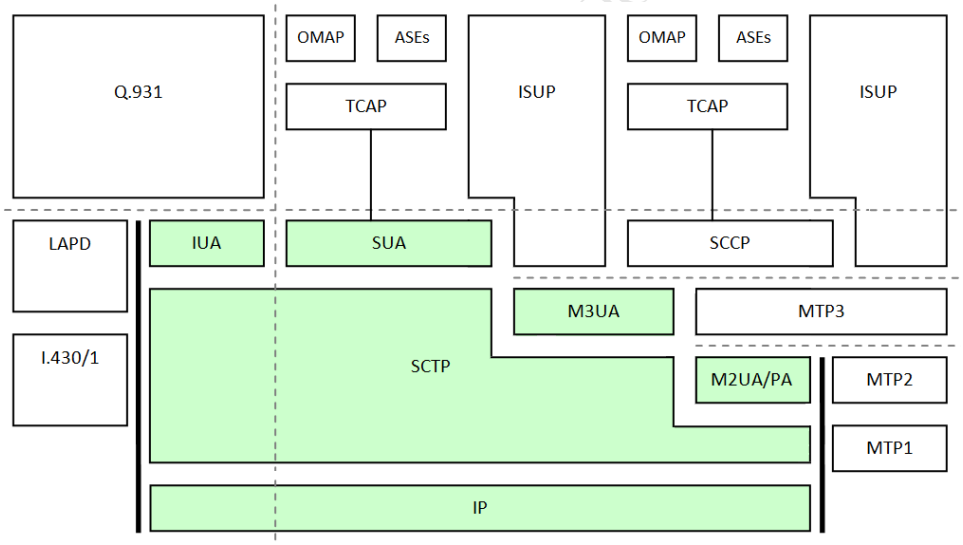

Figura 5.25: Arquitectura Comparada (I): Plano de Control

- **MTP Level 2 User Adaptation (M2UA)**, proporciona los servicios de MTP2 en una situación cliente - servidor, como por ejemplo entre SG $\longleftrightarrow$ AS. Su usuario es MTP3.
- **MTP Level 2 Peer Adaptation (M2PA)**, proporciona los servicios de MTP2 en una situación entre pares (peer to peer), como por ejemplo entre dos SGs (SG $\longleftrightarrow$ SG). Su usuario es MTP3.

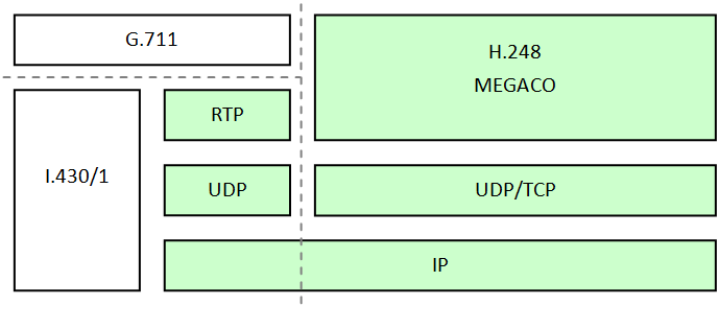

Figura 5.26: Arquitectura Comparada (II): Plano de Control de Dispositivo

- **MTP Level 3 User Adaptation (M3UA)**, Proporciona los servicios de MTP3 tanto en una situación cliente servidor como en una situación entre pares. Definida para el transporte de mensajes de la parte de usuario SS7, como ISUP, SCCP o TUP, ente un SG de SS7 y un MGC o cualquier otro punto de señalización basado en IP, como por ejemplo entre SG $\longleftrightarrow$ AS. Sus usuarios serán por tanto ISUP o SCCP.

- **SCCP User Adaptation (SUA)**, proporciona los servicios de SCCP en una arquitectura entre pares, como por ejemplo entre SG $\longleftrightarrow$ IPSCP. Definida para el transporte de mensajes de usuario TCAP, entre un SG de SS7 y un nodo de señalización IP o base de datos o entre dos puntos finales de la misma red IP.

- **ISDN User Adaptation (IUA)**, proporciona los servicios de la capa de enlace de RDSI (LAPD), definida por tanto para el transporte de Q.931 entre un SG RDSI y un MGC. Soporta tanto acceso básico como primario.

Las otras dos capas de adaptación utilizadas son V5UA, que proporciona los servicios del protocolo V.5.2 y DUA, para usuarios DPNSS/DSS2, aunque se pueden añadir otras capas según se requiera.

En los siguientes apartados estudiaremos en detalle las cinco principales capas de adaptación, aunque antes clarificaremos una serie de conceptos importantes.

Es importante destacar que que no es obligatorio utilizar como protocolo de transporte SCTP. El propietario de la red puede elegir TCP (o cualquier otro apropiado a sus intereses), siendo el único requisito la fiabilidad del mismo. En cualquier caso, puede ser necesario realizar un ajuste fino de los parámetros de control del protocolo, como por ejemplo *RTO, MTU, cwnd,*

nwnd, etc..

SCTP Payload	ID	Puerto
IUA	1	9900
M2UA	2	2904
M3UA	3	2905
SUA	4	14001
M2PA	5	3565
V5UA	6	5675

Tabla 5.6: RFC 1466: Telephony Signalling Transport over SCTP Applicability Statement

La figura 5.27 pone en contexto todos estos elementos.

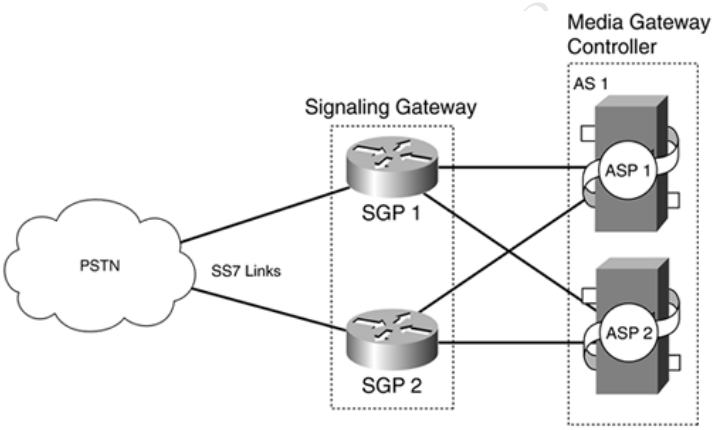

Figura 5.27: Ejemplo terminología UA

Sea cual sea la capa de adaptación, en la definición de las mismas se utilizan unas terminologías comunes (recogidas en la RFC 3332), que pasamos a introducir antes de pasar a estudiarlas:

- **Application Server (AS):** entidad lógica que sirve una entrada o función específica para el encaminamiento. Un ejemplo de AS es conmutador virtual que maneje todas las llamadas para un rango de red SS7 o por ejemplo una base de datos virtual, que implemente las funciones del HLR en una red móvil.
- **Application Server Process (ASP):** un proceso instancia de un AS. Un ASP actúa como un proceso activo (o de respaldo) de un AS, por ejemplo, uno de los procesos que compongan un servidor HLR distribuido.

- **Signaling Gateway Process (SGP):** un proceso instancia de un SG.
- **Signaling Gateway (SG):** agente de señalización, que recibe y envía señalización nativa de conmutación de circuitos en una frontera de red IP.
- **IP Server Process (IPSP):** proceso instancia de una aplicación IP. Un IPSP es esencia lo mismo que un ASP, excepto porque usa M3UA en configuración punto a punto. Conceptualmente, un IPSP no utiliza los servicios de un nodo SG.

Pasamos ahora sí, a estudiar las principales capas de adaptación.

M2UA

Transporta mensajes MTP3 en una configuración cliente - servidor. M2UA se define en la RFC 3331 y puede ser usado entre un SG y un MGC o entre SG y AS. El SG terminaría los enlaces estándares SS7 llegando sólo hasta MTP1 y MTP2, lo que proporciona transporte fiable para los mensajes MTP3 hacia los SPs o STPs. El SG debe proporcionar transferencia fiable de primitivas MTP2 sobre IP, utilizando SCTP como protocolo de transporte.

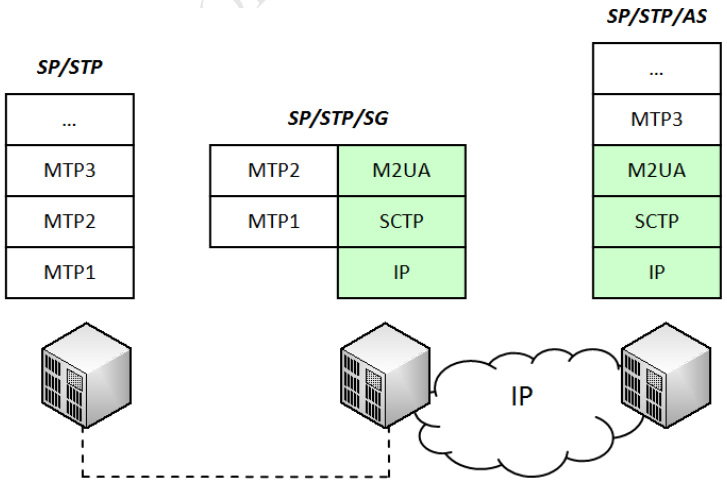

Figura 5.28: Arquitectura M2UA

M2UA también se puede utilizar entre dos SGs, aunque no en configuración peer-to-peer. Uno de los SGs terminaría los enlaces SS7 y reenviaría los mensajes MTP3 al otro SG, el cual terminaría el nivel MTP3.

M2UA soporta las mismas primitivas que entre MTP2 y MTP3, incluyendo soporte para alineamiento de enlace, reenvío de mensajes durante

cambio de enlace, interrupción de proceso local y remota y notificaciones de congestión de enlace.

M2PA

Similar a M2UA, MTP 2 Peer Adaption (M2PA), transporta mensajes MTP3 sobre IP utilizando SCTP, pero en una configuración entre pares. Además, M2PA soporta manejo completo de mensajes MTP3 y gestión de red entre dos nodos SS7 que se comunican por una red IP.

M2PA soporta las siguientes características:

- Operación transparente de entidades MTP3 sobre red IP.
- Soporte para fronteras MTP2 a MTP3.
- Soporte para la gestión de asociaciones SCTP como enlaces IP.
- Soporte para el informe de cambios de estado asíncronos a la capa de gestión.

M2PA puede usarse entre SG y MGC, entre SG y IPSP, incluso entre dos IPSPs, ... En cualquier escenario, se deben asignar sendos códigos de punto a ambos lados del protocolo M2PA. Dos IPSPs pueden utilizar enlaces M2PA y enlaces SS7 estándar de manera simultánea para enviar y recibir mensajes MTP3. M2PA puede utilizarse incluso entre dos SGs, configuración utilizada como reemplazo para enlaces SS7 de largo recorrido.

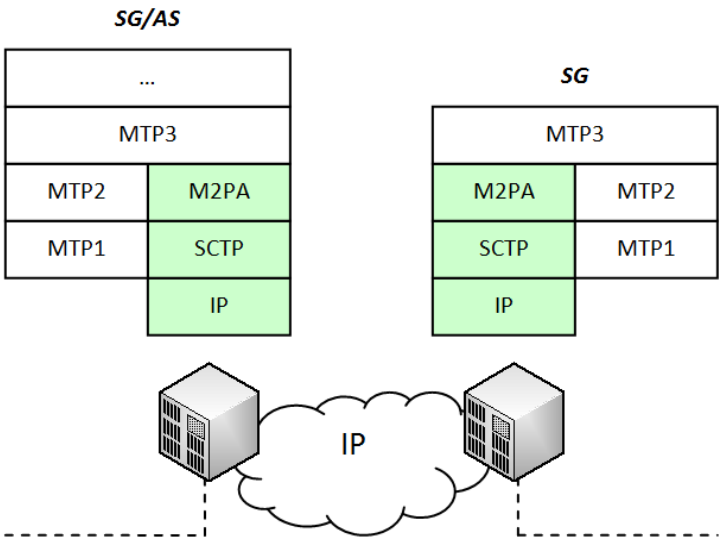

Figura 5.29: Arquitectura M2PA

M2PA y M2UA presentan similitudes y diferencias. Son similares en el sentido que ambos soportan primitivas MTP2 frontera con MTP3 y ambos transportan mensajes MTP3. Las diferencias surgen del tratamiento de las primitivas de la interfaz frontera MTP2. M2UA transporta la primitivas frontera del mismo modo que M2UA transporta los mensajes entre pares M2UA. M2PA procesa las primitivas frontera reemplazando MTP2 sin repetir necesariamente toda la funcionalidad de MTP2. M2PA proporciona enlaces SS7 basados en IP, lo que requiere que el SG/M2PA sea un nodo SS7 con un código de punto asignado. EL SG/M2UA no tiene tal requerimiento, ya que comparte el código de punto del MGC o del IPSP asociado.

M3UA

M3UA, definida en la RFC 3332, proporciona transporte para la señalización de la parte de usuario MTP3, como ISUP o SCCP, sobre IP utilizando SCTP. M3UA proporciona operación transparente entre pares de partes de usuario, soportando completamente primitivas de capa superior MTP3.

M3UA puede ser utilizado entre un SG y un MGC o entidades de bases de datos IP, o entre dos IPSPs.

El uso más común es entre un SG y un MGC o bases de datos IP (como IPSCP). El SG recibe la señalización SS7 sobre enlaces SS7 estándares, implementando los niveles MTP1 a MTP3 y proporcionando distribución de mensajes, o encaminamiento, de los mensajes de la parte de usuario definidos por el MGC o por la entidad de base de datos. Los MGCs pueden enviarse mensajes entre sí a través de un SG.

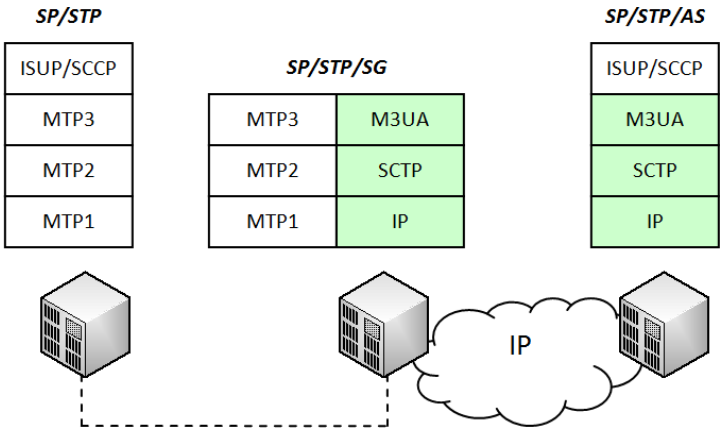

Figura 5.30: Arquitectura M3UA

SUA

SUA proporciona transporte de señalización de usuario SCCP, en nuestro caso principalmente TCAP, sobre IP utilizando SCTP. En efecto. se duplican los servicios SCCP, mediante el ofrecimiento de soporte para la transferencia fiable de mensajes de usuario SCCP, incluyendo soporte tanto para conexiones no orientadas a conexión (clases 0 y 1) como orientadas a conexión (clases 2 y 3). SUA proporciona también gestión de servicios SCCP para controlar el estado de los destinos remotos y subsistemas SCCP. En algunas configuraciones, SUA proporciona mapeo de direcciones y encaminamiento.

SUA puede ser utilizado entre un SG y un IPSP, o entre dos IPSPs.

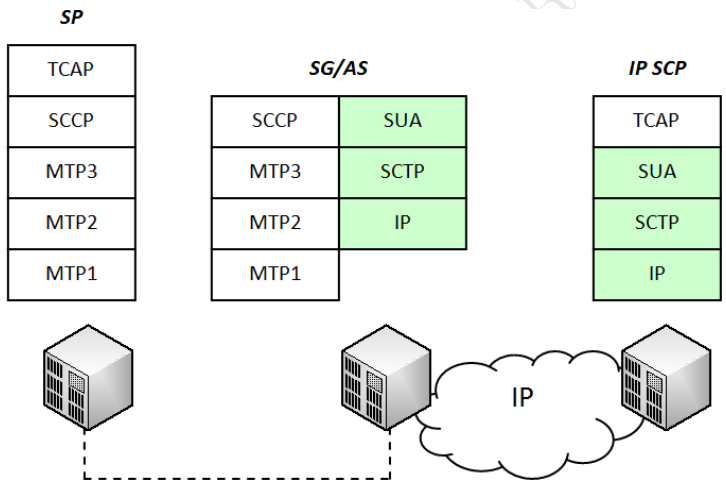

Figura 5.31: Arquitectura SUA

Con SUA, un SG puede actuar como punto final o como nodo intermedio de reenvío. Si se configura como punto final de señalización, necesitará un código de punto y un número de subsistema. Cuando actúe como nodo de reenvío, el SG debe realizar traducción de direcciones antes de poder determinar el destino de los mensajes entrantes. Esta traducción se puede modelar en un SCCP GTT (Global Title Translator) o basarse en hostname, dirección IP o cualquier otra información existente en la dirección de la parte llamada (Called Party Address, CdPA). La determinación de un punto de finalización de señalización IP se basa en el titulo global o cualquier otra información CdPA existente en el mensaje SUA.

IUA

Complementando el soporte de señalización SS7 sobre IP, el grupo SigTran definió el soporte de RDSI sobre red IP. La RFC 3057 define la ISDN User Adaptation (IUA). IUA ofrece soporte para señalización de usuario RDSI, Q.931, soportando accesos básicos (BRI) y primarios (PRI).

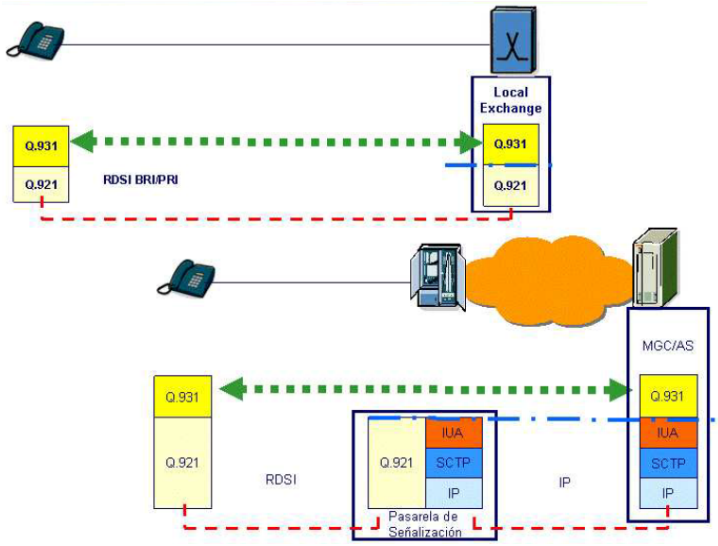

Figura 5.32: Ejemplo IUA

En IUA aparece el concepto de **Identificador de Interfaz**, que identifica la interfaz física a la que corresponden los mensajes de señalización (es el bucle digital de abonado). Tiene significado local a la pasarela y valor preacordado entre pasarela y AS.

En el ejemplo de la figura 5.33, el Application Server (AS) es una entidad lógica que termina señalización Q.931. Para la pasarela será visto como una lista de Application Server Process (ASP). Así la configuración de funcionamiento puede ser dominante (con un ASP activo y el resto de backups) o bien balanceada (con varios ASP activos compartiendo la carga de trabajo).

En la figura 5.34 se recogen los diagramas de paso de estado en AS/ASP.

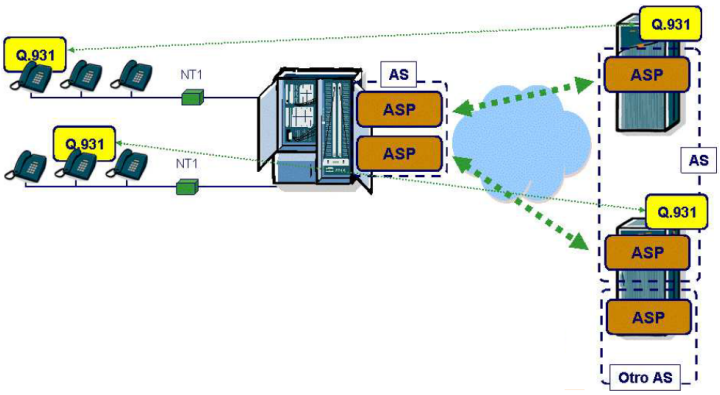

Figura 5.33: ASPs Dominantes o Balanceados

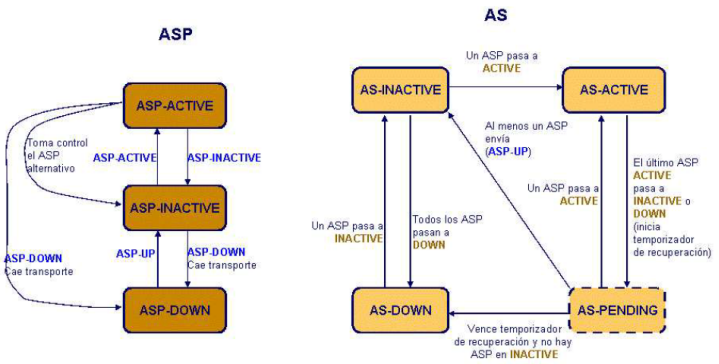

Figura 5.34: Estados AS/ASP

5.4. Arquitecturas Normalizadas: SIP, MEGACO

5.4.1. SIP: Session Initiation Protocol

SIP, recogido en la RFC 3261, es un protocolo de señalización para el establecimiento, mantenimiento y liberación de sesiones (orientadas a flujos multimedia) en redes IP, creado por el IETF.

En este apartado del tema estudiaremos la funcionalidad básica, arquitectura y elementos funcionales de SIP. Los dos componentes en un sistema SIP son los clientes, formalmente llamados agentes de usuario clientes (user agent clients) y los servidores de red (network servers). Las partes llamante y llamada son identificadas por direcciones SIP. Ambas partes necesitan poder localizar servidores y usuarios. Estudiaremos también el concepto de transacción.

Las funciones o capacidades principales del protocolo SIP son:

- Establecimiento y liberación de sesiones.
- Negociación de capacidades (Session Description Protocol, SDP).
- Localización de usuarios (movilidad).
- Disponibilidad de usuarios.
- Servicios suplementarios.
    - Mensajería instantánea.
    - Información de presencia (XML).

SIP se basa en un modelo de funcionamiento de tipo **cliente - servidor**, apareciendo el concepto de **Transacción**, de forma que una transacción se compone de una petición (cliente) y una o unas respuestas provisionales (servidor) más una definitiva.

Es compatible con otros protocolos de señalización y neutral frente a capas inferiores (TCP, SCTP o UDP e IP, IPX, ATM, AAL5, Frame Relay o X.25 en la capa inferior), siendo autodelimitado y sin fragmentación.

Utiliza sintaxis textual (ASCII) con elementos semejantes a HTTP[11] y SMTP[12], protocolos utilizados en los servicios de páginas web y de distribución de e-mails respectivamente. Esta similitud es natural ya que SIP fue

[11]HTTP: Hyper Text Transfer Protocol
[12]SMTP: Simple Mail Transfer Protocol

diseñado para que la telefonía se vuelva un servicio más en Internet.

Los **mensajes SIP** tienen una estructura genérica formada por una línea de inicio + líneas de cabecera + cuerpo opcional + cuerpo, donde este último porta la información de los niveles superiores, principalmente del protocolo SDP, para negociar los parámetros de conexión requeridos.

Existen dos tipos de mensaje:

- **Mensaje de Petición:** la línea de inicio esta formada por nombre de la petición + URI[13] llamado + versión del protocolo. Las peticiones o métodos posibles son: INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER, INFO, REFER, SUBSCRIBE, NOTIFY, MESSAGE, PRACK, UPDATE.
- **Mensaje de Respuesta:** la línea de inicio está compuesta por versión del protocolo + código de estado + motivo. El motivo es una descripción textual de la respuesta, pudiendo ser mensajes de respuesta provisional o definitivas, indicándose según sea en el código de estado.

Algunos campos habituales en los mensajes SIP son:

- **Línea de Inicio:** identifica el mensaje y contiene el tipo de petición/-respuesta, el URI llamado y la versión. Ejemplo: *INVITE sip:bob@biloxi.com SIP/2.0.*
- **VIA:** identificador de equipo. Se inserta una línea por salto, de forma que al final informa de la ruta que ha seguido el mensaje. Nos dice el protocolo de transporte usado, el puerto y un identificador de transacción que correla preguntas y respuestas.
- **Max-Forwards:** número máximo de saltos remanentes en servidores. Se decrementa en cada salto y evita que se produzcan bucles entre servidores SIP.
- **To y From:** son las direcciones origen y destino. En general son de la forma: *usuario@maquina.dominio*. El From lleva una etiqueta (*tag*) que actúa como referencia de llamada en el llamante. Será el mismo para todos los mensajes de una comunicación.
- **Call-ID:** identificador de conexión.
- **CSeq:** número de secuencia del mensaje, para detección de duplicados, no pérdidas y correlado (en ACK). Se incrementa de mensaje en mensaje.

[13]URI: Uniform Resource Identifier, identificador uniforme de recurso, es una cadena de caracteres corta que identifica inequívocamente un recurso

- **Contact:** dirección de acceso al terminal. Es el URI llamante.
- **Content Type y length:** descripción y tamaño del cuerpo del mensaje.

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bobsip:bob@biloxi.com
From: Alicesip:alice@atlanta.com ;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: sip:alice@pc33.atlanta.com
Content-Type: application/sdp
Content-Length: 142

(Aliceś SDP not shown)
```


Una **sesión** se identifica por una tupla **(Call_ID, From:, To:)**. En SIP hay varios tipos de URIs, recogidas en la tabla 5.7.

URI	SIGNIFICADO	LOCALIZACIÓN
sip	URI SIP	To:, From:, Contact:, ...
sips	URI SIP Seguro	
tel	URI Número E.164	To: o From
pres	URI agente de presencia	
im	URI cliente mensajería instantánea	
mailto	URL de correo telemático	Contact:
http	URL Web	

Tabla 5.7: URIs SIP

Las **respuestas** están formadas por un código de estado y un texto opcional (no determina el comportamiento). Hay varios tipos de clases:

- **1xx Informational:** la petición ha sido recibida y está siendo procesada, por ejemplo, 180 RINGING.
- **2xx Success:** la petición ha sido recibida, entendida y aceptada, por ejemplo 200 OK.
- **3xx Redirection:** se requieren más acciones para completar la petición, por ejemplo, 301 MOVED TEMPORALY.

- **4xx Client Error:** mensajes generados cuando la petición solicitada no es correcta, por ejemplo 404 NOT FOUND.
- **5xx Server Error:** mensajes generados cuando el servidor falla al tratar de atender una petición aparentemente correcta, por ejemplo 500 INTERNAL SERVER ERROR.
- **6xx Global Failure Error:** como 604, indicando que el usuario llamado no existe en ningún sitio.

Arquitectura de Protocolos

En SIP hay posibilidad de usar varios protocolos de nivel de transporte, pero siempre teniendo en cuenta que el transporte de señalización requiere fiabilidad, por lo tanto, si se elige un protocolo de transporte no fiable, deberemos implementar la fiabilidad en una capa superior.

La figura 5.35 recoge la torre de protocolos completa.

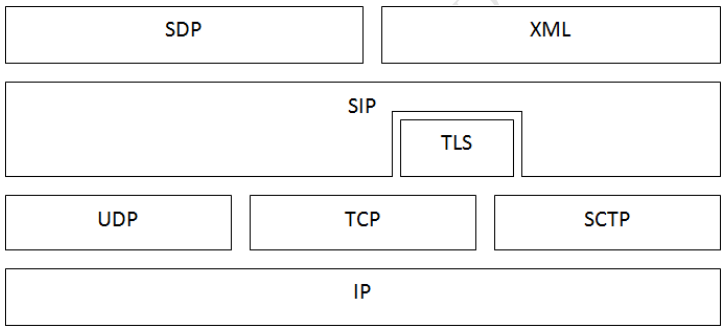

Figura 5.35: Arquitectura de Protocolos SIP

- **UDP:** se usa en entornos simples, con mensajes SIP cortos, autodelimita el mensaje SIP, no necesita establecer conexión. Es necesario usar servidores SIP con estados para fiabilidad.
- **TCP:** es más lento cuantos más servidores (necesidad de conexión) y se usa para mensajes largos. La delimitación debe hacerse con el Content_Length.
- **SCTP:** es el mejor para el control de múltiples llamadas, ya que unas no bloquearían a las otras. Es más robusto ante cambios tecnológicos y autodelimitado (por cada chunk un mensaje SIP).
- **SDP:** es un protocolo para la negociación de capacidades (medios a usar), que estudiaremos un par de secciones más adelante.

- **XML:** Extensible Markup Language, es un lenguaje que define un conjunto de reglas para la codificación de documentos en un formato específico. Puede utilizarse para negociar capacidades pero no lo estudiaremos.

Los contenidos de los protocolos SDP (o XML) viajan en modo texto en el cuerpo del mensaje SIP.

Arquitectura Funcional

La figura 5.36 representa los elementos que componen la arquitectura SIP, donde en general distinguimos agentes y servidores.

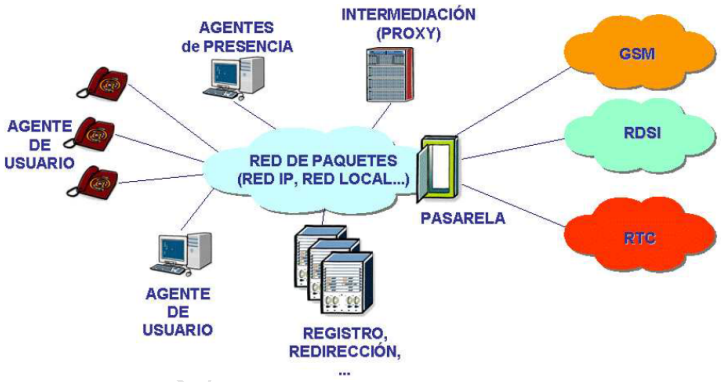

Figura 5.36: Arquitectura de Sistema SIP

Es importante destacar que muchos elementos tienen una parte cliente y una parte servidora.

Los **agentes** son:

- **Agente de Usuario:** establecen/liberan sesiones en nombre del usuario, es decir, genera peticiones y procesa información de sesión y medios. Habitualmente da servicios a pocos usuarios (pocas líneas).
- **Agente de presencia:** no establece ni libera conexiones, sólo recolecta información de presencia vía SIP u otros procedimientos. Utiliza los métodos SUBSCRIBE, NOTIFY.
- **Pasarela de señalización:** convierte señalización SIP en otros tipos (entre SIP e ISUP, CAS, Q.931, ...). Es un caso particular de agente de usuario, donde el usuario es un protocolo. Da servicio a muchos usuarios. Existe una importante diferencia respecto a las pasarelas SIGTRAN, y es que las pasarelas SIP terminan e inician señalización de circuitos.

- **Adosado:** es una pasarela de aplicaciones, pues genera nuevos mensajes SIP. Es un traductor de mensajes SIP-SIP para servicios especiales, como por ejemplo el uso de una pasarela para dotar de anonimato al usuario o bien para el sorteo de cortafuegos o servicios NAT.

Un cliente se puede encontrar dentro de un dispositivo de usuario, lo que podría ser un PC con un accesorio de manos libres portátil o un teléfono SIP, por ejemplo. Los clientes también pueden encontrarse dentro de la misma plataforma como un servidor.

Los **servidores** son

- **Servidor de intermediación (proxy):** *no genera mensajes nuevos*, sólo los reenvía o los contesta. La alteración del mensaje SIP es limitada y normalizada, pues no puede alterar el orden ni eliminar elementos, aunque sí puede añadirlos. No entiende de medios y no procesa el contenido del mensaje SIP, únicamente la cabecera.
- **Servidor de redirección:** contesta a los mensajes pero no reenvía peticiones. Se utiliza para traducir direcciones, localizar destinatarios, etc. Las respuestas las devuelve al llamante (3xx).
- **Servidor de registro:** permite al agente de usuario indicar una dirección de contacto que sustituye a la actual (REGISTER). Se conoce por configuración, por dominio o por multicast. La comunicación con el servidor de intermediación y redirección de su dominio esta fuera del ámbito SIP, pueden incluso residir en el mismo equipo.

Los servidores estudiados en la arquitectura SIP pueden ser implementados con o sin estados.

Un servidor de agente de usuario acepta las peticiones SIP y contacta al usuario. Una respuesta del usuario al servidor de agente de usuario resulta en una respuesta SIP en nombre del usuario. En realidad, un dispositivo de SIP (por ejemplo un teléfono SIP) funcionará como un cliente de agente de usuario y un servidor de agente de usuario. Al actuar como un cliente usuario-agente, que es capaz de iniciar solicitudes SIP. Actuando como un agente de usuario servidor es capaz de recibir y responder peticiones SIP. En la práctica éso significa que es capaz de iniciar y recibir llamadas, es decir, el protocolo cliente-servidor SIP puede utilizarse para establecer comunicaciones entre pares.

Los **métodos para establecimiento de llamadas** son:

- **INVITE:** utilizado para el establecimiento de nuevas sesiones o modificación de una existente, por ejemplo para modificar algunos parámetros. Suele describir los medios del llamante, aunque no es obligatorio.

- **ACK:** para asentimiento de las *respuestas definitivas* al método INVITE. Las de otros métodos no se asienten puesto que siempre son definitivas. Puede ser salto a salto o extremo a extremo (salvo 2xx que son siempre extremo a extremo). Incorpora información de medios si INVITE no lo hace. No incrementa CSeq para identificar a su INVITE.

- **BYE:** termina una sesión establecida.

- **CANCEL:** termina peticiones pendientes o sesiones no establecidas. No incrementa CSeq para identificar a su INVITE.

En las figuras 5.37 a 5.39 se recogen los procedimientos básicos de establecimiento de llamada, llamada cancelada y llamada rechazada.

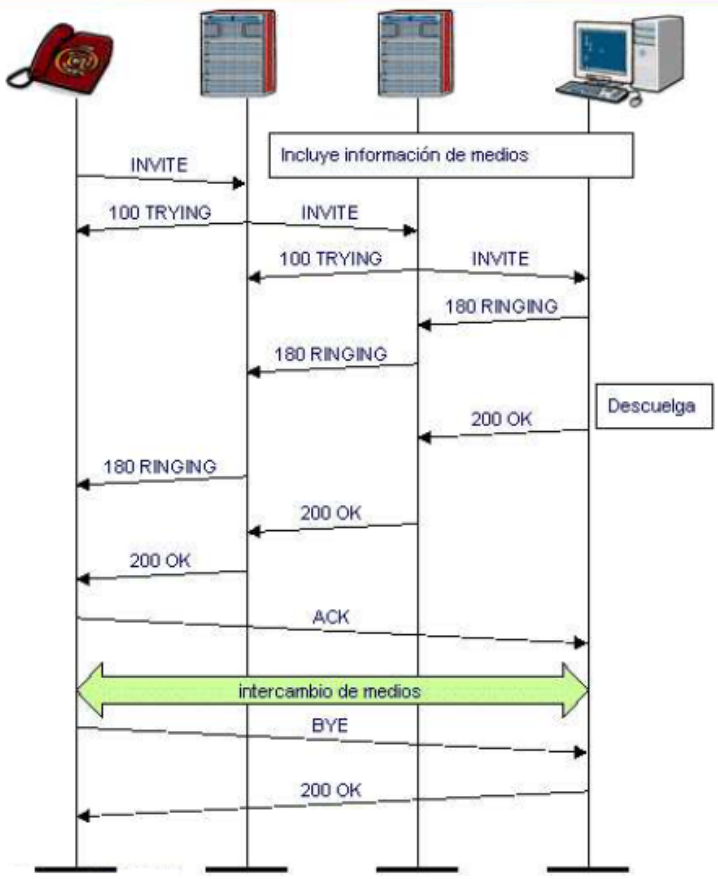

Figura 5.37: Establecimiento de llamada SIP

Los **métodos para suscripción y sugerencia**, utilizados por el servidor de registro y otros, son:

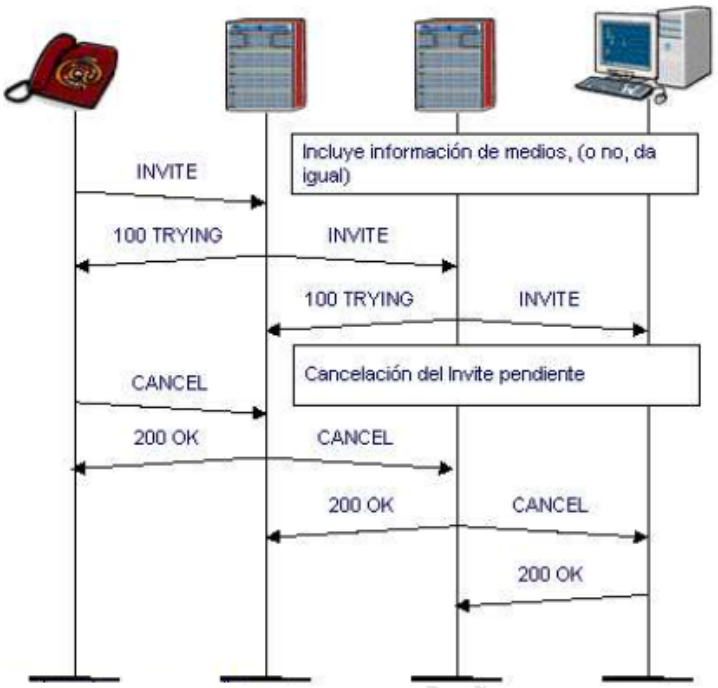

Figura 5.38: Llamada cancelada SIP

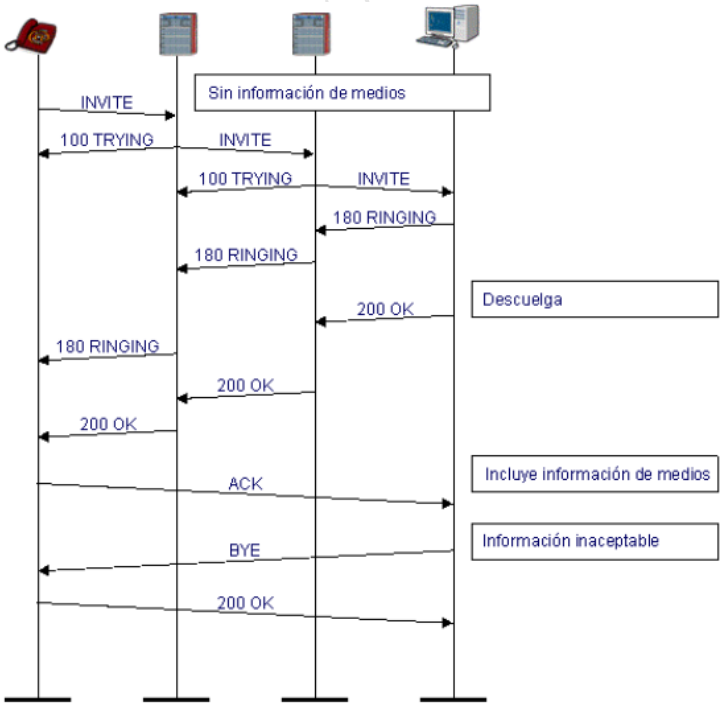

Figura 5.39: Llamada rechazada SIP

- **REGISTER:** notifica al servidor de registro del dominio SIP un cambio transitorio del llamante (1 hora por omisión), aportando el URI conocido y el URI al que hay que traducir. Permite a los proxies encaminar la llamada. No se necesita para iniciar la llamada, sólo se usa para llevar cuenta de los cambios de posición.
- **OPTIONS:** se usa para descubrir capacidades del destinatario (sea servidor o agente).
- **REFER:** se usa para solicitar al receptor que acceda a una URI. El uso es dependiente del URI referido en la línea Refer_ to para transferencias de llamadas SIP, redirigir a una página web (http), ...
- **NOTIFY:** notifica (informa) de un evento. En caso de suscripción requiere un diálogo.
- **SUSCRIBE:** indica la disposición del agente para recibir notificaciones sobre un evento en particular durante un tiempo limitado. Al igual que REGISTER, transcurrido este tiempo caducan.

En la figura 5.40 se recoge un ejemplo de suscripción mientras que en la figura 5.41 se recogen un par de ejemplos del uso del mensaje REFER.

Otros métodos que también se utilizan son:

- **MESSAGE:** se usa para mensajería instantánea, haya o no diálogo en curso.
- **INFO:** para transportar señalización extremo a extremo sin cambiar las características de los medios.
- **PRACK:** para asentimiento de respuestas provisionales.
- **UPDATE:** para cambiar características de una sesión cuando no es posible usar RE-INVITE.

Finalizamos el estudio de SIP con un ejemplo de establecimiento de llamada con redirección, recogido en la figura 5.42.

SDP

Session Description Protocol (SDP), es un protocolo basado en texto para describir los parámetros de inicialización de los flujos multimedia. Corresponde a un protocolo actualmente redactado en el RFC 4566 por la IETF, de los anteriores RFC 2327 de Abril de 1998 y RFC 3266 de Junio

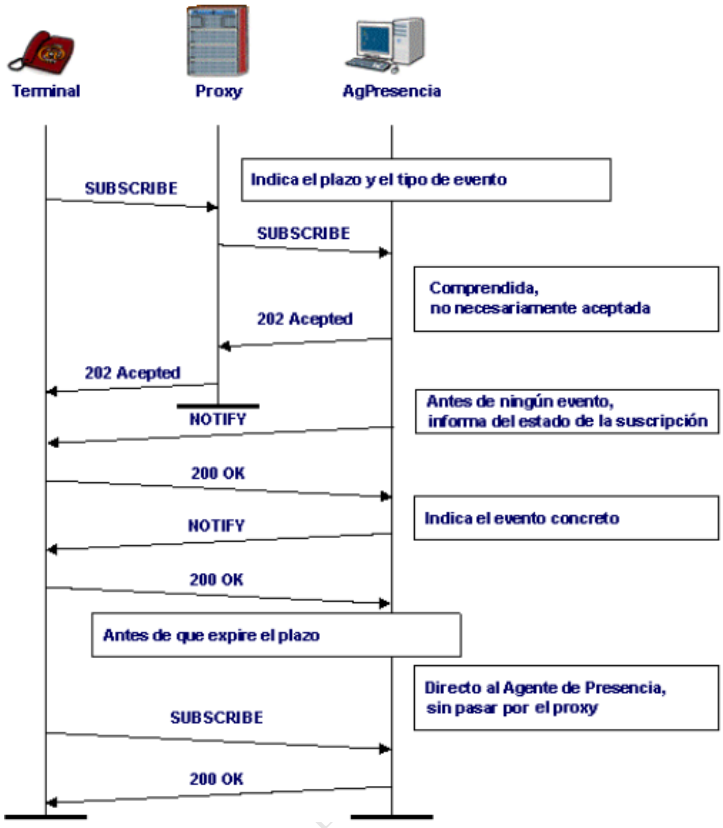

Figura 5.40: Suscripción SIP

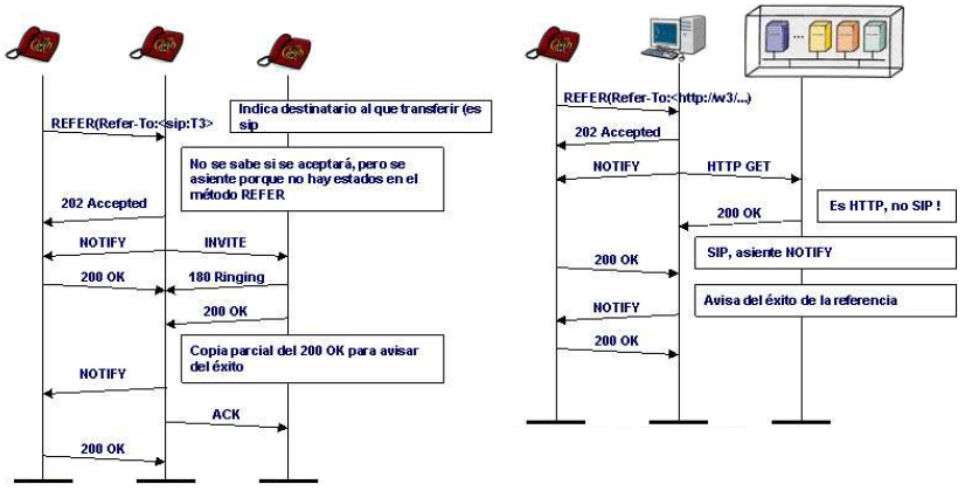

Figura 5.41: Referencia SIP

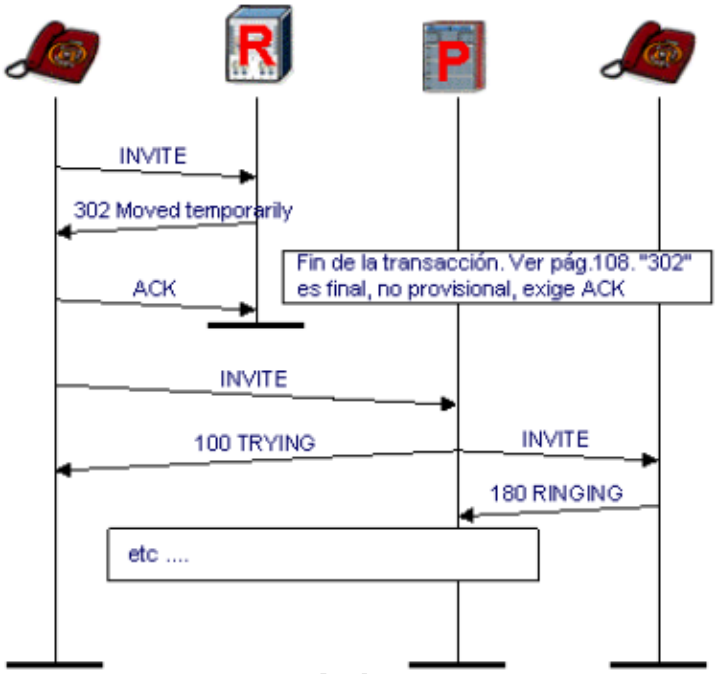

Figura 5.42: Establecimiento de llamada con redirección SIP

del 2002.

SDP está pensado para describir sesiones de comunicación multimedia, es decir, habla de medios, cubriendo aspectos como anuncio de sesión, invitación a sesión y negociación de parámetros. SDP no se encarga de entregar los contenidos propiamente dichos sino de entablar una negociación entre las entidades que intervienen en la sesión como tipo de contenido, formato, y todos los demás parámetros asociados. Este conjunto de parámetros se conoce como perfil de sesión. SDP se puede ampliar para soportar nuevos tipos de medios y formatos.

Comenzó como componente del SAP (Session Announcement Protocol), pero encontró otros usos en conjunto con RTP (Real-time Transport Protocol), SIP y como formato independiente para describir sesiones multicast.

Una sesión se describe con una serie de atributos, cada uno en una línea. Los nombres de estos atributos son un carácter seguido por '=' y el valor respectivo. Existen parámetros opcionales, denotados con '=*'. Los valores pueden ser una cadena ASCII, o una secuencia específica de tipos separada por espacios. La sintaxis de SDP se puede ampliar y ocasionalmente se agregan nuevos atributos a la especificación.

A continuación, en la tabla 5.8 se muestra un formato para el uso de SDP.

Ind.	**Atributo**
v=	(Versión del protocolo)
o=	(Origen e identificador de sesión)
s=	(Nombre de sesión)
i=*	(Información de la sesión)
u=*	(URI de descripción)
e=*	(Correo electrónico)
p=*	(Número telefónico)
c=*	(Información de conexión)
b=*	(Cero o más líneas con información de ancho de banda)
z=*	(Ajustes de zona horaria)
k=*	(Clave de cifrado)
a=*	(Cero o más líneas de atributos de sesión)
t=	(Tiempo durante el cual la sesión estará activa)
r=*	(Cero o más veces de repetición)
m=	(Nombre de medio y dirección de transporte)
i=*	(Título)
c=*	(Información de conexión)
b=*	(Cero o más líneas con información de ancho de banda)
k=*	(Clave de cifrado)
a=*	(Cero o más líneas de atributos de sesión)

Tabla 5.8: Atributos SDP

SIP y SDP forman un potente mecanismo para la transmisión de información de sesiones. SIP proporciona los mecanismos de mensajes para el establecimiento de sesiones multimedia y SIP proporciona un lenguaje estructurado para describir dichas sesiones. El cupero del mensaje SIP, identificado por su cabecera, proporciona el espacio donde se puede utilizar SDP.

SIP utiliza SDP en un modelo ofrecimiento/respuesta. El iniciador de la sesión ofrece una selección de formatos de medios para utilizar en la sesión. El receptor de la oferta puede o bien rechazar la oferta por completo o seleccionar alguno de los formatos ofrecidos a modo de respuesta.

En SIP es utilizado para la negociación de capacidades mediante los métodos:

- **OPTIONS:** un llamador potencial puede utilizar el método OPTIONS para determinar las capacidades de la potencial parte llamada. El receptor de la petición OPTIONS debe responder con las capacidades

(codecs, regímenes binarios, ...) que es capaz de soportar.

- **INVITE:** para el establecimiento o modificación de las sesiones.

Finalizamos con ejemplo de la figura 5.43 donde podemos ver en el cuerpo del mensaje SIP los distintos elementos SDP.

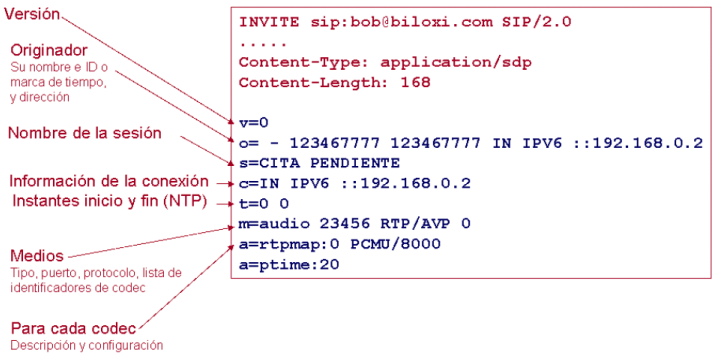

Figura 5.43: Ejemplo SDP

5.4.2. MEGACO/H.248

Motivación

Las arquitecturas de NGN basadas en H.323/SIP presentan problemas de escalabilidad de la pasarela, ya que esta soporta el paso de la señalización así como de los medios (tráficos de abonados), por lo tanto debe realizar almacenamiento de estados de llamada, tratamientos de señalización, ... y realizando el control de llamadas necesariamente en software, por lo que son sistemas altamente cargados y difícilmente escalables.

La solución adoptada consiste en descomponer la pasarela en dos pasarelas, una pasarela de medios y otra pasarela de señalización. Será necesario por tanto un control para la comunicación entre ambas, surgiendo así **Media Gateway Control (MeGaCo)**, que es una arquitectura para el control de dispositivos que permite a un controlador de pasarelas controlar a una pasarela esclava, como recoge la figura 5.44.

MeGaCo, definido en la RFC3015/H.248 y que tiene su precedente en el protocolo MGCP (RFC 2705) permite modos de codificación en texto plano (ABNF; RFC 2234) y binaria (ASN.1/BER). Es un sistema sin memoria de las transacciones previas entre controlador y esclavo.

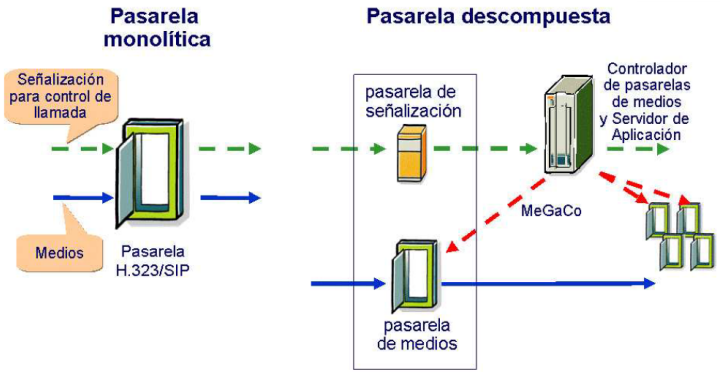

Figura 5.44: Motivación MeGaCo: Pasarela Descompuesta

Debemos destacar, que MeGaCo un protocolo de control de dispositivos, de control de conexión, no es un protocolo de señalización de voz IP. Por lo tanto MeGaCo no se modela dentro del plano de usuario ni del plano de control, sino que se suele representar en un plano propio de Control de Dispositivo.

Arquitectura

En la figura 5.45 se recoge la arquitectura del sistema y los elementos funcionales de MeGaCo, donde distinguimos:

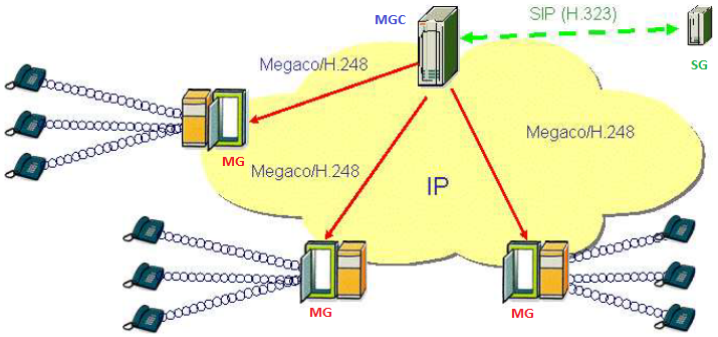

Figura 5.45: Arquitectura Sistema MeGaCo

- Pasarelas de Medios (MG).
- Controlador de Pasarelas de Medios (MGC).
- Pasarela de Señalización (SG).

Conceptos

Para comprender el funcionamiento de un sistema de pasarelas distribuida es necesario introducir los siguientes conceptos:

- **Terminación:** es una entidad lógica que reside en una MG que actúa como fuente o sumideros de flujos de medios. Distinguimos dos tipos:
  - *Persistente:* correspondiente a líneas analógicas o digitales (canal B en RDSI).
  - *Efímeras:* establecidas en la red de paquetes, se corresponden con flujos de medios, como los correspondientes a una sesión RTP. Las terminaciones efímeras son creadas como consecuencia del comando ADD y destruidas como consecuencia del comando SUBTRACT.

  Las terminaciones tienen propiedades especificas y las propiedades de una terminación específica variará acorde al tipo de terminación,es lógico pensar que una línea analógica tendrá distintas propiedades que un canal B RDSI. Las propiedades asociadas con una terminación se agrupan en un conjunto de descriptores, que pueden ser incluidos en los comandos MeGaCO, habilitando así propiedades o capacidades de acuerdo a las instrucciones enviadas por el MGC al MG.

  Es importante asignar a cada terminación identificador, siendo el MG el encargado de elegir el esquema de identificación a utilizar.

- **Evento:** es una situación detectable en la terminación por la MG e informable al MGC. Algunos ejemplos son colgar, descolgar, ... en terminaciones analógicas (no RDSI).

- **Señal:** es una excitación aplicable en la terminación por la MG. Ejemplos puede ser un tono llamando, o anuncios, como mensajes grabados, ...

- **Mapa de Dígitos:** el MG tiene parte de plan de numeración y puede hacer ciertas acciones en función de los dígitos recibidos para descargar a la MGC en algunas de sus funciones. Así, si por ejemplo se marca un dígito inválido no se molesta al MGC. También facilita el envío en bloque de los números marcados, aunque en la interfaz de usuario se hallan enviado solapados. Los mapas de dígitos se cargan en los MGs mediante operaciones de mantenimiento o bien mediante comandos MeGaCo.

- **Paquete:** es una agrupación normalizada de propiedades, eventos, señales, procedimientos y estadísticas soportadas por o asociadas a una terminación. Muchos están definidos en las recomendaciones H.248.6 a H.248.45.

- **Contexto:** es una asociación entre terminaciones con el objetivo de compartir medios entre dichas terminaciones, es decir, un contexto es algo similar a una conexión. En él se produce un intercambio de medios, transcodificación, mezclado de audio/video. Las terminaciones pueden ser añadidas, eliminadas o movidas de un contexto a otro. Una terminación sólo puede existir en un único contexto en cada instante teniendo en cuenta que las terminaciones en un MG únicamente pueden intercambiar medios si pertenecen al mismo contexto.

  Se define también un contexto nulo, utilizado para llevar a él las terminaciones permanentes, que son físicas y por lo tanto no se pueden finalizar, cuando no se están usando.

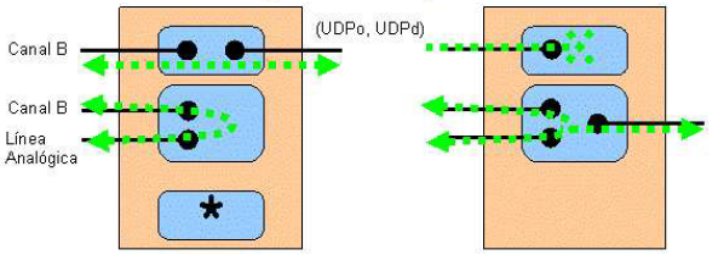

Figura 5.46: MeGaCo: Asociación de terminaciones

- **Transacción:** envuelven el paso de comandos y las respuestas a dichos comandos. Los comandos son dirigidos a las terminaciones asociadas a contextos. Es decir, cada comando especifica un identificador de contexto y uno o más identificadores de terminación sobre los que aplicar el comando. Esto es aplicable incluso para un comando que requiera alguna acción sobre una terminación ociosa que no exista en ningún contexto específico, utilizando en esta situación el contexto nulo.

  Se garantiza la secuencialidad de ejecución en una transacción, haciendo que el primer error detenga las órdenes de los siguientes. Por conveniencia las transacciones pueden organizarse en mensajes para su envío, pero no se garantiza la secuencialidad entre transacciones, aún en el mismo mensaje.

- **Mensaje:** no sólo es posible combinar múltiples comandos en una única transacción sino que es posible concatenar mútiples transacciones en un mismo mensaje. Las transacciones en un mensaje son tratadas de manera independiente. El orden de las transacciones en el mensaje no implica un orden en el que el receptor del mensaje deba ejecutar dichas transacciones. Aparece aquí una diferencia respecto al manejo de comandos en una transacción, donde el orden de los comandos sí es relevante y debe respetarse.

Las comunicaciones entre entidades MeGaCo siguen un modelo de comunicación basado en el intercambio de órdenes y respuestas, organizadas en transacciones. Las **órdenes** son:

- **ADD:** añade una terminación (o varias) a un contexto,(MGC $\longrightarrow$ MG). Si el comando no especifica un contexto en particular al que añadir la terminación, se crea un nuevo contexto. Si el comando no indica un identificador de terminación, el MG creará una nueva terminación efímera y la añadirá al contexto.

- **MODIFY:** cambia las propiedades de una terminación en un contexto, indica a una terminación que emita una o más señales o indica a una terminación detectar y reportar eventos específicos.

- **SUBTRACT:** elimina una terminación de un contexto. La respuesta al comando puede proporcionar estadísticas relacionadas con la participación de la terminación en el contexto. Estas estadísticas dependen del tipo de terminación en cuestión. Por ejemplo, para una terminación RTP pueden incluir elementos como paquetes enviados, recibidos, jitter, etc. Si el resultado del comando SUBTRACT es la eliminación de la última terminación de un contexto, el contexto es también eliminado.

- **MOVE:** mueve una terminación de un contexto a otro. Este comando no se utiliza para mover una terminación de o desde el contexto nulo, sino que dichas operaciones se realizan con los comandos ADD y SUBTRACT respectivamente. La capacidad de mover una terminación de un contexto a otro proporciona una poderosa herramienta para dar soporte a los servicios de llamada en espera.

- **AUDIT_VALUE:** es utilizado por el MGC para recabar información sobre valores de propiedades, eventos y señales asociadas con una o más terminaciones.

- **AUDIT_CAPABILITIES:** similar al comando AUDIT_VALUE, con la diferencia que este último recaba información sobre los posibles estados que una terminación puede asumir.

- **NOTIFY:** utilizado por el MG para informar de los posibles eventos detectados al MGC. Los eventos a reportar normalmente han sido seleccionados a tal fin previamente, como parte de un comando MODIFY del MGC al MG. Los eventos reportados irán acompañados de un parámetro de identificación de petición que habilite al MGC a correlar los eventos detectados con las solicitudes previas de notificación de eventos.

- **SERVICE_CHANGUE:** habilita al MG a informar al MGC que un grupo de terminaciones va a ser puesto fuera de servicio o bien que está siendo puesto en servicio de nuevo. Se utiliza también en una situación en la que un MGC cede el control de un MG a otro MGC. Es decir, sirve para realizar labores administrativas o de gestión de la pasarela de medios.

Las **respuestas** (REPLY) son asentimientos a las órdenes. Existe un REPLY por cada orden que se envía.

Tanto las órdenes como las respuestas utilizan una serie de parámetros, llamados **descriptores**, que pueden a su vez contener más parámetros. Ejemplos: *Modem, Multiplex, Media, TerminationState, Stream, Local, Remote, Events, Digitmap.*

Las figuras 5.47 y 5.48 muestran unos ejemplos de diálogo ante las órdenes ADD y MODIFY respectivamente.

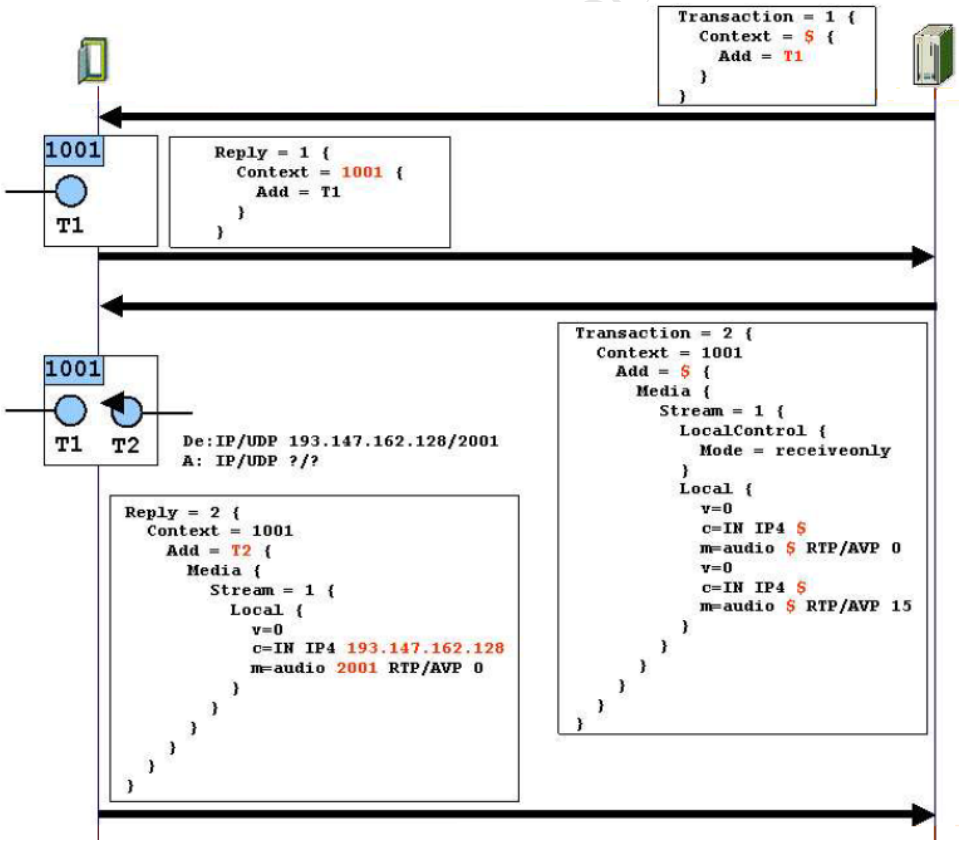

Figura 5.47: MeGaCo: ADD

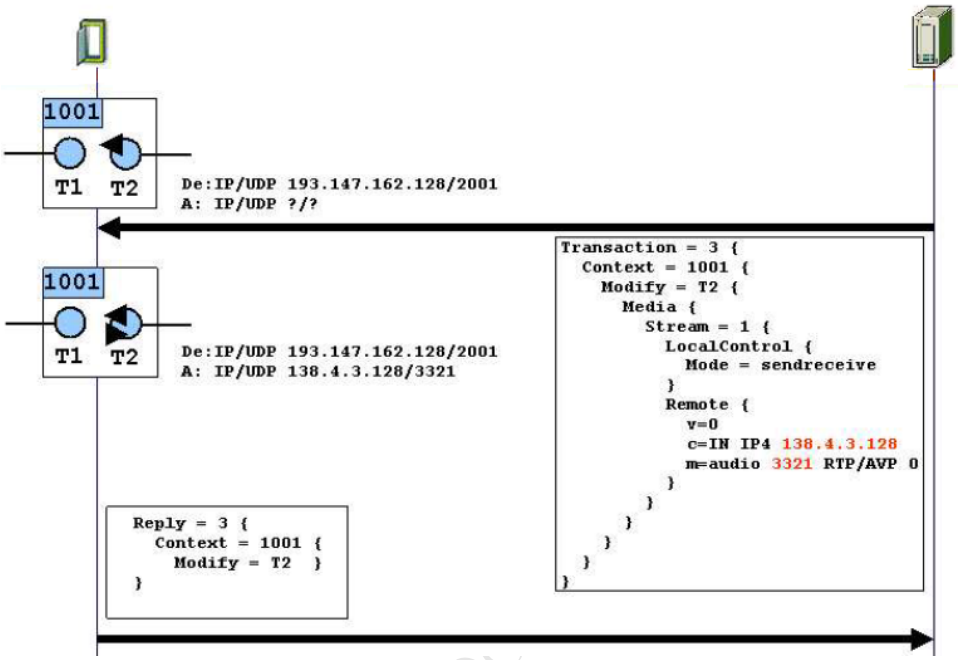

Figura 5.48: MeGaCo: MODIFY

El protocolo de transporte utilizado en MeGaCo es abierto, con la condición de que sea fiable. Podemos usar por tanto:

- *UDP:* con entramado ALF y fiabilidad *At-Most-Once*, en la que una transacción como mucho se ejecuta una vez. El originante guarda el identificador de transacción hasta que recibe una respuesta.
- *TCP:* con entramado RFC 1006. Se define un formato de paquete sobre TCP y puede incorporar también el modelo *At-Most-Once*.
- *SCTP:* puede utilizarse con las ventajas ya conocidas sobre TCP.

Para el negociado de las capacidades se puede utilizar SDP, que iría dentro de mensajes MeGaCo. La arquitectura completa de protocolos se recoge en la figura 5.49.

Finalizamos el tema estudiando un ejemplo de establecimiento de llamada en MeGaCo, recogido en la figura 5.50, donde debemos ser conscientes que en paralelo a este diagrama es necesario otro pero referente al plano de control, que queda fuera de la arquitectura MeGaCo.

Existe un concepto adicional en MeGaCo, denominado **softswitch**, en el que si se añaden ciertas características adicionales al MGC, como tarificación, y se le añaden también capacidades de pasarelas y red, se comporta

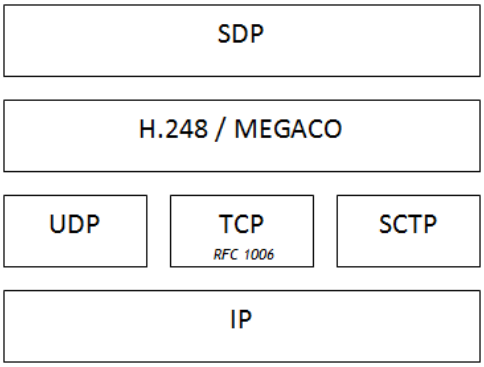

Figura 5.49: Torre de protocolos MeGaCo

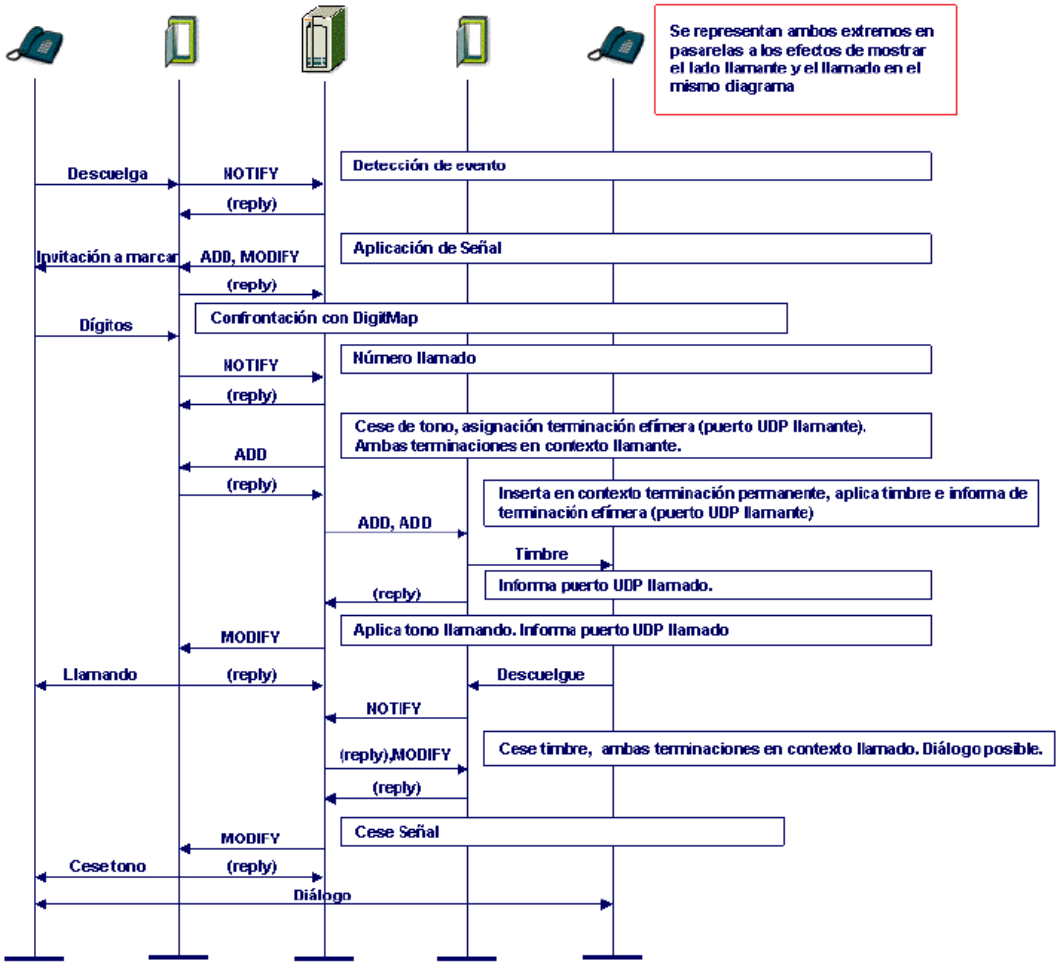

Figura 5.50: Ejemplo establecimiento de llamada MeGaCo

como una central (switch), siendo la conmutación realizada íntegramente en software y no en hardware. De ahí el nombre, softswitch.

Por implicaciones económicas, un sistema softswitch puede actuar como central local o de tránsito.

Capítulo 6

Redes de Acceso [1]

El tema de redes de acceso se estructura en tres secciones independientes donde se introducirán tres de las tecnologías más extendidas en el despliegue de redes de acceso basadas en tecnología sobre cable (o medio físico) que podemos considerar como dominantes actualmente del mercado, a saber:

- **Bucle Digital de Abonado.** Donde estudiaremos las distintas tecnologías xDSL existentes de manera comparativa y su grado de extensión en el mercado. Es decir, estudiaremos la evolución en la explotación del cable de pares para proporcionar servicios de banda ancha.
- **Redes de Telecomunicación por cable.** Describiremos la infraestructura de redes híbridas de fibra y cable (Hybrid Fiber Cable, HFC) y el modelo de distribución de señal así como el acceso a servicios de datos de banda ancha.
- **El acceso Ethernet (EFM).** Se estudiará la tecnología de Ethernet en la primera milla (EFM) así como la arquitectura para el soporte de los denominados comercialmente servicios triple-pay.

Debemos destacar que existen en el mercado otras tecnologías de acceso mediante medio físico, fibra óptica (FFTx) o comunicaciones por línea eléctrica (PLC) y que, por supuesto, no entramos en el estudio de las tecnologías de acceso inalámbricas, como pueden ser LDMS, acceso por satélite, redes locales inalámbricas (WLAN), redes móviles (GSM, UMTS) o televisión digital terrestre (TDT).

6.1. Bucle Digital de Abonado

Bajo las siglas xDSL se agrupan un conjunto de tecnologías que, utilizando códigos de línea y técnicas de modulación adecuados, permiten transmitir

[1] Este capítulo está basado en el trabajo [11], [9] y [1].

regímenes de datos de alta velocidad sobre el par trenzado telefónico.

Esta tecnología surge para reutilizar los más de 700 millones de pares de cobre instalados en todo el mundo, con unas previsiones de uso de 25 años, momento en el que se estima que comenzarán a predominar las conexiones de abonado con fibra (FTTH). Hasta entonces el par de cobre coexistirá con la fibra.

La familia de texnologías xDSL permite transmisión de datos del orden de varios Mbit/s sobre los pares de abonado de cobre, con lo cual parece ser la solución natural para operadores con bucle existente e incluso para operadores en despliegue terrestre.

Para el operador existente tiene la ventaja evidente que reutiliza la infraestructura ya desplegada a la vez que presenta una ventaja adicional que produce una descongestión de las centrales, que fueron dimensionadas para un patrón de llamadas más cortas (5 minutos).

Para el usuario presenta la ventaja de disponer de un acceso físico individual por abonado y con un elevado ancho de banda potencial, para las necesidades medias estimadas de los mismos.

En la tabla 6.1 se recogen las recomendaciones principales ITU-T para sistemas DSL.

6.1.1. Antecedentes

La explotación digital del bucle de abonado de cable de pares fue desarrollado a principio de los 80 como tecnología de acceso para líneas de abonado RDSI (Red Digital de Servicios Integrados). Su objetivo es usar los pares de cobre del servicio telefónico para proporcionar dos canales de 64 Kbit/s (canales B), que pueden ser utilizados para voz y datos en modo circuito, más un canal de 16 Kbit/s (canal D) para señalización o datos en modo paquete. El caudal útil total es por tanto de 144 Kbit/s, al que hay que añadir una tara de 16 Kbit/s adicional para funciones de mantenimiento, resultando en un régimen binario total de 160 Kbit/s.

En principio se utilizó un código 4Binario/3Ternario (4B3T) que fue pronto sustituido por un código 2Binario/1Cuaternario (2B1Q) que ocupa menos ancho de banda y por tanto tienen alcances mayores.

Existe también un Acceso Primario RDSI cuyo régimen binario es de 2 Mbit/s, transportando 30 canales B de 64 Kbit/s y un canal D de 64 Kbi-

Rec.	Descripción
G.991.1	Transceptores de línea digital de abonado de alta velocidad binaria (HDSL)
G.991.2	Transceptores de línea digital de abonado de alta velocidad binaria por un sólo par (SHDSL)
G.992.1	Transceptores de línea de abonado digital asimétrica (ADSL)
G.992.2	Transceptores de línea de abonado digital asimétrica (ADSL) sin divisores
G.992.3	Transceptores de línea de abonado digital asimétrica 2 (ADSL2)
G.992.4	Transceptores de línea de abonado digital asimétrica 2 (ADSL2) sin divisores
G.992.5	Transceptores de línea de abonado digital asimétrica 2 de banda extendida (ADSL2+)
G.993.1	Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria (VDSL)
G.993.2	Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria 2 (VDSL2)
G.994.1	Procedimiento de entrada en contacto para transceptores de línea de abonado digital
G.995	Panorámica de las recomendaciones de los transceptores de línea de abonado digital
G.996.1	Procedimientos de prueba para transceptores de línea de abonado digital
G.997.1	Gestión de capa física para transceptores de línea de abonado digital

Tabla 6.1: Recomendaciones ITU-T para DSL

t/s. Su aplicación principal es la conexión de centralitas privadas digitales. En principio utilizó los códigos de línea habituales en la transmisión PCM (HDB3). En la actualidad se utiliza transporte HDSL (ver más adelante) en algunas ocasiones.

Otra variante del acceso RDSI es el sistema AODI (Always On-line Dynamic ISDN) en el que el canal D (16 Kbit/s) está disponible permanentemente para el intercambio de datos y señalización. En caso de requerir más caudal, el sistema se encarga de activar uno o los dos canales B (64 Kbit/s), liberándolos cuando no son necesarios.

Podemos entender entonces, que los actuales accesos basados en tecnologías xDSL surgen como evolución de los accesos BRI y PRI definidos para RDSI.

6.1.2. G.991 - Transceptores de línea digital de abonado de alta velocidad binaria

G.991.1 - HDSL

Proporciona enlaces primarios E1 a 2 Mbit/s (o T1 a 1,5 Mbit/s, en países que siguen normativa ANSI) sobre uno o varios pares telefónicos convencionales evitando el empleo de repetidores, al menos en la mayoría de los casos, existiendo la posibilidad de utilizar repetidores HDSL en caso contrario.

Existen diversas variantes de esta tecnología, que difieren en cuanto a códigos de línea, velocidades de transmisión, distancias máximas alcanzables, así como el número de pares requeridos, el cual puede variar entre uno y tres, como se recoge en la figura 6.1.

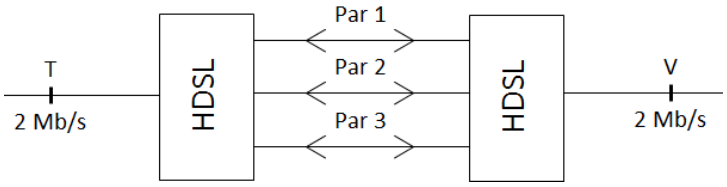

Figura 6.1: Pares HDSL

Las características técnicas más destacadas son:

- Código de línea: se utilizan las siguientes variantes:
  - PAM 2B1Q: consiguiendo 1544 Kbit/s sobre 2 pares.

  - PAM 2B1Q: con un régimen binario de 2048 Kbit/s sobre 1, 2 o 3 pares. A más pares, menor velocidad de símbolos y mayor longitud de línea.
  - CAP: logrando 2048 Kbit/s sobre 1 o 2 pares.
- Duplexión por compensación de eco.
- Banda incompatible con POTS[2].

Los sistemas HDSL se emplean para proporcionar accesos primarios RDSI, así como para el suministro de líneas alquiladas. Otra aplicación habitual de este tipo de sistemas es la interconexión de equipos de red situados en la planta exterior de acceso del operador (por ejemplo, estaciones base de telefonía móvil o concentradores remotos de abonados).

Debido a que los sistemas HDSL emplean distintos sistemas de transmisión de línea, así como a la existencia de realizaciones propietarias de la operación y mantenimiento, los equipos de central y de usuario han de ser suministrados por el mismo proveedor.

En el año 2002, el total de líneas HDSL instaladas mundialmente se estima en 12,6 millones. Los precios de una línea HDSL, incluyendo equipo lado central y equipo lado usuario pueden oscilar entre 550 y 1.000 euros, variando mucho por volúmenes de compra y mercado.

HDSL se verá sustituido a relativo corto plazo por sistemas HDSL-2 en regiones ANSI y por sistemas SHDSL en regiones que siguen normativa ETSI.

G.991.2 - SHDSL

El sistema SHDSL (o su variante ANSI: HDSL-2) requiere un solo par y tiene mayor alcance que los sistemas HDSL monopar. Una de sus principales ventajas es su compatibilidad espectral con otros sistemas DSL, particularmente ADSL, con los que pueden coexistir en el mismo mazo de pares. Además, existe una normativa sobre su implementación, con lo que los equipos de abonado y central pueden ser de distintos suministradores.

Por todo ello, se prevé que en el año 2005 todas las ventas de HDSL habrán sido reemplazadas por SHDSL y HDSL-2. La especificación de estas tecnologías se ha desarrollado en tres frentes de normalización, dando lugar a los tres estándares siguientes, ANSI: T1E1.4/2001-174, para Norteamérica, ETSI TS 101524, para Europa, ITU-T (G.991.2), para todo el mundo,

[2]POTS: Plain Old Telephone Service.

Figura 6.2: Red de Acceso SHDSL

aunque nosotros nos centraremos únicamente en el G.991.2.

Es decir, el SHDSL está diseñado para el transporte de datos de forma simétrica, a regímenes que se adaptan a las características del canal y que van desde 192 Kbit/s hasta 2,3 Mbit/s, con una granularidad de 8 kb/s, con opción multipar (1 a 4), que permite multiplicar por M alcance, tasa, etc., por ejemplo desde 384 Kbit/s hasta 6 Mbit/s sobre dos pares.

Utiliza 8 kb/s para alineamiento, CRC y OAM, manteniendo una BER de 10E-7 y un alcance de 1.544 Mbps/ 12 km.

El código de línea utilizado es TC-PAM (Trellis Coded Pulse Amplitude Modulation), utilizando 16 niveles en línea (4B1H) (3 bits a 16 niveles), lo que le reporta menor diafonía, menor latencia y una implementación más simple. Además, la señal se conforma en frecuencia para mejorar la compatibilidad espectral respecto a otros sistemas que compartan el mismo mazo.

Mientras las aplicaciones de HDSL se limitan al transporte de servicios de Múltiplex por División en el Tiempo (TDM), desde un principio SHDSL está siendo utilizado para transportar cargas tanto TDM como ATM así como accesos BRI. Existen también repetidores opcionales para aumentar el alcance de estos sistemas de línea. El volumen de mercado para el 2004 de esta tecnología (considerando que está empezando a desplegarse en el 2002) será superior a los 1.000 millones de euros.

6.1.3. G.992 - Transceptores de línea de abonado digital asimétrica, con y sin divisores

G.992.1 - Transceptores de línea de abonado digital asimétrica (ADSL)

También conocido como **G.dmt**, es el sistema más desplegado en la actualidad, con previsiones de 32 millones de abonados a finales del 2002; llegando a 90 millones en el 2005. En la Unión Europea, a finales de 2001, destacaban países como Alemania (2 millones de líneas), Francia (750.000 líneas), España (500.000 líneas) y Holanda (500.000 líneas), según la firma

IDC. La misma firma estima que para el 2005 se sobrepasarán los 35 millones de líneas ADSL en el conjunto de los actuales miembros de la UE. Se trata de un sistema de gran popularidad debido a su comercialización en el segmento residencial (en EE.UU. un 77 % de los abonados ADSL son residenciales).

El nombre ADSL fue acuñado por Bellcore (actualmente, Telcordia) en 1989. Es importante situarse en esta fecha, en la que se estaba definiendo la non-nata Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA), para explicarse algunas de las características del ADSL. Así, en 1989 el ITU-T (por entonces, el CCITT) escoge ATM como tecnología de transporte para la RDSI-BA y define salomónicamente la longitud de la celda.

Por entonces, los operadores de telefonía establecidos apuntaban a introducirse en el servicio de televisión, es la época de los éxitos y mayores despliegues de los operadores de cable en EE.UU. Las operadoras tradicionales vieron en ADSL la solución para revalorizar su planta de cobre instalada ofreciendo servicios de vídeo (*convertir el cobre en oro*). Este cúmulo de circunstancias condujo a considerar el empleo de ATM sobre ADSL como forma de establecer prioridades para los tráficos de tiempo real (vídeo, audio y voz) frente a los tráficos de datos, y además determinó los objetivos iniciales de capacidad (8 Mbit/s hacia el abonado y 640 Kbit/s en sentido inverso), que hacían posible la transmisión de más de un canal de TV comprimido hacia el abonado.

Las expectativas puestas por los operadores en los servicios de vídeo para el despliegue de ADSL no se cumplieron. Sin embargo, pronto aparecería una aplicación que actuaría como verdadero catalizador en el despliegue de esta tecnología: el acceso a Internet. En este nuevo escenario se cuestionó, entre otros por Bellcore, la utilización de ATM, proponiéndose el transporte directo de tramas Ethernet sobre ADSL. Pero en octubre de 1996 el Joint Procurement Consortium, formado por las operadoras Ameritech, BellSouth, Pacific Bell y SBC Communications, decidió optar por una solución ADSL basada en transporte ATM, marcando la tendencia definitiva.

Una característica importante de ADSL es la compartición del espectro disponible en el par telefónico con el servicio telefónico (o con el servicio RDSI), permitiendo el acceso simultáneo a la red telefónica y a Internet, utilizando modulación MDT. Esto se logra mediante el empleo de un **splitter** (filtro separador de bandas) en casa del abonado.

El filtro separador se instalaba en un PTR especial, que tiene dos salidas, una dedicada para el módem ADSL y otra conexión a la instalación telefónica del abonado, con lo cual no era necesario el uso de los conocidos microfiltros.

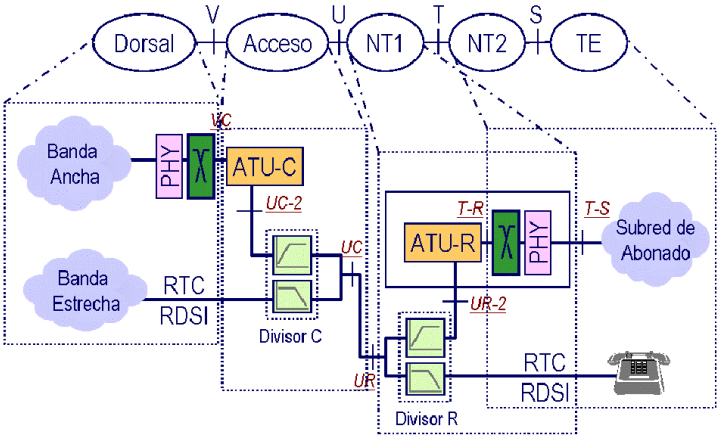

Figura 6.3: G.992.1: Modelo de referencia ADSL con splitters

La simultaneidad de la voz y los datos, unida a las considerables tasas de bit proporcionadas, hace de ADSL una técnica muy atractiva. Gracias a ella se puede disponer de un acceso permanente a Internet, con tarifa plana, y sin necesidad de contratar una línea adicional ni de cambiar los aparatos telefónicos. Todo ello, sin duda, constituye un factor diferencial frente a las técnicas HDSL y SHDSL vistas anteriormente.

G.992.2 - Transceptores de línea de abonado digital asimétrica (ADSL) sin divisores

Conocido como **G.lite**, sigue el modelo de G.992.1 pero eliminado la instalación de filtros separadores en el hogar, como recoge la arquitectura de referencia de la figura 6.4. La finalidad del filtro paso bajo es eliminar la banda inferior de la señal ADSL para que no interfiera con la voz y eliminar la banda superior de los tonos de señalización, para que no interfiera con la señal ADSL.

Al eliminarlo se ahorra en la instalación, pues no se necesita operario y se instala como un módem de banda vocal. La contrapartida es que sin filtro aumenta la posibilidad de interferencias reduciendo el número de portadoras, y por lo tanto se consigue una menor tasa binaria.

El filtro paso alto suele ir incorporado en el propio módem ADSL, que incorpora gestión de potencia, permaneciendo en un estado latente o de reposo cuando el usuario no transmite ni recibe y con capacidad de activación rápida, en caso de comenzar a utilizarse y opcionalmente se pueden instalar pequeños filtros paso bajo en cada roseta donde se conecte un terminal

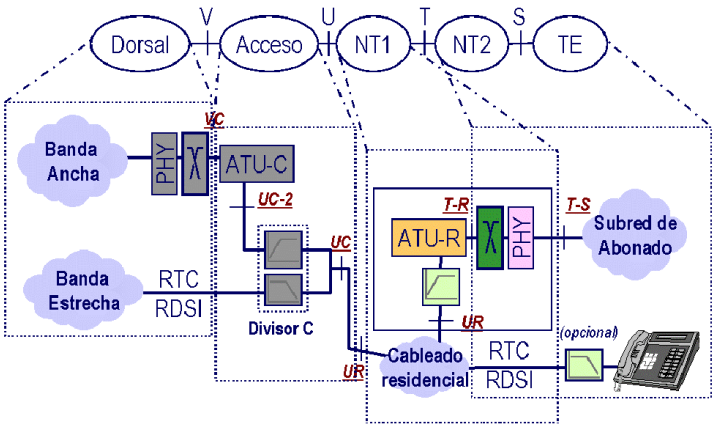

Figura 6.4: G.992.2: Modelo de referencia ADSL sin splitters

analógico o RDSI, los denominados microfiltros.

Tenemos 3 circuitos portadores en ADSL:

- Canal simplex ascendente.
- Canal simplex descendente.
- Canal dúplex analógico en banda base.

Donde debemos tener en cuenta que existe una tara de línea ADSL para alineación de trama, control de errores, operaciones y mantenimiento, que lastran la capacidad teórica del acceso, recogida en la tabla 6.2.

	Up (Max)	**Down (Max)**
G.992.1	640 Kb/s	6,144 Mb/s
G.992.2	512 Kb/s	1,544 Mb/s

Tabla 6.2: Capacidad sobre el par ADSL

Módem ADSL

Es interesante estudiar también la instalación de estos sistemas desde el punto de vista físico. El sistema consta de un módem o terminal de red en las dependencias del usuario y de un equipo que agrupa los correspondientes módems o terminales de línea en la central. Concretamente:

- módem ADSL de Abonado (ADSL Terminal Unit-Remote, ATU-R).

- módem ADSL de Central (ADSL Terminal Unit-Central Office, ATU-C).

Actualmente la práctica totalidad de las instalaciones se basan en el empleo de un multiplexor digital DSL, conocido como **DSLAM, Digital Subscriber Line Access Multiplexer**, desplegándose en escenarios como el de la figura 6.5.

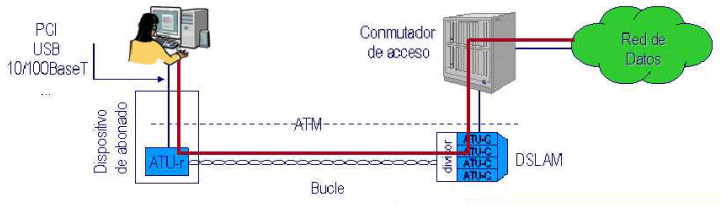

Figura 6.5: módem ADSL - DSLAM

El DSLAM es un equipo que agrupa gran número de tarjetas, cada una de las cuales consta de varios módems ATU-C, y que además concentra el tráfico de todos los enlaces ADSL hacia una red WAN. La integración de varios ATU-Cs conectados por uno o varios buses (backplane) en un montaje en bastidor de 19 pulgadas, es un factor fundamental que ha hecho posible el despliegue masivo del ADSL.

El módem ADSL es un dispositivo de capa física, similar en ATU-C y ATU-R que suele utilizar SDH para concentradores remotos y ATM para acceso indirecto, siendo esta la solución dominante en la industria, aunque existen otras posibles soluciones tecnológicas de menor impacto en el mercado, como el uso de Ethernet o Frame Relay.

Se prefiere el uso de ATM ya que es independiente del protocolo de red (IP, IPv6, IPC, ...), proporciona mecanismos de soporte de QoS, granularidad y escalabilidad en capacidad y es independiente del medio físico.

El nivel físico distingue en dos subniveles:

- **TC:** realizando labores de multiplexión, FEC, Entramado y OAM. Implementa multiplexación STM o ATM.
- **PMD:** encargándose de modulación (QAM, DMT, CAP, ...), iniciación del sistema, filtrado, aleatorización y mantenimiento del canal de control.

Una característica importante en estos sistemas es que el equipo de central incorpora funciones de multiplexión ATM. Ello, junto a las características del tráfico del principal servicio ofrecido en la actualidad, el acceso a

Internet de Alta Velocidad, permite obtener ganancia estadística mediante *sobre suscripción*, es decir, la suma de los tráficos *medios* ofrecidos a los abonados es superior al tráfico total que puede suministrar la red.

Por tanto es evidente que el ADSL también es un medio compartido, en este caso en la conexión que va hacia la red. En ambos casos, el comportamiento del sistema dependerá del grado de sobre suscripción existente en un isntante determinado en el DSLAM.

G.992.3 y 4 - Transceptores de línea de abonado digital asimétrica 2 (ADSL2) con y sin divisores

Manteniendo el mismo modelo de referencia con y sin divisores, permitiendo además un modo de funcionamiento sin POTS, lo que permite utilizar un mayor número de tonos (portadoras), así como un modo paquete además de ATM y SDH, introducen una serie de mejoras derivadas de la experiencia obtenida con los despliegues realizados:

- Mejoras en las pruebas de interoperabilidad, así como en señales y mensajes de iniciación, es decir, se implementa una negociación más robusta.
- Modo de bajo consumo, algo importante en los concentradores remotos.
- Posibilidad de usar todo el espectro para el transporte de la señal digital, desde 0 Hz, en aquellas aplicaciones en que no se requiera servicio telefónico simultáneo (all digital mode).
- Mejoras en prestaciones de alcance/caudal, logrando tasas máximas de 8 Mb/s de bajada y 800 Kb/s de subida, con incremento de longitud de bucle hasta 300 metros.
- Posibilidad de usar varios pares simultáneamente: 32 Mbit/s sobre 4 pares, 24 Mbit/s sobre 3 pares, 16 Mbit/s sobre 2 pares (inverse multiplex bonding).
- Capa de convergencia para transportar directamente Ethernet sobre ADSL.
- Soporte de multiplexión inversa G.998.X.

G.992.5 - Transceptores de línea de abonado digital asimétrica 2 de banda extendida (ADSL2+)

Nueva mejora del modelo que permitiendo doblar el número de tonos (256, al menos en el descendente) consigue obtener unas tasas de 16 Mb/s

en el enlace descendente y de 800 Kb/s mínimo en el ascendente, aunque no logra un aumento en el rango de cobertura.

6.1.4. G.993.1 - Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria (VDSL)

Extendiendo los límites de la tecnología del ADSL es posible utilizar un ancho de banda mayor sobre el par de cobre, hasta alcanzar los 11 MHz. Por supuesto, esto sólo es factible para alcances más reducidos que los vistos en ADSL.

Así, mientras el objetivo de alcance en ADSL era cubrir el área de servicio de la central, en VDSL las zonas geográficas cubiertas son mucho menores, tal como se representa en la figura 6.6. Por este motivo, la tecnología VDSL va acompañada de un amplio despliegue de fibra hasta los nodos desde los cuales se alcanza al abonado mediante tiradas de cobre muy cortas.

La batalla entre las técnicas de modulación DMT y CAP se ha vuelto a escenificar en VDSL. En el caso de DMT, se usan las mismas frecuencias y el mismo espaciado que en ADSL, lo que permite que un módem VDSL pueda comunicarse con un módem ADSL (a velocidades ADSL). Sin embargo, actualmente la técnica que predomina es una versión de CAP multiportadora, con dos o más subbandas por sentido, lo cual permite gestionar la utilización del ancho de banda en función del alcance y ruido de las líneas.

El VDSL, al igual que el ADSL, permite la coexistencia del servicio telefónico en el par (compatible con POTS y RDSI). Existen también versiones de VDSL simétricas, lo que permite su empleo, por ejemplo, para proporcionar accesos de alta velocidad a empresas.

VDSL tiene dos modos de operación:

- **Simétrico:** utilizado en servicios a empresas o entre centrales, ofreciendo unas tasas de 13 Mbit/s a 1 Km y de hasta 26 Mbit/s hasta 300 metros.

- **Asimétrico:** utilizado en servicio residencial, reutilizando el bucle RTC/RDSI-BE. Permite unas tasas de 13-26/2-3 Mbit/s a 1 Km y de hasta 52/2-3 Mbit/s a 300 metros.

6.1.5. G.993.2 - Transceptores de línea de abonado digital asimétrica de muy alta velocidad binaria 2 (VDSL2)

Existe una segunda versión, VDSL2, recogida en la recomendación G.993.2 que utiliza la banda hasta 30 MHz, para provisión de HDTV[3] (al menos tres canales simultáneos) consiguiendo un aumento del régimen binario a 100 Mbit/s en modo duplex. Presenta la posibilidad de sustituir ATM por un entramado Ethernet, logrando un aumento de eficiencia.

Su objetivo es lograr un alcance de 1,8 Km logrando la migración a este sistema desde ADSL2+ cuyas prestaciones dan un alcance de hasta 2,5 Km. Más allá de esa distancia, ADSL2+/RE-ADSL2+ es la mejor alternativa.

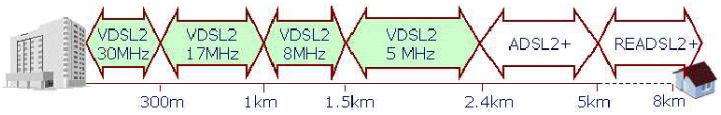

Figura 6.6: Alcance VDSL

El despliegue de fibra óptica que requiere VDSL, hasta distancias de pocos cientos de metros del abonado, dista mucho de ser habitual en las plantas exteriores actualmente desplegadas. Por otro lado, suponiendo que la fibra llega cerca del abonado (por ejemplo, hasta la fachada del edificio), cabe plantearse si merece la pena conservar el último tramo de cobre, o es preferible ya dar el salto final de fibra hasta el usuario.

Por compatibilidad con ADSL2+, utiliza una modulación DMT y no CAP. Para aumentar la capacidad utiliza receptores más sensibles, aumenta la potencia y el número de tonos, logrando:

- Mejorar en 2 dB el comportamiento de VDSL1, y utiliza mecanismos de corrección de errores más potentes, lo que proporciona unos 600 Kbit/s• MHz adicionales.
- Aumenta la potencia de transmisión en el canal descendente hasta los 20,5 dBm para los bucles largos.
- Para no aumentar la potencia en el canal ascendente, lo que empeoraría los problemas de telediafonía (FEXT), extiende la bandas ascendente, por debajo, desde los 138 KHz de VDSL1, hasta los 25 KHz. Con esto mejora el canal ascendente en los bucles largos.
- Pasa de los 512 tonos de ADSL2+ a 4096. La separación entre portadoras puede ser de 4,3125 KHz, compatible con ADSL2+ y que lleva

[3]HDTV: High Definition TV.

la banda hasta los 17,67 MHz, o bien de 8,624 KHz, lo que lleva la banda hasta el tope de los 30 MHz, lo que mejora el comportamiento en los bucles cortos.

El uso de estas técnicas produce una mejora conjunta del sistema, reflejada en la figura 6.7, donde se comprueba que en bucles cortos VDSL2 es mucho mejor que VDSL1, mientras que a partir de los 1200 metros, donde VDSL1 deja de ser útil, VDSL2 empieza a comportarse como ADSL2+.

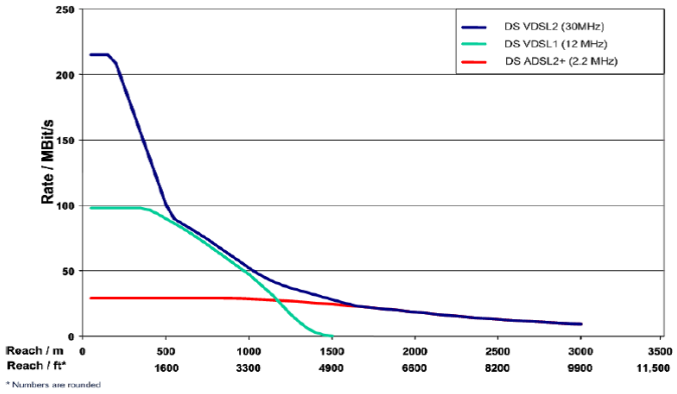

Figura 6.7: Comparativa VDSL2/VDSL/ADSL2+

Tal y como se recoge en la figura 6.8, donde las bandas ascendentes se muestran rayadas, la banda de VDSL2 se solapa con las del resto de tecnologías xDSL. Por eso, por compatibilidad con VDSL1 se utiliza su mismo plan de frecuencias, entre los 138 KHz y los 12 MHz, pudiendo deshabilitarse la banda entre 25 y 138 KHz.

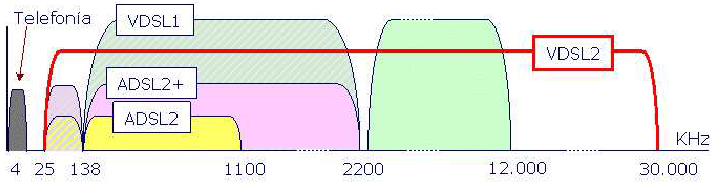

Figura 6.8: Plan de frecuencias VDSL2 comparado

Si no se armonizaran los planes de frecuencia, podrían coincidir en una misma banda la transmisión ascendente de un bucle con una tecnología y la descendente en otro adyacente con otra diferente. En el extremo de la central esto provocaría un aumento de la paradiafonía (NEXT).

Es necesario adaptar las distintas configuraciones de coexistencia y a los distintos países, así como los distintos servicios (simétricos o asimétricos), tal y como se recoge en la figura 6.9.

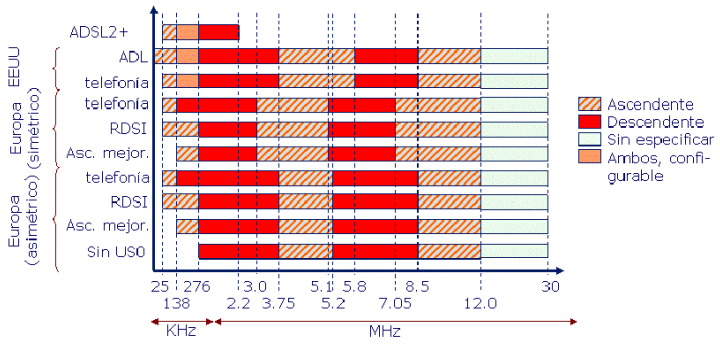

Figura 6.9: Armonización Plan de frecuencias VDSL2

Nótese como se superponen con sentidos coincidentes las bandas de VDSL2 y ADSL2. Hasta los 12 MHz el plan es el mismo que para VDSL1 por compatibilidad.

En VDSL2 es necesario definir distintos **perfiles de uso.** Los perfiles de uso limitan los parámetros de funcionamiento para implementaciones menos complejas adaptadas a las condiciones específicas del despliegue, como por ejemplo, DSLAM en central, remoto o edificio.

Los perfiles indican la frecuencia de la subportadora más alta para cada banda, su número y espaciado (que determinan la frecuencia máxima utilizada), la potencia máxima de transmisión y la utilización (o no) de la banda US0.

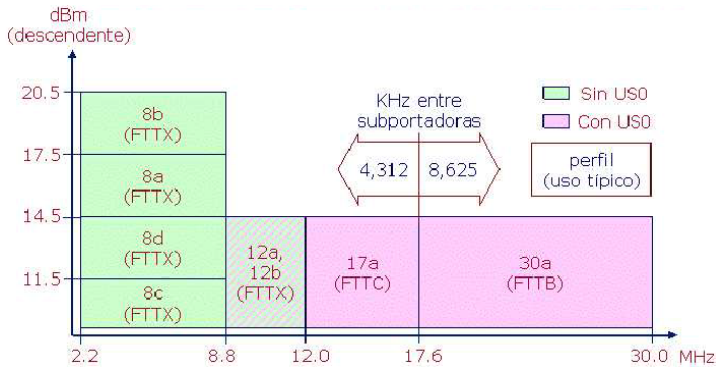

Figura 6.10: Perfiles VDSL2

Una implementación VDSL2 tiene al menos que soportar un perfil, y

debe seguir alguno de los planes de frecuencia anteriores, ya que es éste, y no el perfil quien se adapta al espectro del país, a la simetría de uso, y a la compatibilidad o no con el servicio telefónico básico o con RDSI.

La **arquitectura de referencia de VDSL2** es la misma que la de ADSL. El divisor en el domicilio del cliente puede sustituirse, como se hace en ADSL2+, por un filtro paso alto integrado en el dispositivo VDSL2 y, opcionalmente, utilizando un microfiltro en las tomas telefónicas, aunque se advierte que esta opción está expuesta a graves anomalías e interferencias, debido al mayor ancho de banda y mayor potencia utilizada frente a ADSL2+.

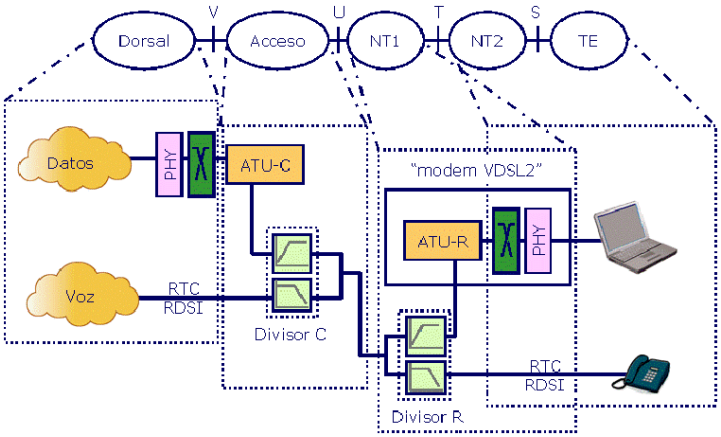

Figura 6.11: Arquitectura de Referencia VDSL2

La **instalación** de VDSL2, sobre todo a 30 MHz es más delicada, siendo necesaria la utilización de cableado de categoría Cat5e, entre el DSLAM y el banco de filtros, respetando el torcido de los pares en el conectorizado, como refleja la figura 6.12, donde en la figura izquierda se muestra un conector Cat3e donde no se respeta el torcido en el conectorizado y a la derecha un Cat5e donde sí se respeta en todo momento.

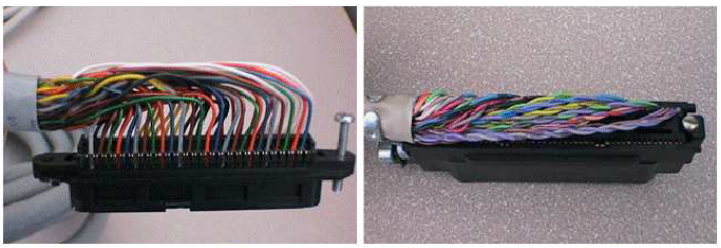

Figura 6.12: Instalación VDSL2

VDSL2 soporta el **modo paquete** en dos métodos:

- *ATM en el bucle de abonado:* necesitando una tara de entre el 10 y el 30 %, pero que permite la coexistencia del tráfico de datos y el tráfico sensible al retardo (televisión y telefonía sobre IP).
- *Modo paquete opcional:* con un encapsulado de 46/65 octetos, basado en el IEEE 802.3ah, fragmenta las tramas de usuario en bloques de 64 octetos y le añade otro de sincronismo. Incorpora un mecanismo que permite al tráfico de alta prioridad interrumpir la transmisión de los fragmentos de baja prioridad.

Presenta además algunas características adicionales, algunas de ellas ya presentes en ADSL2+:

- Mejora el procedimiento de inicio y aprendizaje de los canceladores de eco y los ecualizadores.
- Control avanzado de potencia en el canal ascendente, para eliminar problemas de telediafonía (FEXT).
- Proporciona un modo de diagnóstico robusto, capaz de monitorizar el bucle aunque éste resulte inutilizable para el servicio.
- Soporte de interfaces ATM, PTM y STM.
- Extiende el abanico de parámetros de entrelazador y del codificador Reed-Solomon, mejorando las propiedades correctoras de errores.
- Reduce el tiempo de reconfiguración y aumenta la estabilidad de funcionamiento.
- No se descarta ningún tono para enviar datos, ya que se soportan todas las constelaciones entre 1 y 15 bits.
- Aumenta la ortogonalidad entre la señal recibida y el eco de la transmitida añadiendo un prefijo y un sufijo cíclicos que eliminan la interferencia entre símbolos.

6.1.6. Comparativa tecnologías xDSL

En la 6.13 se muestran los anchos de banda requeridos por cada tecnología xDSL, así como los regímenes binarios que proporcionan. En la tabla 6.3 se muestra la evolución de las velocidades obtenidas por las técnicas xDSL en los últimos años, en comparación con el crecimiento de las velocidades de los módem en banda vocal (300-3400Hz).

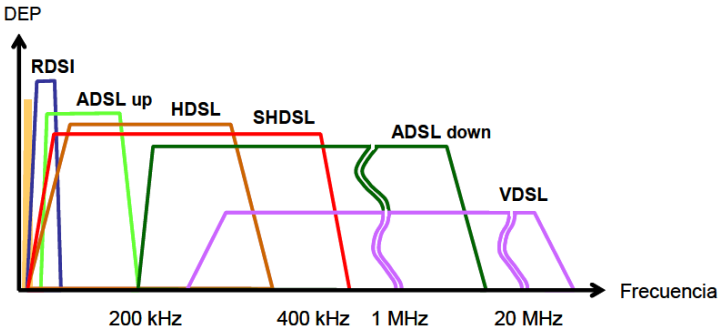

Figura 6.13: Espectros Comparados Tecnologías xDSL

Acrónimo	Ancho de Banda	Tasa Binaria
POTS	300 Hz - 3.4 KHz	56 Kbit/s
RDSI	0 - 50 KHz	144 Kbit/s
HDSL	0 - 292 KHz	2 Mbit/s
SHDSL	0 - 386 KHz	2 Mbit/s
ADSL up	25 KHz - 138 KHz	640 Kbit/s
ADSL down	138 - 1.1 MHz	8 Mbit/s
VDSL	200 KHz - 20 MHz	52 Mbit/s

Tabla 6.3: Velocidades Tecnologías xDSL

6.1.7. Regulación y mercado

Las redes de acceso sobre cableado existente telefónico tienen como principal ventaja su facilidad de despliegue, pero su capacidad está limitada por las características de los medios de transmisión empleados. La tecnología mejor situada para ofrecer todos los servicios de forma integrada es la familia de tecnologías xDSL, por lo que su despliegue ha tenido un alto impacto en las infraestructuras de red.

Las redes que despliegan fibra óptica hasta el usuario, o hasta un punto cercano al mismo, ofrecen capacidad suficiente para todos los servicios. Su principal inconveniente radica en el coste de la planta exterior, donde se requiere realizar inversiones significativas para llegar a los abonados.

Actualmente, el coste de la planta HFC, que estudiaremos en la próxima sección, supone un buen compromiso, mientras que FTTH[4] es, de momento, una solución cara, que no se ha extendido en el mercado residencial. *¿Para qué hacerlo si el usuario obtiene un servicio suficiente con tecnologías xDSL?*

[4]FTTH: Fiber To The Home.

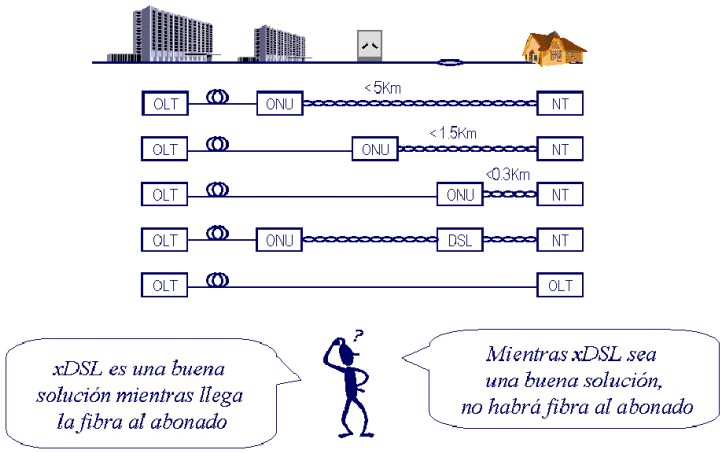

Figura 6.14: Evolución en la red

Como cabría esperar, la tecnología ADSL es principalmente una tecnología de operadores establecidos. La planta exterior de pares de cobre pertenece en su inmensa mayoría a los primeros operadores, que la han ido desplegando desde la invención del teléfono en 1876. Este hecho constituye una posición de ventaja competitiva frente a cualquier nuevo operador: el operador establecido, que posee el par (la conexión al usuario), parte con ventaja en cualquier escenario de libre competencia. Es un hecho que se inscribe dentro del concepto, muy contestado, de *monopolio natural*.

La liberación de las telecomunicaciones, comenzada en EE.UU. en 1986 con el Communication Act, y seguida en el resto del mundo con similares medidas que favorecen la competencia, ha llevado al concepto de **Desagregación del Bucle de Abonado (Local Loop Unbundling).**

Su principio es muy sencillo: el operador establecido ha de ceder al nuevo operador la conexión a «su» abonado. El nuevo operador paga una cuota mensual por el mantenimiento del bucle al operador establecido: no podemos olvidar que el par desagregado sigue yendo en un cable con otros pares que pertenecen al operador establecido. Una de las hipótesis del ejercicio es que el par ya está amortizado, e incluso, ha sido subvencionado por los años de monopolio que normalmente ha disfrutado el operador establecido.

La desagregación del bucle es una de las acciones de la Comisión Europea, acordada en la cumbre de Lisboa de Diciembre de 2000, para:

- Favorecer la competencia en las redes de acceso.
- Incrementar la penetración de los servicios de banda ancha: acceso a Internet de Alta Velocidad, Multimedia, etc.

- Reducir el precio de los servicios avanzados de telecomunicación.

La Comisión recomienda tres alternativas de Desagregación de Bucle, aunque sólo obliga a regular la Desagregación completa. La idea, aunque sencilla, da origen a una reglamentación muy compleja. Un ejemplo es la OBA (Oferta de acceso al Bucle de Abonado) de España, donde se regulan las obligaciones y precios de los distintos servicios que el operador establecido debe procurar al nuevo operador:

- Cuota mensual (que suele ser una cantidad muy parecida a la que paga el usuario particular por su cuota de abono).
- Espacios que el operador establecido debe proporcionar en su edificio, así como el precio de su alquiler.
- Precios de los cableados desde el Repartidor Principal hasta la ubicación del nuevo operador.
- Número máximo de servicios de banda ancha que se pueden proporcionar en un mazo de 25 pares (para evitar problemas de diafonía).
- Medidas de seguridad de acceso al edificio, así como precio que el nuevo operador deberá abonar por acceder al mismo.

Las tres alternativas de desagregación de bucle son:

- **Acceso totalmente desagregado:** la operadora no propietaria del bucle accede directamente al bucle (en el Main Distribution Frame, MDF) con un equipo propio, que incluye el divisor de frecuencias, dando servicio a través de esos pares de cobre a sus clientes, pudiendo ofertar los mismos servicios que la operadora propietaria, voz y datos.
- **Acceso desagregado compartido:** el bucle de abonado se comparte por bandas, la baja es para el operador dominante y la otra del otro operador, que únicamente puede ofrecer servicio de datos.
- **Acceso indirecto:** el otro operador recibe del dominante o propietario un flujo de células ATM. El flujo que se le da a cada operador se identifica con un VPI/VCI concreto, lo cual es una gran ventaja que permite separar de forma clara la interfaz entre el dominante y las alternativas. Es el modo más utilizado en el mercado actual.

La posibilidad de tener pares controlados por operadores distintos del dominante tiene un impacto técnico en la ingeniería de red:

- **Limitación de potencia:** si en un bucle corto se transmite a una tasa alta, se inunda de FEXT al resto de pares, por lo que no puede aumentarse el alcance aumentando la potencia de transmisión.

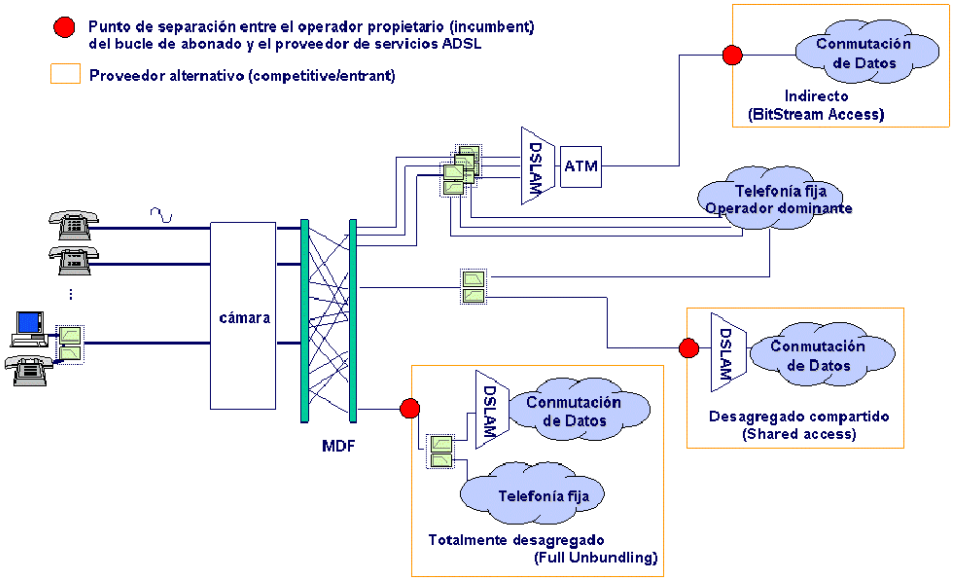

Figura 6.15: Modos desagregación bucle de abonado

- **Planes de frecuencia:** si no se homologa en todos los pares, se agrava la NEXT. En algunos casos, como en los proveedores IP interesa la asimetría, mientras que en el mercado empresarial interesa la simetría.

- **Duplexión:** el uso de Duplexión por División en el Tiempo (Time Division Duplex, TDD) está invalidada con acceso indirecto ya que es imposible mantener una referencia temporal única entre todos los operadores, por lo que la Duplexión por División en Frecuencia (Frequency Division Duplex, FDD) aparece como la única opción valida.

El 26 de Marzo de 1.999 se aprobó, por medio de una Orden Ministerial del Ministerio de Fomento, publicada en el BOE del 10 de Abril de 1.999, ORDEN de 26 de Marzo de 1.999[5] por la que se establecen las condiciones para la provisión del acceso indirecto al bucle de abonado de la red pública telefónica fija.

Dicha orden ministerial establece la obligatoriedad de que el Operador dominante (Telefónica, Sociedad Anónima), disponga de los medios técnicos necesarios para la provisión del acceso indirecto al bucle de abonado, permitiendo el acceso de cualquier operador al bucle de abonado, permitiendo a su vez el acceso a cualquier servicio por el bucle así como al bucle mismo. Para ello:

[5] `http://www.boe.es/boe/dias/1999/04/10/pdfs/A13506-13513.pdf` y `http://www.boe.es/boe/dias/1999/04/10/pdfs/A13513-13515.pdf`.

- Fija los diferentes tipos de licencias preceptivas para la operación del servicio (Operadores autorizados).
- Fija los medios técnicos necesarios (conexiones ATM y elementos terminadores en los puntos de acceso indirecto).
- Fija las velocidades de conexión de los operadores a los puntos de acceso indirecto (PAIs).
- Fija las modalidades de acceso (A, B, C y D) de los usuarios finales.
    - La modalidad A, proporciona un flujo binario máximo en sentido operador a usuario de 256 Kbits/segundo, y en sentido usuario operador de 128 Kbits/segundo.
    - La modalidad B, proporciona un flujo binario máximo en sentido operador a usuario de 512 Kbits/segundo, y en sentido usuario operador de 128 Kbits/segundo.
    - La modalidad C, proporciona un flujo binario máximo en sentido operador a usuario de 2 Mbits/segundo, y en sentido usuario operador de 300 Kbits/segundo.
- Establece la necesidad de un proceso de certificación técnica de los equipos de usuario (módems ADSL).
- Fija las tarifas de acceso e interconexión en el punto de acceso indirecto.
- Fija las fases para el despliegue del servicio (cobertura).
- Fija todas las demarcaciones geográficas ADSL del territorio nacional, en concreto 109.

El acceso a internet a través de un operador alternativo se ilustra en las figuras 6.16.

Los puntos de acceso al operador pueden ser remotos de forma que el operador remoto concentra todo el tráfico dirigido a un punto (o a varios puntos) para facilitarle las labores de conmutación y acceso.

Vemos como tenemos un VPI/VCI por operador (sólo un operador por abonado). A la salida de la central local tenemos un PAI (Punto de Acceso) por operador y demarcación, y tantos VPI/VCI como sean necesarios para dar servicio a todos los usuarios y operadores. En la tabla 6.4 recogemos la configuración básica de los operadores mayoritarios.

El encapsulado IP es elección del proveedor del servicio de internet (Internet Service Provider, ISP), como se recoge en la figura 6.17. El operador

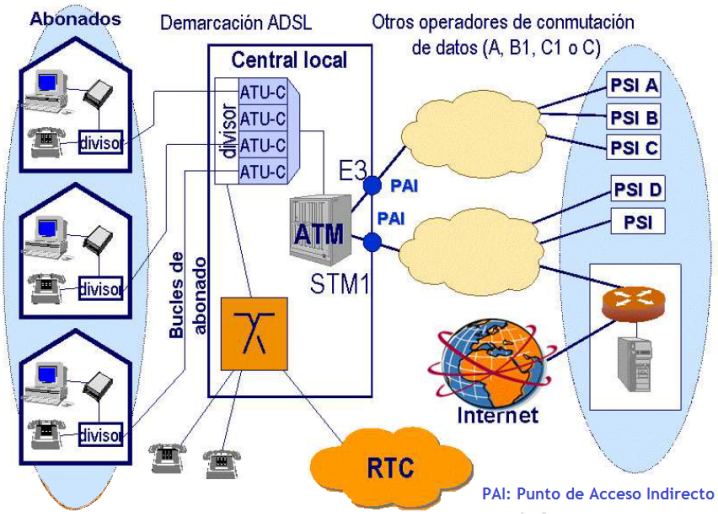

Figura 6.16: Acceso a Internet por ADSL

Proveedor	Protocolo	VPI/VCI	Encapsulación	DNS
EuskalTel	PPPoA	8/35	VC-MUX	[212.55.8.132] [212.55.8.133]
Jazztel	PPPoA	8/35	VC-MUX	[62.14.63.145] [62.14.2.1]
Jazztel	PPPoE	8/35	LLC	[87.216.1.65] [87.216.1.66]
Movistar	PPPoE	8/32	LLC/SNAP	[80.58.0.33] [80.58.32.97]
Orange	PPPoE	8/35	LLC/SNAP	[62.36.225.150] [62.37.228.20]
Ya.com	PPPoE	8/32	LLC/SNAP	[62.151.2.8] [62.151.4.21]
Ya.com	PPPoA	8/32	VC-MUX	[62.151.2.8] [62.151.8.100]

Tabla 6.4: Asignación VPI/VCI operadores

dominante sólo llega hasta la capa ATM.

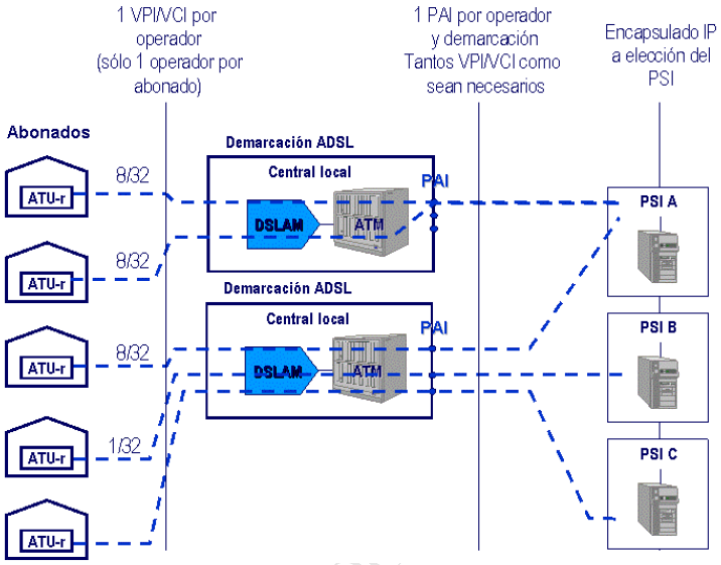

Figura 6.17: Acceso a Internet por ADSL

En el domicilio del abonado es habitual instalar un módem, o directamente un equipo que incorpore las dos funcionalidades (módem-router):

- **Módem:** el módem ADSL típicamente utiliza una interfaz PCI o USB para conectar a un único PC, como por ejemplo el modelo de US Robotics USR805637 recogido en la figura 6.18. Incorpora AAL5 para la salida hacia la central y la configuración del PC puede ser manual (IPoATM) o automática (PPPoATM).

Figura 6.18: Modem de abonado USB

- **Módem-Router:** suele incorporar una interfaz Ethernet/10BaseT, lo que facilita la configuración del PC, ya que incorpora un servidor DHCP preconfigurado y con opción NAT-P, lo que permite mantener

una LAN privada, asignando a los ordenadores IPs privadas y hacia la red usando IPs propias del operador (IPs públicas), como por ejemplo el modelo Linksys WAG120N recogido en la figura 6.19. Por supuesto es imprescindible la inclusión del sistema módem ADSL, lo que explica las dos torres de protocolos de la figura 6.19.

Figura 6.19: Router de abonado

En el acceso residencial a internet por ADSL existen dos arquitecturas de protocolos predominantes, recogidos en la figura 6.20.

- **IPoATM:** encapsulado IP sobre ATM, recogido en la RFC 2684. Se realiza una configuración manual del abonado, al que se le proporcionan una IP pública, máscara y router por defecto fijas.
- **PPPoATM:** encapsulado IP sobre PPP sobre ATM, recogido en las RFCs 2364 y 2684. Soluciona la asignación de IP al abonado y la identificación del usuario mediante el uso de PPP.

Aunque es cierto que existen otras arquitecturas de referencia mucho menos extendidas, como PPPoEoA, PPPoEoATM, etc., todas recogidas en la torre de protocolos representada en la figura 6.20.

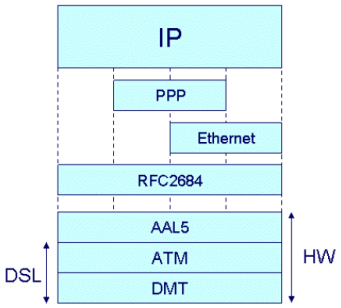

Figura 6.20: Arquitectura de Protocolos Acceso Internet ADSL

La figura 6.21 muestra el encapsulado correspondiente a las torres de protocolos utilizadas.

Para la provisión del servicio de acceso a red IP, se utiliza un único VC por usuario en el acceso ADSL, por lo que sólo se puede ofrecer una calidad

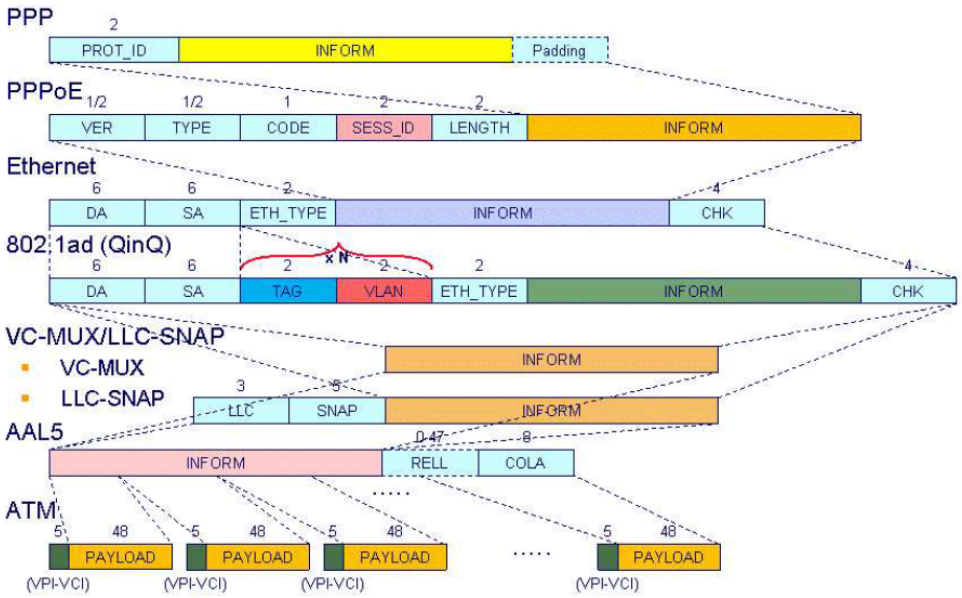

Figura 6.21: Encapsulados Acceso Internet ADSL

de servicio. Habrá por tanto, tantos VC como usuarios en el punto de acceso a internet (PAI). La sesión PPP debe terminarse en el servidor de acceso a la red del proveedor, para independizar la red de transporte IP de la de acceso, se transportan las sesiones PPP sobre túneles L2TP y se terminan en el/los servidor/es de acceso (Broadband Remote Access Server, BRAS.

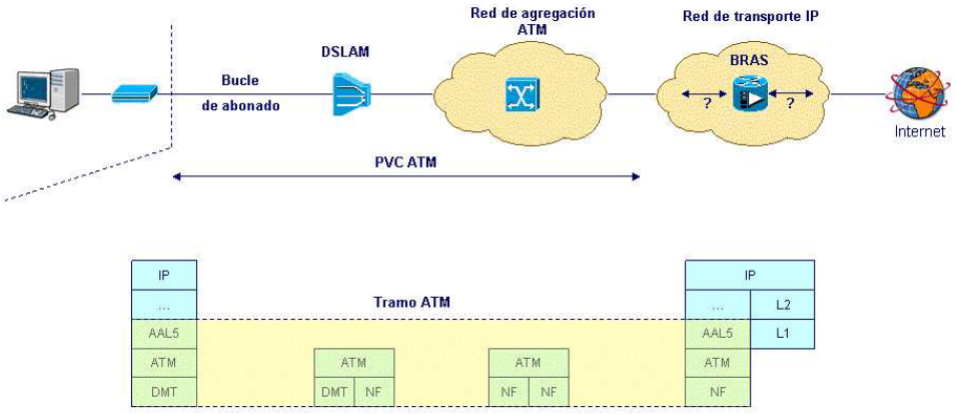

Figura 6.22: Red de Agregación ATM (I)

Por ejemplo, Telefónica vende su capacidad de transmisión a otros operadores, bajo el nombre comercial de GigADSL para el acceso indirecto por parte de otros operadores.

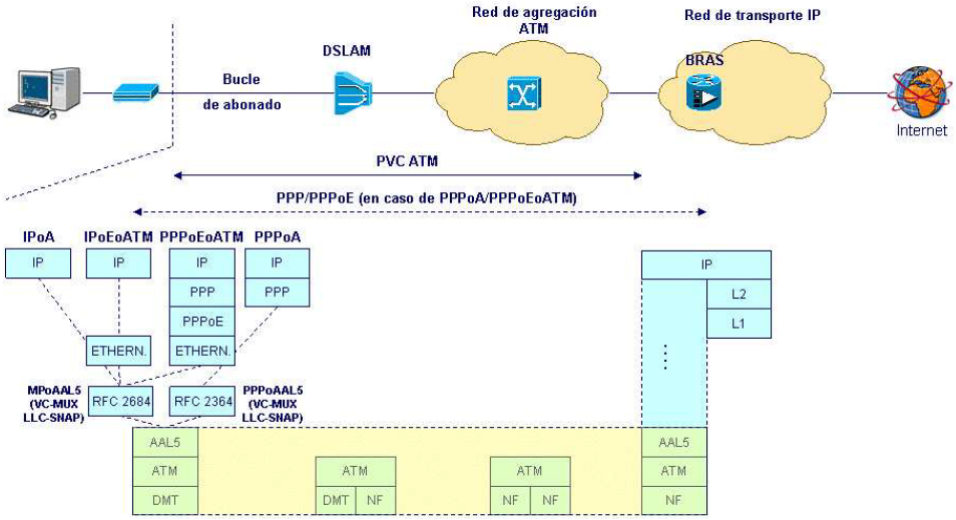

Figura 6.23: Red de Agregación ATM (II): Alternativas

Una vez estudiado el acceso, para clarificar los conceptos vamos a estudiar un ejemplo en el que se muestra un escenario para una petición http a un servidor de público de internet, como por ejemplo `http://www.google.es`. En la figura 6.24 se muestra la arquitectura de protocolos completa del escenario hasta el nivel IP.

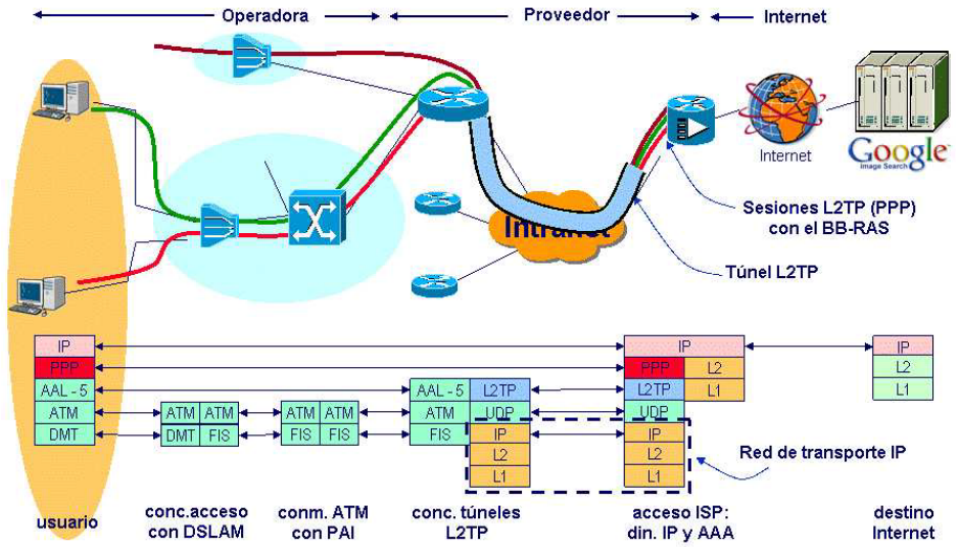

Figura 6.24: Ejemplo Acceso HTTP

Para cerrar el apartado, 6.25 a 6.27 recogemos unos ejemplos de diálo-

gos para el establecimiento de sesiones PPPoE y para la asignación de una dirección IP a un equipo mediante DHCP.

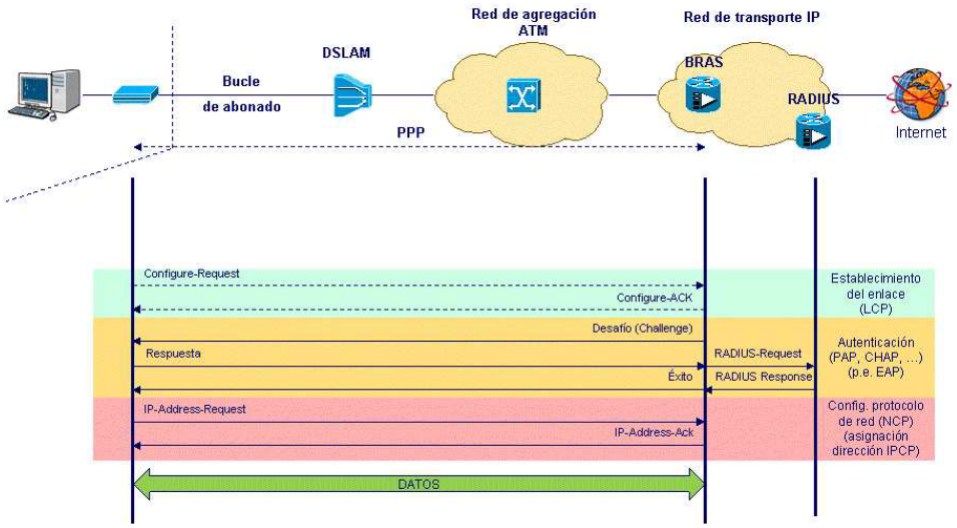

Figura 6.25: Ejemplo PPPoE: Establecimiento de Sesión (I)

6.2. Redes de Telecomunicación por cable

6.2.1. Introducción

Podemos *definir las redes de telecomunicación por cable* como infraestructuras de telecomunicación que, utilizando principalmente cables de comunicaciones, sean capaces de transportar cualquier tipo de señales de sonido, datos, imágenes o combinación de ellas, al público en el ámbito de una determinada demarcación territorial.

Los distintos servicios que se pueden proporcionar con estas redes son:

- Distribución de televisión y radio, distinguiendo la posibilidad de canales abiertos y canales de pago (servicio premium).
- Acceso a internet de alta velocidad/banda ancha.
- Telefonía integrada y alquiler de circuitos.

6.2.2. Aspectos de Mercado

El mercado de redes de cable en España está caracterizado por una regulación inicial, en la que se definió un operador por demarcación territorial

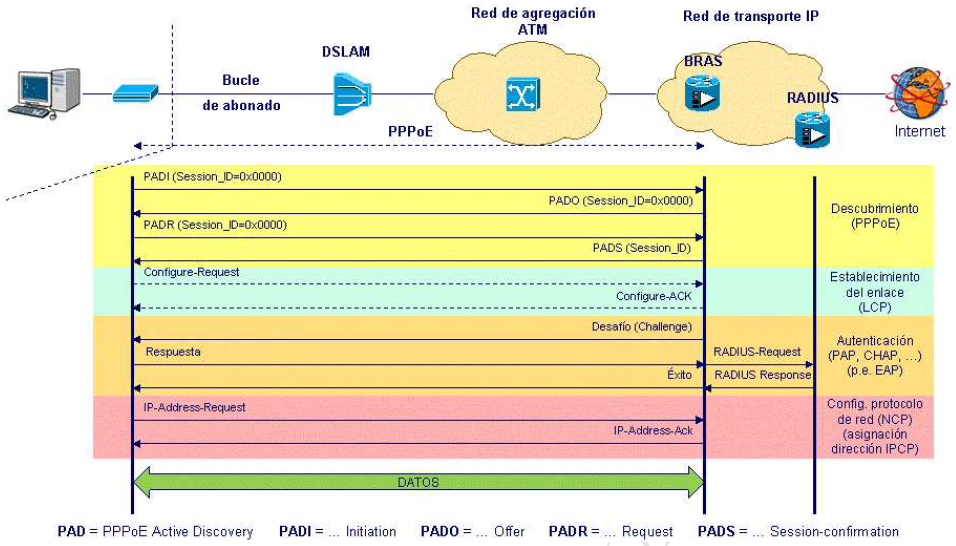

Figura 6.26: Ejemplo PPPoE: Establecimiento de Sesión (II)

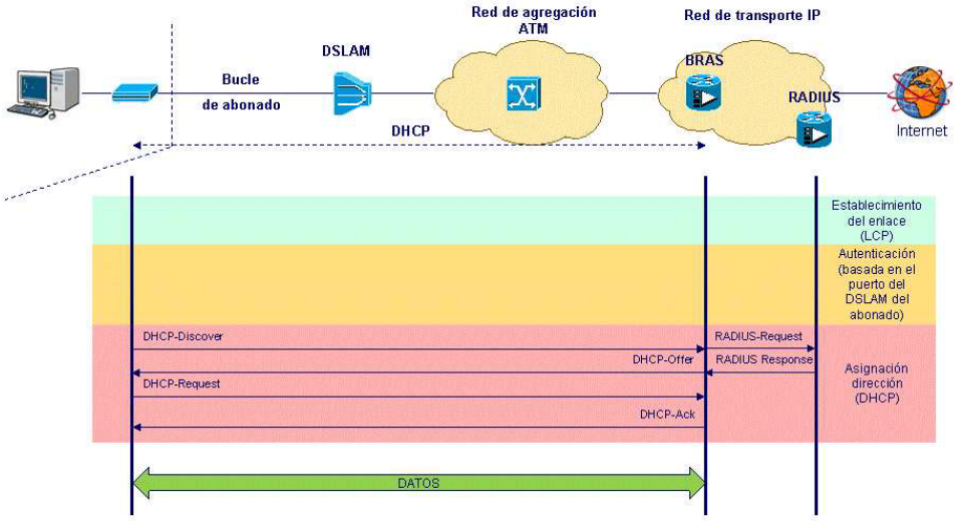

Figura 6.27: Ejemplo IPoE: DHCP

(Ono, Madritel, Menta, Able, Canarias Telecom, Supercable, Euskaltel, R, Telecable, Retecal y Tenaria) a la vez que se prohibió el acceso a este segmento a Telefónica de España S.A., operador mayoritario del país para evitar un posible monopolio.

Posteriormente, desde junio de 2005 el mercado se encuentra liberalizado, lo que provocó una concentración de operadores, situándose ONO[6] como operador mayoritario en el segmento y en menor medida AOC, que es una agrupación, no operadora, formada por Euskaltel, R y Telecable.

Figura 6.28: Operadores de Cable en España

Las redes de cable compiten en el mercado con otros servicios, como pueden ser TDT para distribución de televisión y con las tecnologías xDSL, principalmente con el Servicio Imagenio de Telefónica S.A. Realmente, los accesos por redes de cable y tecnologías xDSL son los dominadores del mercado, y su evolución se recoge en la figura 6.29

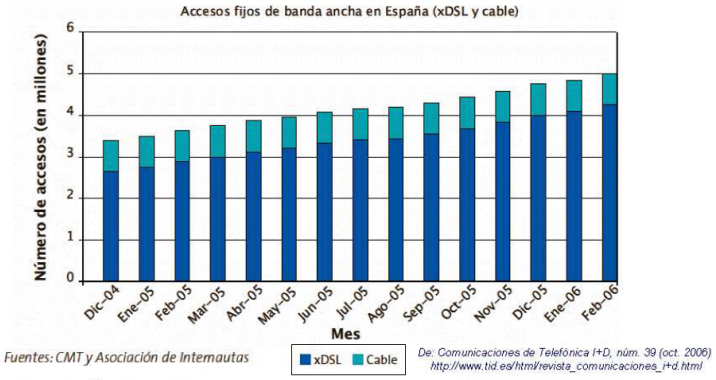

Figura 6.29: Situación Actual Cable frente a xDSL

En el resto del mundo, la evolución del mercado de redes de cable ha sido bastante dispar:

[6]El actual operador ONO proviene de la fusión de ONO, AunaCable, Madritel, Menta, Able, Canarias Telecom y Supercable más la compra de Retecal.

- **EE.UU.:** llega al 90 % de los hogares y tiene el 62 % de abonados (60 millones). Su regulación permite la integración de operadores de cable y telefonía.
- **Reino Unido:** desde 1991 ofrecen servicios de telefonía y TV sobre redes superpuestas. Es necesaria una doble licencia, para operación de red y operación de servicios. El servicio telefónico tiene una penetración del 9 %, mayor que la de TV.
- **Alemania:** operador público en origen. 60 % de penetración con 12 millones de abonados.
- **Francia:** como en Reino Unido, es necesaria una doble licencia, para operación de red y operación de servicios. Ha tenido una penetración muy baja.
- **Bélgica:** el más desarrollado de la Unión Europea, con un 88 % de penetración.

Las actuales redes HFC (Hybrid Fiber Coaxial) son una evolución de las redes de distribución de televisión por cable coaxial (CATV). Podemos considerar varios pasos en esta evolución.

Su origen se atribuye a Ed Parson de Astoria, Oregón, quien en 1950 distribuyó la señal que recibía por medio de ondas terrestres convencionales mediante un cable paralelo tendido de tejado a tejado, ubicando la antena en un sitio adecuado y amplificando la señal, para paliar los problemas de pobre recepción que sufría la comunidad. En el mismo año, Tarlton construyó el primer sistema utilizando cable coaxial que tendió utilizando los postes del tendido eléctrico previa adquisición de la correspondiente licencia municipal. Estas primeras aplicaciones se limitaron a resolver los problemas de deficiente recepción de las señales radioeléctricas. Un caso interesante fue la ciudad de Nueva York, donde la recepción estaba fuertemente afectada por las reflexiones producidas en los rascacielos. De estas primeras aplicaciones provienen las siglas CATV (Community Antenna Television).

Actualmente los sistemas CATV (cuya notación ha evolucionado a Cable TV) son sistemas de antena colectiva gestionadas por pequeñas compañías privadas (que habitualmente sólo proporcionan servicios de difusión de TV/-radio) para resolver la mala calidad de las señales de TV y Radio, debida a diversos motivos como imagen fantasma por propagación multitrayecto, pobre nivel de señal por atenuación atmosférica o topográfica, efecto nieve por ruido externo o interferencias cocanal.

Este sistema presenta limitaciones de base, como ser una arquitectura en árbol, sin canal de retorno y de alcance limitado, por lo que se utiliza

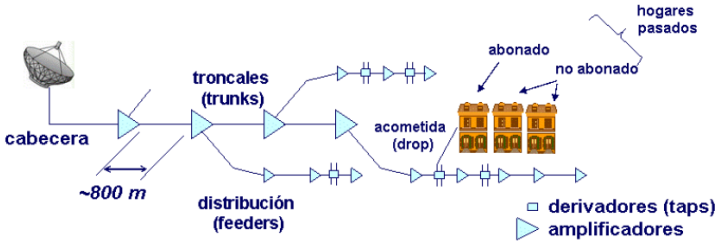

Figura 6.30: Arquitectura Sistemas CATV

como decimos para difusión de radio y TV en zonas muy localizadas.

La industria de la distribución de televisión por cable experimentó un fuerte impulso a mediados de los 70, cuando la tecnología de transporte de señal por satélite añadió canales a los disponibles vía la distribución por ondas terrestres. Aunque la tecnología de recepción del satélite en aquella época era muy cara, sus costes eran abordables al ser repartidos entre los abonados del sistema de cable. Mediante este método, la oferta de contenidos se enriqueció con canales de ámbito nacional e internacional, canales temáticos (noticias, deportes documentales) y canales de películas. Además se añadió la prestación de acceso condicional (sólo accesible a determinados usuarios) que permitió negocios con canales de suscripción (Pay TV) o de pago por visión (Pay Per View, PPV), e incluso de compra impulsiva (Impulse Pay per view, IPPV) requiriendo estos últimos algún tipo de señalización hacia el proveedor, que se hacía por la red telefónica.

A mediados de los 90, da comienzo una nueva etapa en la evolución de las redes de cable, por la introducción de la televisión digital. Con ello se consigue multiplicar el número de canales que pueden transportarse en el ancho de banda del sistema, proporcionando mayor calidad de imagen y sonido, así como nuevas facilidades de interactividad, evolucionando hasta las **redes híbridas de fibra y coaxial (HFC, Hybrid Fiber Coax)** desplegadas en la actualidad, que han sido posibles gracias al abaratamiento de la fibra óptica, lo que ha permitido la posibilidad de servicios interactivos y por supuesto, la sustitución del coaxial por fibra hasta donde convenga.

6.2.3. Arquitectura de Red

La figura 6.31 recoge la arquitectura de red básica de una red híbrida de fibra y coaxial.

En ella distinguimos los siguientes elementos:

- **Cabecera de Red:** su principal función es combinar las distintas fuentes de programación, ubicándolas en los canales del espectro del

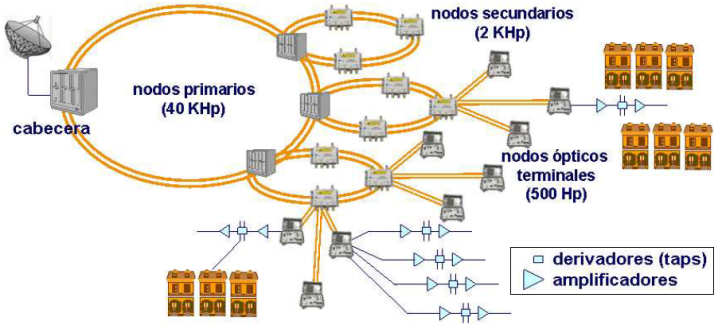

Figura 6.31: Arquitectura de Red HFC

cable, con la modulación de los receptores analógicos convencionales. Las posibles fuentes de programación son:

- Recepción de canales analógicos por satélite, cada uno de ellos ocupando el ancho de banda de un transpondedor de satélite (27 MHz). La captación de estas señales, moduladas en FM para mantener la calidad, se realiza con antenas parabólicas orientadas hacia el correspondiente satélite. Cada antena dispone en su foco de un amplificador de bajo ruido (Low Noise Block, LNB) que, además, traslada la señal del satélite a una banda de frecuencias más baja. Debido a las polarizaciones ortogonales usadas en la transmisión vía satélite, es posible que una misma antena alimente a dos LNB con distinta polarización. También es posible utilizar una antena motorizada como sistema redundante, que puede sustituir a cualquiera de las fijas en caso de fallo de algún elemento. La salida de los LNB se lleva a los receptores de satélite analógico, que producen a la salida señales de vídeo y audio en banda base.
- Otra fuente de programación son las emisiones terrestres. Con el fin de garantizar la calidad (realmente, conseguir que sea mejor que la que podría conseguir el usuario por captación directa), se utilizan antenas altamente direccionales y sintonizadas a cada canal, ubicadas en sitios desde donde se consiga visión directa con los emisores. Como sistema redundante se utiliza una antena de banda ancha y un receptor sintonizable, capaz de servir a cualquiera de los canales recibidos.
- Otras posibilidades de contribución de programas son: recepción desde estudio (en banda base, o con interfaz digital sin comprimir SDI); captación de señales terrestres; emisiones de satélite digitales (de 8 a 15 canales por transpondedor); o canales modulados en FM por microondas, sistemas de fibra o coaxiales. En cualquier

caso, se requiere el correspondiente demodulador/decodificador para la obtención de las señales de audio y vídeo en banda base.

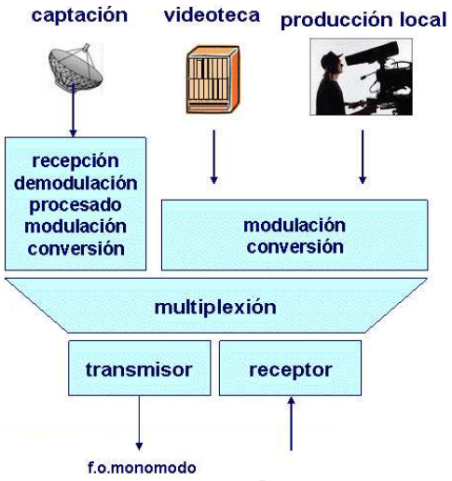

Figura 6.32: Funciones Cabecera de Red HFC

- **Red Troncal:** Normalmente, las redes troncales son redes ópticas con una topología a dos niveles, lo que permite la cobertura económica de una gran área. Distinguimos normalmente 3 segmentos de red troncal, la primaria, secundaria y terciaria.

  - **Red Troncal Primaria:** anillo de fibra que une la cabecera con los nodos primarios. Está formada por fibra redundante en ambos sentidos, permitiendo difusión en AM para TV analógica (a extinguir) y difusión en MPEG2 para TV digital. Es importante destacar que la cabecera, desde el punto de vista de la arquitectura es un nodo primario más.

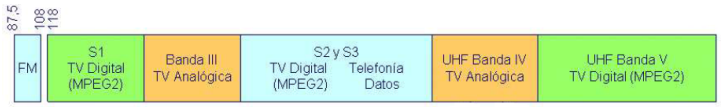

Figura 6.33: Espectro en Red Troncal

    - **Nodos Primarios:** las cabeceras alcanzan los nodos primarios, generalmente distantes de la misma y que atienden a áreas que sirven entre miles y decenas de miles de abonados[7], similar a los abonados de una central telefónica. Los nodos primarios utilizan redundancia de fibras y tienen un

[7] En redes de cable es habitual utilizar la nomenclatura de Hogares pasados, Hp, para referirse a abonados o potenciales abonados.

equipamiento similar al de la cabecera, con lo que tienen la posibilidad de insertar contenidos. Su mantenimiento es altamente complejo: sistemas de alimentación ininterrumpida, control de temperatura, etc.

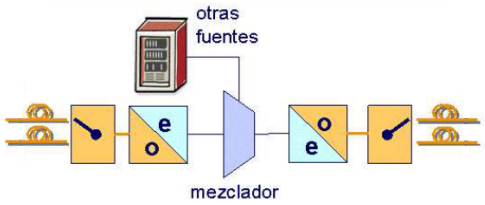

Figura 6.34: Equipamiento Nodo Primario

- **Red Troncal Secundaria:** segmento de red entre los nodos primarios y secundarios. Formada por anillos de fibra óptica redundante en ambos sentidos.
  - **Nodos Secundarios:** atienden a unos 200 hogares, presentando como principal diferencia respecto a los primarios en que son pasivos. Sus principales características son:
    - Utilizan divisores ópticos (típicamente 1 a 8).
    - Comparten el coste del láser monomodo que se ubica en el nodo primario.
    - Incluyen un repartidor de fibra.
    - Necesitan poco espacio, por lo que suelen ubicarse junto a uno de sus nodos terciarios, compartiendo espacio y gastos de obra civil.

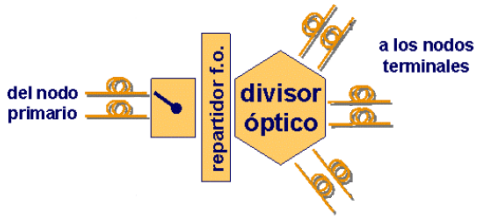

Figura 6.35: Equipamiento Nodo Secundario

- **Red Troncal Terciaria:** segmento de red desde el nodo secundario al terciario, óptico terminal. Formada por anillos de fibra óptica redundante en ambos sentidos.

Por su parte, las **Terminaciones de Red óptica (TRO/ONT)**, o nodos terciarios, son los equipamientos dónde se realiza la conversión a la señal eléctrica que alimenta los cables coaxiales. Las

TRO cubren áreas típicamente de 500 usuarios (Hp), aunque en sistemas con gran penetración de fibra el número se puede reducir a 100 e incluso a unas pocas decenas. Además se encargan de la telealimentación de equipos.

- **Red de Distribución:** desde el nodo óptico terciario (óptico terminal) al descodificador de abonado. La red de distribución HFC está basada en transporte mediante cable coaxial, siendo sus principales componentes los siguientes:

  - **Segmento Coaxial:** se ramifican 4 segmentos de coaxial por nodo terciario, atendiendo a 125 abonados por cada segmento de coaxial. Presenta una atenuación dependiente de la frecuencia por lo que es necesario implementar técnicas de amplificación y ecualización. Presenta límites físicos por no linealidades (productos de intermodulación) y por ruido (degradación de la SNR).

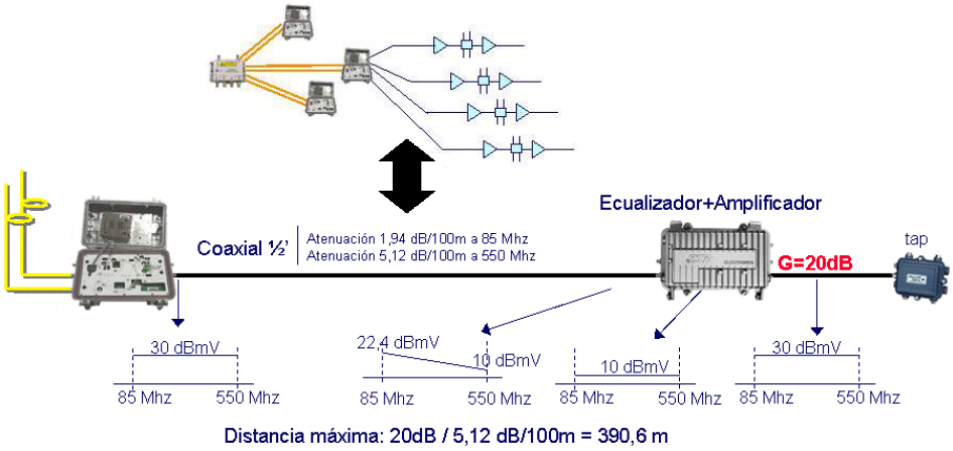

Figura 6.36: Red de distribución: Segmento Coaxial

Es un medio expuesto a fuentes de ruido, como taps no terminados, microroturas, equipos terminales con mala adaptación, tomas adicionales no terminadas, ...

  - **Amplificadores troncales en cascada y Extensores de Línea:** distintos tipos de amplificadores utilizados para compensar la atenuación en los tramos de coaxial.
  - **Taps:** que derivan parte de la energía que circula por el coaxial hacia las terminaciones donde se conectan las acometidas de usuario. Las derivaciones se presentan en configuraciones multiterminal de dos, cuatro u ocho salidas.

- **Acometida:** finalmente, segmento que va desde el tap al descodificador de abonado, que puede no estar presente si no hay TV digital ni

canales de pago. Se implementan distintos mecanismos de seguridad para evitar el pirateo de señal.

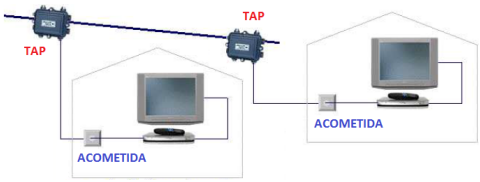

Figura 6.37: Acometida

Por último, para finalizar la arquitectura del sistema es importante destacar la presencia del **canal de retorno** en la red HFC, para servicios de datos y servicios interactivos (VOD [8] y PPV).

Los primeros sistemas para el canal de retorno utilizaban la red telefónica, ya fuese propia o de terceros, para posteriormente utilizar un sistema integrado en la propia red HFC, donde hay que distinguir la parte de retorno por el segmento coaxial y por el segmento óptico.

- *Canal de Retorno por Segmento Coaxial:* requiere amplificadores bidireccionales, utilizando la banda de 5 a 55 MHz que presenta el problema de estar muy afectada por ruido e interferencias (señales de telefonía móvil, señales de radio, la red eléctrica del usuario, motores eléctricos etc.). El segmento coaxial es un medio compartido por los abonados del servicio, que son servidos por el mismo coaxial, por lo que para servicios interactivos utilizan un mecanismo de acceso por sondeo y para el servicio de datos se constituye una red de área local normalizada.

- *Canal de Retorno por Segmento óptico:* el nodo terminal suma (no multiplexa) las señales de las cuatro ramas de coaxial y se envía mediante una fibra dedicada (con redundancia de caminos) hacia el nodo primario, en segunda ventana de transmisión óptica.

La capacidad nominal máxima en el canal de retorno es de 5 Mbit/s en la especificación DOCSIS[9] 1.0, de 10 Mbit/s en DOCSIS 1.1 y de 30 Mbit/s en DOCSIS 2.0. En la práctica sin embargo, el caudal efectivo suele está entorno a los 2 Mbit/s. Esto es debido a que el caudal efectivo depende de la modulación empleada y de la relación señal/ruido (CNR). Por otro lado, ha de tenerse en cuenta que muchos operadores con implantación nacional desde hace 4 ó 5 años, tienen equipos propietarios que no siguen el estándar

[8] VOD: Video On Demand y Pay Per View.
[9] Ver sección 6.2.6.

DOCSIS.

La capacidad nominal en el canal descendente es de 55,6 Mbit/s (para canales de 8 MHz), con un caudal efectivo de aproximadamente 30 Mbit/s.

A modo de ejemplo, en la tabla 6.5 se resumen las especificaciones tanto de canal descendente como de retorno de un fabricante:

Característica	**Canal Descendente**	**Canal de Retorno**
Capacidad Nominal	30,336 Mbit/s	2,56 Mbit/s
Capacidad Útil	23,9 Mbit/s	1,92 Mbit/s
Rango de Operación	88-800 MHz	5-40 MHz
Modulación	64-QAM	QPSK
Cifrado	DES (40 ó 56 bits)	DES (40 ó 56 bits)
BER	10-9 a 23 dB CNR	10-9 a 16 dB CNR

Tabla 6.5: Características de ejemplo de canales descendente y retorno

En el caso de usuarios empresariales, es posible proporcionar un ancho de banda fijo o garantizado (CBR), pero poco significativos en cuanto a cantidad.

En las próximas secciones estudiaremos la prestación de los servicios de televisión digital, telefonía y servicio de datos mediante redes de cable.

6.2.4. El servicio de televisión digital

Las redes HFC no sólo son adecuadas para este tipo de servicios, sino que además es la aplicación estrella. Ello se debe tanto al ancho de banda disponible, que típicamente permite 100 canales de TV digitales, como por la posibilidad de interactividad por el canal de retorno.

La interactividad normalmente se trata de funciones básicas, para las que se requiere poca capacidad en el canal ascendente (o incluso nula, ya que la interactividad puede proporcionarla el propio set-top box en modo carrusel, efectuando la selección el usuario mediante una especie de menú de teletexto).

Para servicios de pago (acceso condicional) de TV digital es necesario un set-top box que, además de las funciones de demodulación y decodificación, incorpore funciones específicas para acceso condicional.

La digitalización y compresión de señales de vídeo permite la difusión simultánea de un número de canales cada vez mayor. El servicio de Vídeo

Bajo Demanda puro, digital, para muchos abonados requiere sistemas en cabecera complejos y de gran capacidad.

Es necesario un equipamiento de cabecera para TV digital para generar el flujo MPEG2 que se distribuirá por la red.

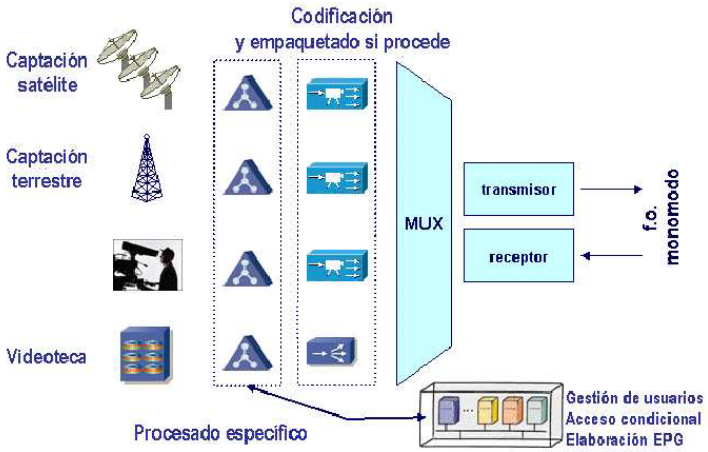

Figura 6.38: Cabecera TV Digital

El equipamiento de cabecera es costoso, por lo que es necesario un compromiso entre capacidad y costes para decidir su ubicación final. Normalmente se instala o bien como un sistema independiente o bien en un nodo primario.

Los componentes de cabecera identifican funciones a implementar, pero son independientes de las redes de transporte, aunque sí es lógico que el servicio establezca requisitos a la red.

Las funciones a realizar por una cabecera son las mismas para todos los sistemas de difusión de TV, ya sea para televisión digital con acceso vía satélite, televisión digital con acceso por redes de cable o para televisión digital con acceso EFM/DSL. En cualquiera de estos sistemas se pueden añadir elementos adicionales como canales locales, canal internet, correo electrónico, HDTV, inserción de anuncios, servicios de videoconferencia y sistemas de interacción con gestión de abonado y control de acceso.

La cabecera captará los distintos canales a transmitir y procederá a codificarlos y empaquetarlos en un flujo MPEG2. Puede ser necesario un procesamiento específico (demodulación, decodificado, selección de flujos de programa, extracción de información de programación, cifrado de flujos digitales, inserción de anuncios, ...) para unificar los contenidos.

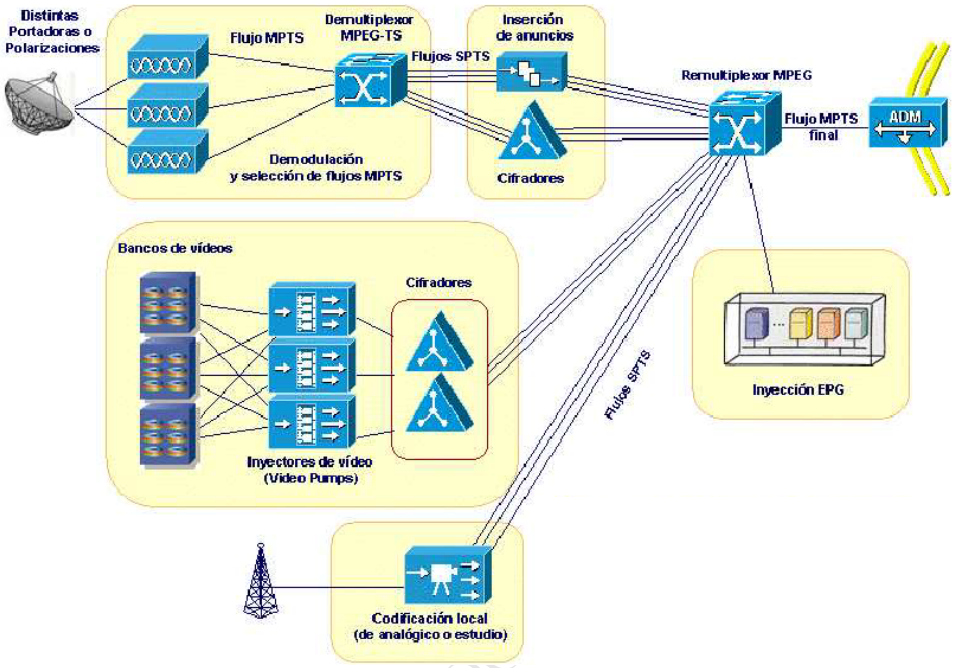

Figura 6.39: Equipamiento de Cabecera

Además es necesario realizar una gestión de usuarios para el acceso condicional así como para la elaboración de la EPG (Electronic Program Guide).

Se permite la distribución de contenidos en definición normal (SD: 200 Mb/s) y alta definición (HD: 1.5 Gb/s) así como de audio en calidad CD (1.5 Mb/s). Todo ello, tal y como decimos en un flujo de transporte MPEG2.

Sin entrar en una descripción exhaustiva, que sin duda cae fuera del field of view del texto, podemos decir que existen varios flujos transmitiéndose:

- *Flujo elemental de vídeo:* flujo que contiene el vídeo original de partida segmentado en paquetes que contienen secuencias o GOP (Group Of Images).

- *Flujo elemental empaquetado (PES, Packetized Elementary Stream):* añade marcas temporales y otra información de interés al flujo elemental de vídeo. Aún faltaría por añadir el audio, los datos y la indicación del programa al que pertenece. Un error en la cabecera destruye el paquete completo, produciendo la pérdida de toda la secuencia de imágenes.

- *Flujo de Transporte (TS, Transport Stream):* es una agrupación de

PES para transportar varios programas. Segmentados y opcionalmente protegidos (FEC) para su transmisión.

- *Tabla de Programación (PAT PSI):* se utiliza para determinar los PES que contienen información del programa deseado en ese flujo. Un TS puede llevar los PES de un sólo programa (SPTS). Hay PES con información adicional.

En la figura 6.40 se recoge la arquitectura de protocolos de MPEG2 (Moving Pictures Experts Group 2), que es la designación para un grupo de estándares de codificación de audio y vídeo acordado por MPEG (grupo de expertos en imágenes en movimiento), y publicados como estándar ISO 13818.

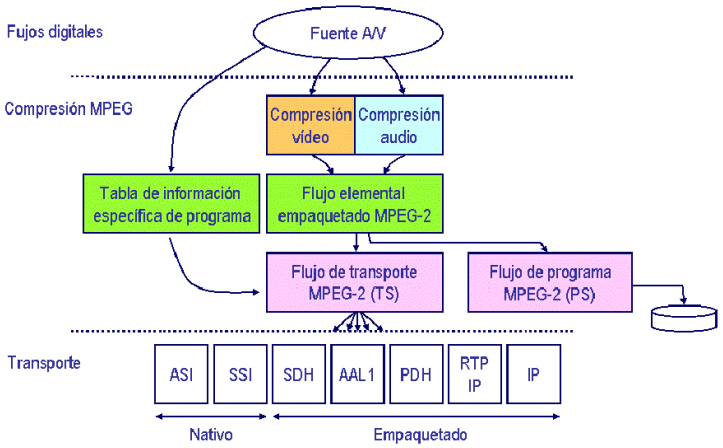

Figura 6.40: Arquitectura de Protocolos MPEG2

6.2.5. El servicio de telefonía

El servicio de telefonía o servicios de voz, también se puede integrar en las redes de cable debido a su bidireccionalidad. Requiere tiempo real y ancho de banda constante mientras dure la transmisión. La alimentación de dichos equipos puede ser local (en el domicilio del abonado), a partir de la red de distribución de energía, con batería de respaldo para asegurar el servicio, o remota a partir de los TRO.

No obstante, la mayoría de operadores de cable han optado por suministrar la telefonía a sus abonados mediante un par de cobre (gemelo o siamés) junto al cable coaxial. Se trata de operadores que desplegaron su red antes de que los fabricantes ofreciesen integración de voz, datos y TV sobre un mismo cable. La solución en este caso es el despliegue de una red telefónica

superpuesta a la red de cable, con la que comparte canalizaciones y armarios, equipando concentradores telefónicos junto a los TRO.

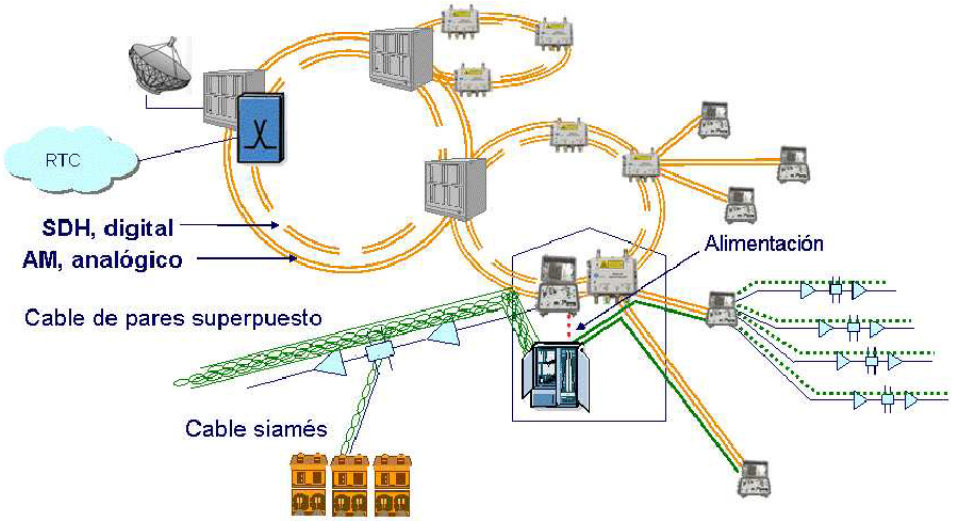

Figura 6.41: Servicio de Telefonía en redes HFC

Este tipo de soluciones tiene como ventaja el no compartir el espectro con el canal de retorno, así como disponer de la alimentación en el nodo de distribución.

Se implementa pues una red superpuesta de transporte SDH (en la fibra óptica) y de cable de pares (en las redes de distribución). Para ello son necesarios equipamientos adicionales en la arquitectura estudiada:

- *Cabecera:* incorpora una central de conmutación para conexión a otras redes (RTC, RDSI, ...).
- *Anillos:* en los anillos primarios se implementa una estructura STM-16 ó STM 4, mientras que en los secundarios se implementa una STM-4 ó STM-1.
- *Nodos primarios:* incorporan ADM (Add and Drop Multiplexers) del anillo primario y tantos ADM como anillos secundarios tenga la red troncal.
- *Nodos secundarios:* incorpora un ADM secundario y un concentrador remoto. La alimentación se extrae del terciario coubicado.
- *Nodos terciarios:* incorporan repartidores de pares.

6.2.6. El servicio de datos. DOCSIS.

Las redes HFC son adecuadas para los servicios de Internet y datos, adaptándose al crecimiento esperado de las aplicaciones punto a punto y multimedia, y con las limitaciones propias de la reparto del canal de retorno entre todos los usuarios que comparten el canal. Puede considerarse una solución comparable con otras alternativas, e incluso a veces más ventajosa. No en vano, en EE.UU., las redes de cable constituyen la tecnología de acceso con mayor número de usuarios a Internet a Alta Velocidad. La posibilidad de combinar el acceso a Internet con la transmisión de vídeo digital en aplicaciones ligadas al contenido de la TV digital, le confiere un potencial adicional.

Existen dos métodos de acceso al servicio de datos en redes HFC:

- **Módem ADSL:** utilizando la red de pares, en el caso explicado anteriormente de telefonía superpuesta. Como ventajas plantea el precio del equipo ADSL además que libera el canal de retorno.
- **Módem de Cable:** integrado en la red HFC. Simplifica el equipamiento de la red superpuesta, si existe. Utiliza el elevado ancho de banda potencial en el canal descendente y aprovecha el canal de retorno, preparado en cualquier caso para ofrecer servicios interactivos, permitiéndose incluso la telefonía sobre IP.

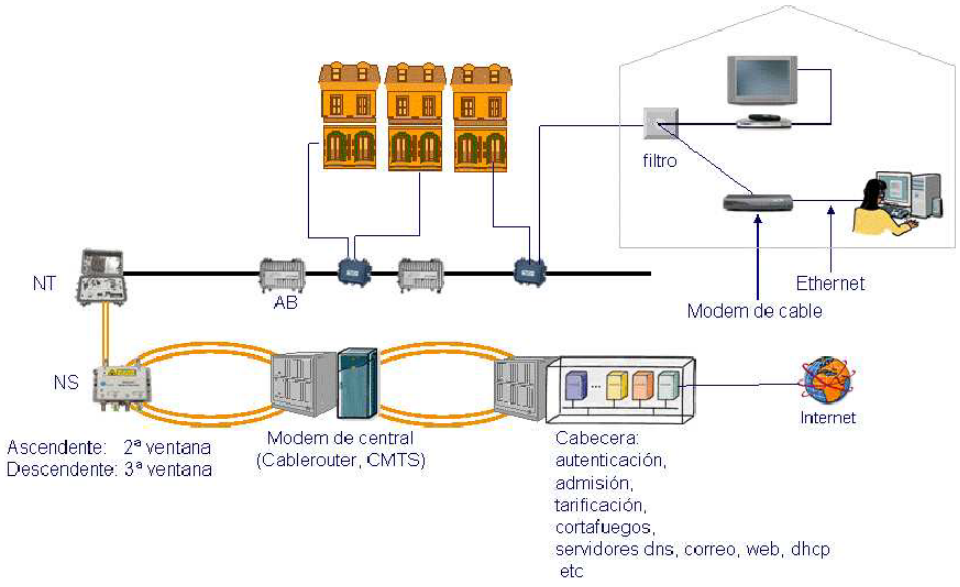

Figura 6.42: Servicio IP sobre redes HFC

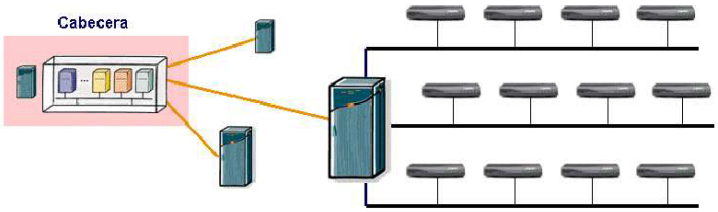

Figura 6.43: Servicio IP sobre redes HFC: Arquitectura Lógica

Los módems de central (CMTS, Cable módem Termination System), que podrían interpretarse como equivalentes al DSLAM en la tecnología DSL, instalados en los nodos terminales, se encargan del encaminamiento IP, cifrado y corrección de errores, gestión del espectro RF (garantía de QoS), siendo gestionable remotamente desde la cabecera.

Los módems de cable de los usuarios actúan como puente o repetidor, realizando monitorización RF, cifrado y corrección de errores y son gestionables remotamente. Se distribuyen en diferentes tecnologías: módems externos, PCI, USB, ...

El segmento coaxial es pues una red local de alta latencia, por lo que se necesita especificar sus capas físicas y MAC.

Tras el fracaso de la IEEE 802.14, el estándar **DOCSIS (Data over Cable Service Interface Specification**), desarrollado por el consorcio CableLabs, es quizá el más importante dentro del ámbito de las redes de cable. Prueba de ello es su aceptación como estándar por ITU, ETSI y SCTE. Hasta la fecha, se han definido tres versiones de DOCSIS:

- ITU-T J.112 (DOCSIS 1.1).
- ITU-T J.122 (DOCSIS 2.0).
- ITU-T J.222 (DOCSIS 3.0).

DOCSIS presenta la arquitectura de protocolos que se recoge en la figura 6.44.

La **capa física DOCSIS** presenta compatibilidad con el plan de frecuencias existente en el segmento coaxial, realizando una distribución asimétrica de la capacidad. Sus principales características se recogen en la tabla 6.6.

La **capa de enlace DOCSIS** emplea una mezcla de métodos de acceso determinísticos para las transmisiones ascendentes, específicamente TDMA para DOCSIS 1.0/1.1 y TDMA y S-CDMA para DOCSIS 2.0 y 3.0, con un

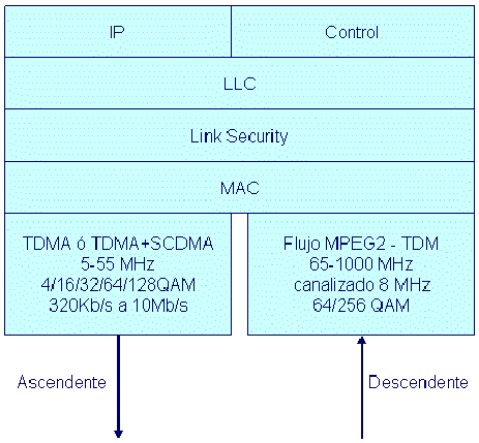

Figura 6.44: Arquitectura de Protocolos DOCSIS

		Canal	**Modulación**	**Tasa**
Ascendente	J.112	0,5 a 3,2 MHz	QPSK ó 16 QAM	9 Mb/s
	J.122	6,4 MHz	32/64/128 QAM	27 Mb/s
	J.222	6,4 MHz	32/64/128 QAM	n x 27 Mb/s
Descendente	J.112	6 u 8 MHz	64 ó 256 QAM	50 Mb/s
	J.122	6 u 8 MHz	64 ó 256 QAM	50 Mb/s
	J.222	n x (6 u 8) MHz	64 ó 256 QAM	n x 50 Mb/s

Tabla 6.6: Características Capa Física DOCSIS

uso limitado de la contienda para las solicitudes de ancho de banda.

En contraste con la métodos basados en acceso por contienda pura, como CSMA/CD utilizada en los sistemas más antiguos Ethernet (no hay contienda en Ethernet con los switches actuales), los sistemas DOCSIS experimentan pocas colisiones.

Para DOCSIS 1.1 y superiores, la capa MAC también incluye calidad de servicio (QoS) que ayudan a soportar de manera eficiente aplicaciones con requisitos específicos de tráfico, tales como baja latencia, como por ejemplo voz sobre IP.

DOCSIS 3.0 soporta unión de canales, lo que permite a un único abonado utilizar múltiples canales para flujos ascendentes y descendentes al mismo tiempo.

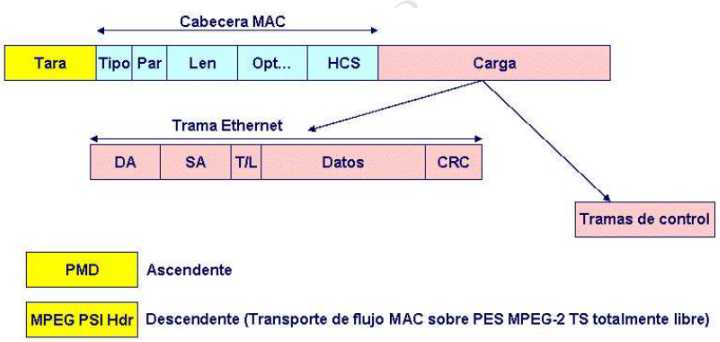

Figura 6.45: Trama Capa de Enlace DOCSIS

La transmisión en el medio compartido tiene lugar en unos intervalos de tiempo, denominados ranuras o minislots, por lo que es necesario mantener el sincronismo. Encontramos los siguientes tipos de ranuras:

- **Reservadas (Reserved Slots):** ranuras de tiempo asignadas a un módem específico, por lo que ningún otro módem puede utilizarlas. Son asignadas por el CMTS y sirve para garantizar una capacidad de tráfico mínima.
- **De Contienda (Contention Slots):** cualquier módem puede utilizarlas. La colisión se resuelve con un retroceso aleatorio.
- **De Alcance (Ranging Slots):** reservadas para gestión entre CMTs y módems de abonado. Implementan control de relojes, compensando los distintos retardos de propagación y control de potencia, compensando las diferentes atenuaciones, algo imprescindible para detectar colisiones.

Es el CMTS el encargado de informar a todos los módems, tanto de la estructura de la trama ascendente (patrón de ranuras) y de asignar las ranuras reservadas para cada módem.

El mecanismo de acceso al medio está por tanto basado en reserva (ranuras reservadas) con varios tipos de servicio posibles:

- **Asignación sin petición (Unsolicited Grants):** tipo tasa de bit constante. Se realiza una asignación periódica de permisos de transmisión de tamaño constante. El retardo y su variación es fácilmente controlable.
- **Sondeo para Tiempo Real (Real Time Polling):** se sondea al módem y si éste no necesita transmitir se reasignan sus permisos. Asigna un tipo tasa de bit variable sensible al retardo.
- **Tasa garantizada (Committed Information Rate):** el módem compite por el canal cada vez que transmite un datagrama. Se garantiza un ancho de banda mínimo aunque no el retardo.
- **Sin garantía (Tiered Best Effort):** se asignan flujos sin requisitos de retardo, variación de retardo o capacidad. Existen mecanismos de prioridades con hasta 8 niveles.

6.3. El acceso Ethernet (EFM)

Antes de comenzar con estos apartados finales, se recomienda al lector repasar los estándares Ethernet y VLAN 802.1q, recogidos en el anexo F.

6.3.1. IEEE: Ethernet para Operador (Carrier Ethernet) (I)

Carrier Ethernet es un término de marketing para denominar algunas extensiones técnicas implementadas sobre Ethernet, para permitir a los proveedores de red (denominados en EE.UU common carriers) proporcionar servicios de transporte Ethernet a sus clientes, utilizando así mismo Ethernet en sus redes.

En primer lugar, en este contexto hemos de distinguir entre la red del abonado y la red del operador. La red del operador es una red ethernet etiquetada, con restricciones de cobertura. El abonado interconecta sus redes locales a través del servicio ofrecido por el operador, utilizando:

- Múltiples puntos de acceso.
- Posiblemente, distintas VLAN del mismo abonado en cada punto de acceso.

- El tráfico se envía sólo a los puntos de acceso necesarios respetando las VLAN que el usuario defina.

En esta arquitectura inicial, **todos los equipos son puentes**, es decir equipos que trabajan en la capa de enlace, ya sean: puentes VLAN, puentes de operador, ...

Estudiaremos dos alternativas técnicas para estas implementaciones, en primer lugar la 802.1ad (QinQ) y más adelante estudiaremos la segunda opción 802.1ah (MinM).

802.1ad Apilado QinQ

IEEE 802.1ad es un estándar de red Ethernet informalmente conocido como IEEE 802.1QinQ y es una enmienda a la norma IEEE 802.1Q-1998. La técnica también se conoce como puentes de operador, VLAN apiladas o simplemente QinQ o Q-in-Q.

El apilado QinQ consiste en añadir una etiqueta 802.1q adicional respecto a la trama 802.1q, es decir añadimos dos etiquetas respecto a Ethernet convencional. Así logramos hacer una separación del espacio de etiquetado del cliente y del operador, como vemos en la figura 6.46.

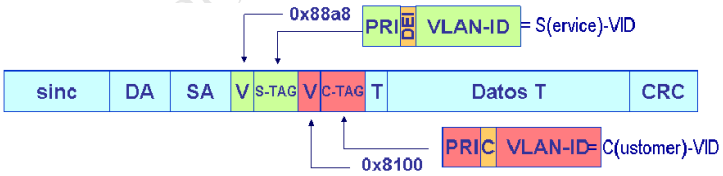

Figura 6.46: 802.1ad Apilado VLAN - QinQ

La etiqueta V del operador se fija al valor V=0x88a8, que identifica el servicio QinQ, mientras que la etiqueta del cliente es una etiqueta 802.1q convencional, es decir, con un valor de V=0x8100. Así, el cliente puede transportar sus 4094 VLAN encapsuladas en las 4094 VLAN del proveedor u operador, que se desentiende de las etiquetas del cliente.

La etiqueta S-TAG sustituye el CFI por el DEI (Discard Elegibility Bit), que permite multiplicar el rango de prioridades PRI para las tramas, pero que requiere un Ethertype diferente.

QinQ separa espacios de etiquetados VLAN y aumenta el número total de identificadores a 4094x4094, al disponer de un doble etiquetado: S(ervice)-VID/C(ustomer)-VID.

En el ejemplo de la figura 6.47 se representa un escenario con dos clientes, a los que el operador asigna unos identificadores S-VID=(qA,y qB). Por su parte, cada cliente dispone de dos redes locales virtuales etiquetadas como C-VID=(q1,q2), que por supuesto, pueden asignar las mismas etiquetas ya que son clientes independientes.

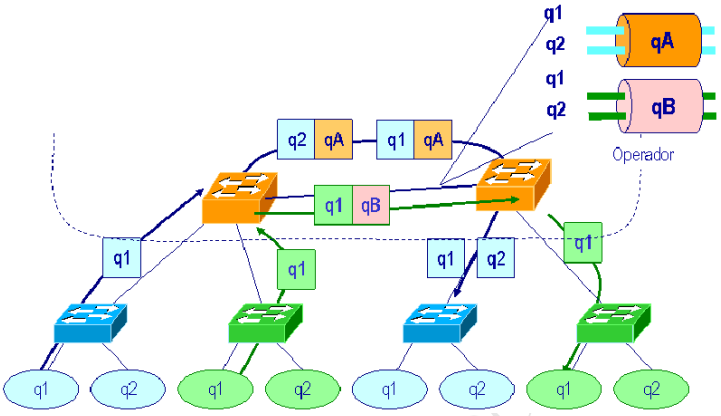

Figura 6.47: Ejemplo 802.1ad Apilado VLAN - QinQ

Estos primeros sistemas presentan una serie de limitaciones:

- *VLAN (802.1q)* permite únicamente 4094 VLAN posibles con hasta 8 niveles de calidad o prioridad.
- *QinQ (802.1ad)* permite 4094 VLAN por cliente, pero sólo 4094 clientes por proveedor, por lo tanto no son suficientes para un proveedor completo, aunque sí es suficiente para un área metropolitana. Agrandar el espacio VLAN-ID no es una solución posible. Además presenta una importante brecha de seguridad, pues las direcciones MAC del cliente son visibles en la red del operador y viceversa, y un cambio topológico en la red del cliente desencadena envío de BCPDU[10] globales.

La solución adoptada por el IETF consistió en modificar el núcleo de la red, utilizando IP/MPLS en lugar de utilizar Ethernet.

6.3.2. IETF: Marco Conceptual para Servicios Corporativos de Red Privada Virtual VPN

> *RFC 4026: To a certain extent, more than one term covers the same concept, and sometimes the same term covers more than one concept.*

[10]BPDU: Bridge Configuration Protocol Data Units.

El término **red privada virtual (Virtual Private Network, VPN)** se refiere a un conjunto de sitios de comunicación, donde:

1. se restringe la comunicación entre sitios fuera del conjunto y sitios dentro del conjunto, pero
2. la comunicación entre los sitios pertenecientes a la VPN se realiza sobre un infraestructura de red que es también utilizada por otros sitios que no pertenecen a dicha VPN.

El hecho de que la infraestructura de red sea compartido por múltiples VPNs (y posiblemente también por tráfico no VPN) es lo que distingue a una VPN de una red privada. Nos referiremos a esta infraestructura de red compartida como *Backbone VPN*.

En la RFC 4026 se realiza una clasificación básica de servicios VPN, que recogemos en la figura 6.48.

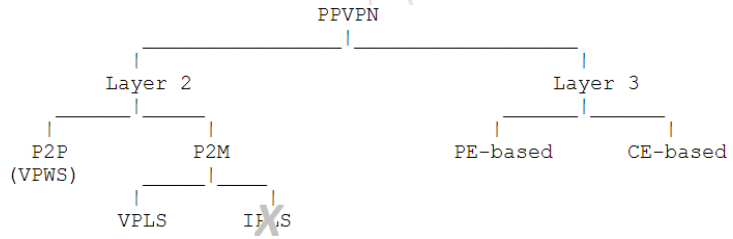

Figura 6.48: Clasificación Servicios VPN

Nos centraremos en el estudio de las L2VPN, concretamente de los modelos VPLS y VPWS (no estudiaremos IPLS) y de L3VPN, con los modelos basados en CE y basados en PE.

Una vez estudiadas las tecnologías VPN, estudiaremos como utilizar dichas tecnologías de redes privadas virtuales para construir redes y servicios públicos, tales como:

- *Servicios residenciales:* los denominados servicios de triple oferta TV, Telefonía e Internet.
- *Servicios corporativos:* redes privadas virtuales.

En este caso, la *red del operador es una red de conmutación de paquetes (MPLS/IP)* con cobertura ilimitada, es decir, nacional. Distinguimos los distintos tipos de equipamiento en estos escenarios:

- **P:** Encaminadores interiores (routers).

- **Provider Edge (PE):** Encaminadores/Conmutadores de la frontera de red (routers o puentes).
- **Customer Edge (CE):** Encaminadores/Conmutadores del abonado, en la frontera de la red (routers o puentes).

El abonado, interconecta sus *redes locales* a través del servicio ofrecido, utilizando:

- Múltiples puntos de acceso.
- Posiblemente, distintas VLAN del mismo abonado en cada punto de acceso.
- El tráfico se envía sólo a los puntos de acceso necesarios respetando las VLAN que el usuario defina.

L2VPN

Distinguimos dos variantes (tipos) de servicio de redes privadas virtuales de capa 2 (L2VPN Services):

- **Virtual Private Lan Service (VPLS):** servicio de emulación de una red local sobre una red área extensa. La red del proveedor se comporta como un puente transparente.
- **Virtual Private Wire Service (VPWS):** servicio de interconexión de dos redes locales a través de una red de área extensa. La red del proveedor proporciona un circuito punto a punto.

Un VPLS es un servicio de nivel 2 que emula el servicio LAN a través de una red de área extensa (WAN). Con respecto a la cantidad de información de estado que debe mantenerse en los equipamientos frontera para soportar la función de transmisión, tiene las características de escala de una LAN. Otras cuestiones de escala podrían venir del número de puntos finales que puede soportar un PE particular.

Un VPWS es un servicio VPN que suministra un servicio de conexión punto a punto a de nivel 2. Como se trata de un servicio de punto a punto, hay muy pocas cuestiones de escala con el servicio en sí. Cuestiones de escala podrían derivarse del número de puntos finales que pueden ser soportados en un PE particular.

Debemos tener en cuenta que VPLS utiliza un servicio que no tiene capacidad de multidifusión nativa para emular un servicio que sí tiene capacidad de multidifusión nativa. Como resultado, habrá problemas de escalabilidad

en relación con el manejo de tráfico de multidifusión en VPLS.

Un servicio VPLS también puede imponer mayores retrasos y ofrecer transporte menos fiable de lo que proporcionaría un servicio LAN nativo. Los protocolos de control estándar de LAN no han sido diseñados para este tipo de entorno y por tanto pueden experimentar problemas de escala.

Existen diferentes tecnologías para implementar cada variante e igualmente existen numerosas normativas (IEEE 802, IETF RFC 4664, ITU-T G.80xy/Y.13xy, MEF) para su estandarización. Es decir, encontramos muchos nombres diferentes para un mismo concepto.

Nosotros nos centraremos en estudiar la RFC 4664, comenzando con la arquitectura genérica recogida en la figura 6.49.

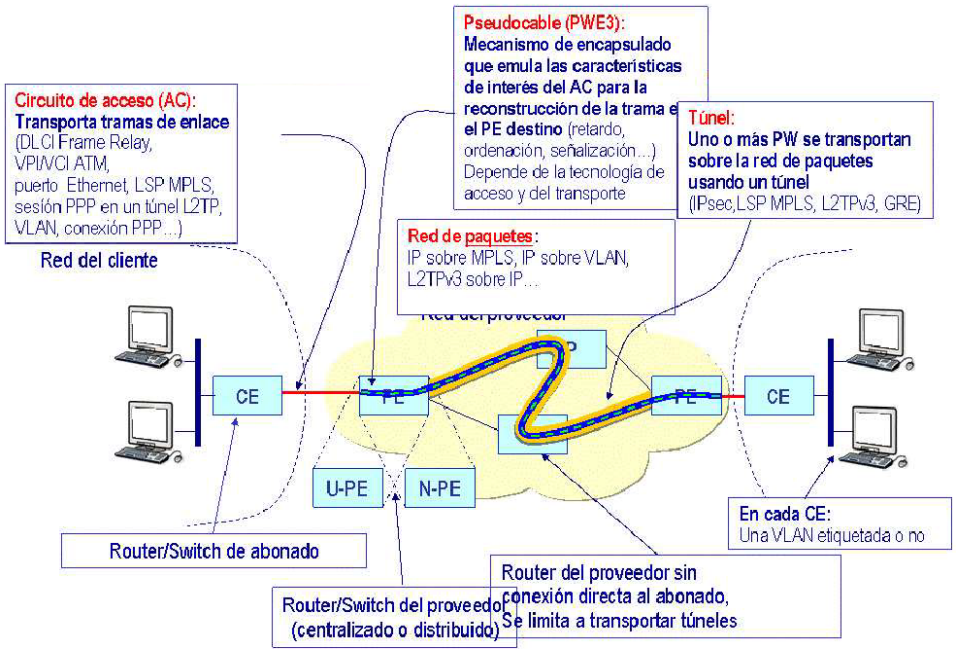

Figura 6.49: Arquitectura RFC 4664

En dicha arquitectura distinguimos los siguientes elementos:

- **Circuito de Acceso (Access Circuit, AC):** transporta tramas de enlace (DLCI Frame Relay, VPI/VCI ATM, puerto Ethernet, LSP MPLS, sesión PPP en un túnel L2TP, VLAN, conexión PPP, ...).
- **Pseudocable (PWE3):** mecanismo de encapsulado que emula las características de interés del AC para la reconstrucción de la trama

en el PE destino (retardo, ordenación, señalización, ...). Depende de la tecnología de acceso y del transporte.

- **Túnel:** Uno o más pseudocables se transportan sobre la red de paquetes usando un túnel (IPsec, LSP MPLS, L2TPv3, GRE).
- **Red del Cliente:** en cada CE podemos encontrar una VLAN, etiquetada o no.
- **Red del Proveedor:** red de paquetes, típicamente IP sobre MPLS, IP sobre VLAN, L2TPv3 sobre IP, ...
- **Router del Proveedor (Centralizado o distribuido):** si no tiene conexión directa al abonado se limita a transportar túneles.

Un pseudocable (PW) es una relación entre dos dispositivos PE. Del mismo modo que un circuito de acceso (AC) es utilizado para portar una trama desde un CE a un PE, un pseudocable (PW) se utiliza para transportar una trama entre dos PEs.

El establecimiento y mantenimiento de los pseudocables es tarea de los PEs. La información de estado para un pseudocable en particular se mantiene exclusivamente en los dos PEs que forman sus extremos, pero nunca en otros PEs ni en otros routers de backbone (P). El establecimiento y liberación del pseudocable se realiza mediante LDP (Label Distribution Protocolo) o L2TP (Layer Two Tunneling Protocol)

Estudiaremos ahora un modelo de pseudocable Ethernet que permite transportar PDUs Ethernet 802.3 sobre una red MPLS, recogido en la RFC 4448.

Vamos a distinguir dos tipos de etiquetas VLAN según su uso:

- **Delimitadora del servicio:** asignada por el proveedor, para marcar el tráfico (por ejemplo diferencias tráfico de distintos clientes). Como máximo una.
- **No delimitadora:** la pone un equipo cliente, y por tanto no significa nada para el proveedor.

Vamos a considerar dos modos de funcionamiento del pseudocable:

- **Etiquetado:** hay al menos una VLAN-ID con significado para el proveedor y debe llevar el mismo valor en ambos extremos del pseudocable.
- **Bruto:** si hay VLAN-ID, no importa el proveedor.

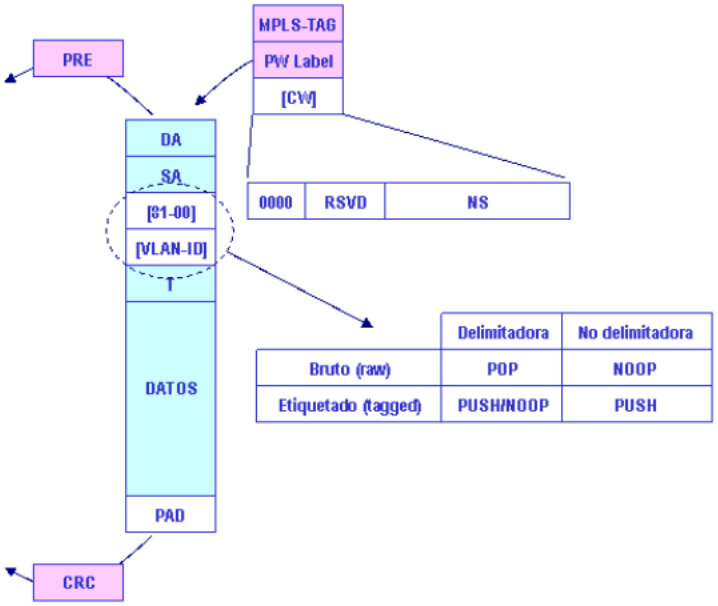

Figura 6.50: Pseudocable Ethernet para MPLS

Estudiaremos ahora la arquitectura de los dos tipos de servicio existentes en L2VPN:

- **Virtual Private Lan Service (VPLS):** atendiendo a la figura 6.51 vemos que el PE se comporta casi como un conjunto de puentes virtuales (al menos un VSI[11] por VPN emulada). Los PE se conectan con pseudocables (p.a.p./p.a.mp.[12]), en malla total, árbol, o árbol malla. Cada VPLS tiene un identificador único en la red (VPN-Id), cuya implementación concreta depende de la tecnología de la dorsal.

  La elección del PW de envío atiende a la MAC destino de la trama. El VSI hace autoaprendizaje y envejecimiento de las SA sólo de las tramas que recibe por los PW.

  Entre PE se sustituye el STP por el horizonte dividido, por ejemplo, en malla lo que ingresa por un PW nunca se reenvía por otro PW.

- **Virtual Private Wire Service (VPWS):** acorde a la nomenclatura de la figura 6.52 las tramas que el CE envía al AC de entrada aparecen por el AC de salida (1) prefijado sin alterar, punto a punto. (2) La elección del PW sólo atiende al AC y no a ningún campo de la trama.

[11] VSI: Virtual Switching Instance.
[12] Punto a Punto/Punto a Multipunto.

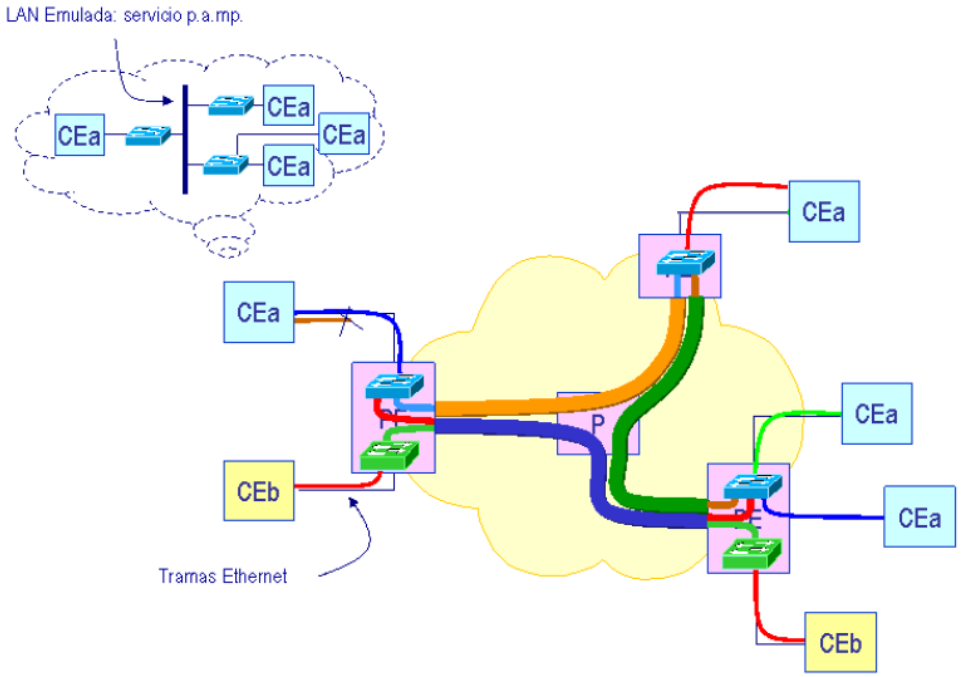

Figura 6.51: L2VPN VPLS

(3) El PW permite al PE seleccionar el puerto y AC de salida sin mirar la trama.

En la figura 6.53 se recoge un escenario donde se da una visión global con un sólo abonado.

VPLS ha demostrado ser un modelo robusto, barato y simple, pero por desgracia difícilmente escalable, lo que presenta problemas al realizar mallados en la red, pues es necesario un pseudocable para realizar un túnel entre dos PEs.

Como solución aparece la RFC 4762, donde se define H-VPLS (Hierarchical VPLS) que introduce una jerarquía de pseudocables, distinguiendo entre nucleares y radiales:

- *Nucleares:* en el núcleo de la red, entre PEs.
- *Radiales:* une un PE con un equipo intermediario al usuario (Multi-Tenant Unit, MTU).

Con este modelo se logran utilizar menos PEs y un menor mallado de pseudocables. siendo necesarios mayores tamaños de caché de MAC en los

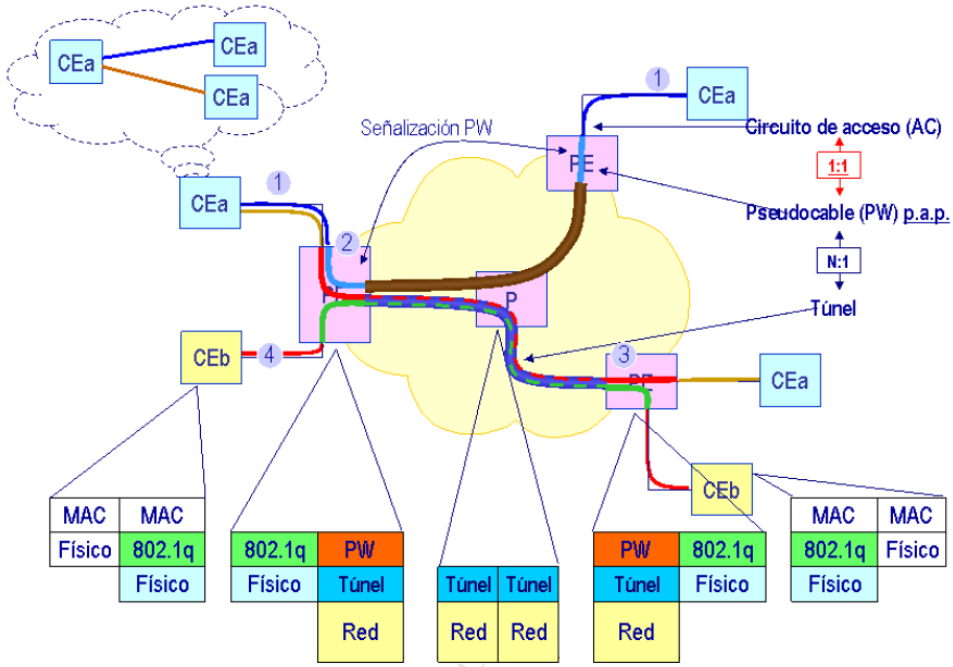

Figura 6.52: L2VPN VPWS

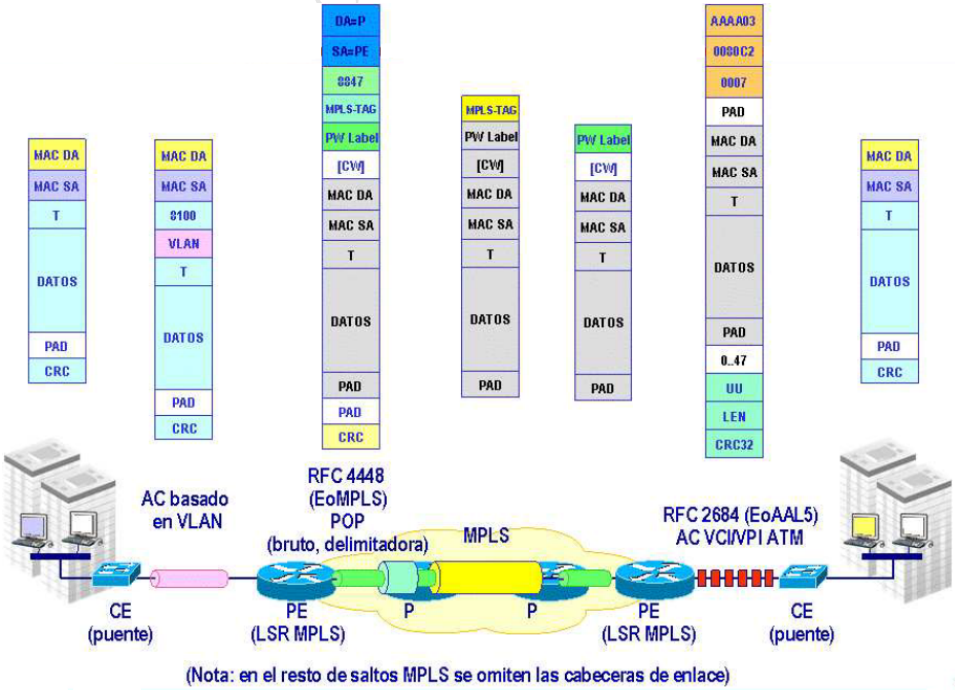

Figura 6.53: L2VPN Visión global con un sólo abonado

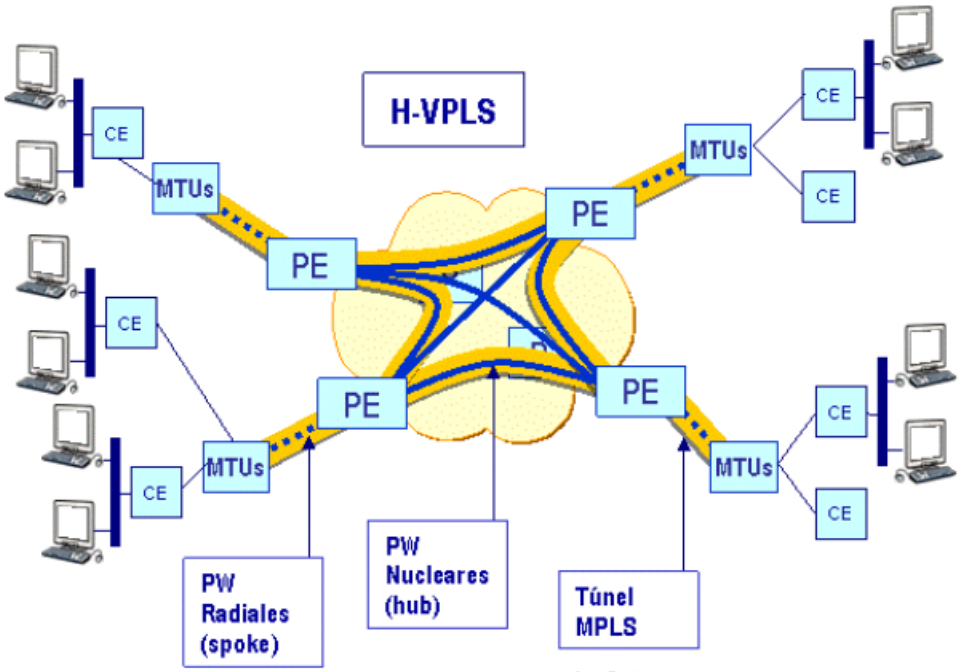

Figura 6.54: L2VPN Hierarchical VPLS

PE.

Finalizamos recogiendo una serie de aspectos comunes a las VPN, tanto L2VPN como las L3VPN que estudiaremos en la siguiente sección. Dichos aspectos comunes son:

- *Descubrimiento:* identificación de extremos miembros de la misma VPN. Se puede realizar mediante servidores Radius, BGP, LDP, DNS.
- *Señalización:* ncesaria para el establecimiento de pseudocables entre dos extremos miembros de la misma VPN. Se implementa mediante L2TP, LDP, BGP.

L3VPN

Estudiaremos únicamente el caso en que la infraestructura de red compartida (backbone VPN) es una red IP/MPLS. Además, únicamente con el caso en que los dispositivos del proveedor de servicios, ya sea en el borde del proveedor (PE) o en el extremo del cliente (CE), determinan cómo enrutar el tráfico VPN mirando las cabeceras IP/MPLS de los paquetes que reciben de los dispositivos de borde de los clientes. Esto es lo que caracteriza de manera distintiva las VPNs de Capa 3. Es decir, estudiaremos la RFC 4110.

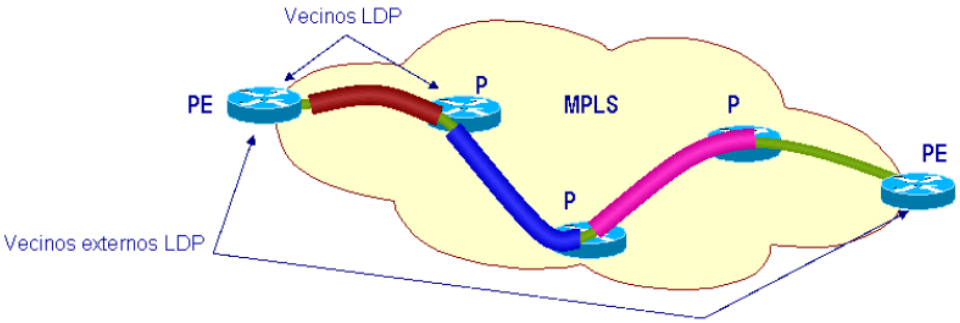

Figura 6.55: Aspectos Comunes VPN

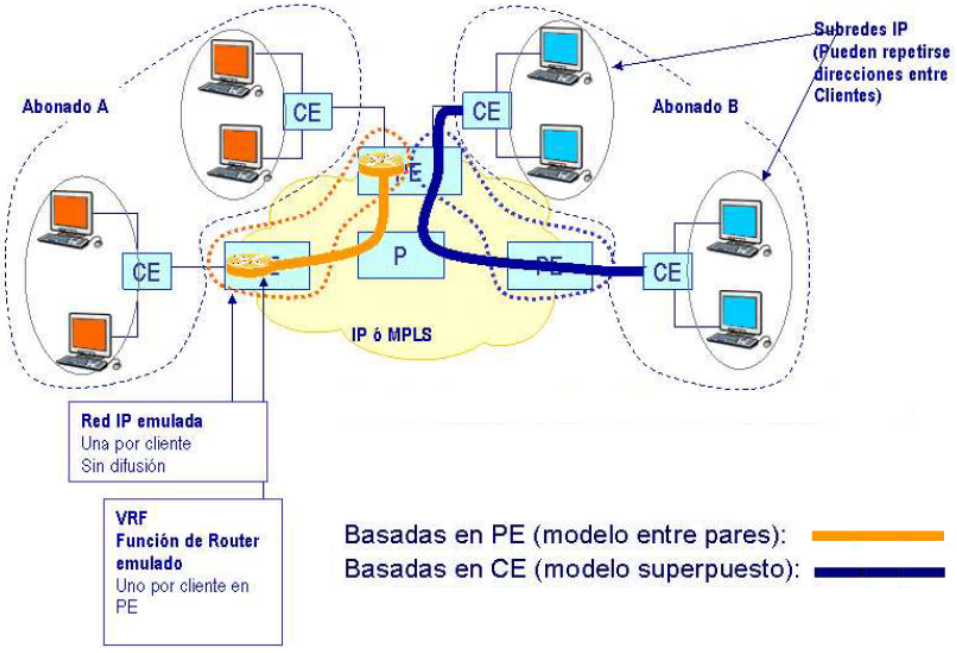

Figura 6.56: L3VPN PE Based y CE Based

Distinguimos dos tipos de L3VPN, recogidos en la figura 6.56:

- **Basadas en PE (modelo entre pares):** En una VPN basada en PE, los paquetes de los clientes se transportan a través de las redes del proveedor del servicio en túneles, tal y como se hace en las VPNs basadas en CE. Sin embargo, en una VPN basada en PE, los extremos del túnel son los dispositivos de PE, y los dispositivos PE deben saber cómo enrutar los paquetes de los clientes, basándose en las direcciones IP que llevan. En este caso, los dispositivos de CE en sí no tiene que tener ninguna capacidad especial de VPN, y ni siquiera tiene que saber que ellos son parte de una VPN.

  En el contexto de L3VPN basadas en PE, un dispositivo **(CE)** puede ser un router, LSR, o host que no tiene ninguna funcionalidad VPN específica. Está vinculado a través de una conexión de acceso a un dispositivo PE.

  Un router **(P)** dentro de una red de proveedores que se utiliza para interconectar dispositivos de PE, pero que no tiene ningún estado VPN y no tiene ninguna conexión directa con los dispositivos CE.

  En el contexto de L3VPN basadas en PE, un dispositivo **(PE)** implementa una o más VFIs (VFI: VPN Forwarding Instance) y mantiene tablas de estado VPN, para el soporte de una o más VPNs. Puede ser un router, LSR, u otro dispositivo que incluye VFIs y funcionalidades de frontera VPN por parte del proveedor, tales como el aprovisionamiento, gestión y clasificación de tráfico y separación. Un dispositivo de PE está unido a través de un circuito de acceso a uno o más dispositivos de CE.

  Es decir, ni CE ni P saben de la existencia de una VPN y el PE es un encaminador (o LSR) con un router virtual para cada abonado cuyo CE se conecta a dicho PE.

  La figura 6.57 recoge un escenario de una red L3VPN basada en PEs sobre MPLS, cuya arquitectura de referencia se puede consultar en la RFC 4364.

- **Basadas en CE (modelo superpuesto):** El término VPN basada en CE basada en VPN se refiere a un enfoque en el que los dispositivos de PE no saben nada acerca del enrutamiento o direccionamiento de las redes de los clientes. Los dispositivos PE ofrecen un servicio IP simple, y esperan recibir paquetes IP cuyos encabezados contienen

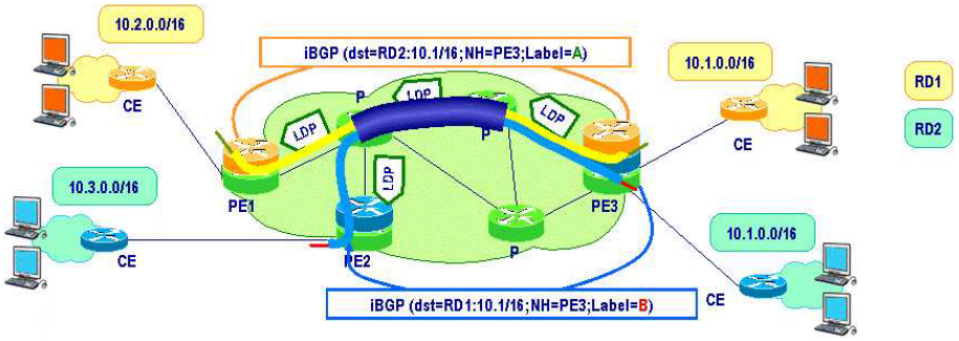

Figura 6.57: L3VPN basadas en PEs/MPLS

sólo direcciones IP globales.

En el contexto de L3VPN basadas en CE, un dispositivo **(CE)** proporciona conectividad de Capa 3 a las instalaciones del cliente. Puede ser un router, LSR, o host que mantiene uno o más puntos finales del túnel VPN. Un dispositivo (CE) se une a través de un circuito de acceso a un dispositivo (PE) que normalmente se encuentra en la frontera de un sitio de cliente o co-situado en un local de SP.

En el contexto L3VPN basado en CE, un router **(P)** en el interior de la red del proveedor se utiliza para interconectar dispositivos (PE), desconociendo la existencia de cualquier VPN y sin estar conectado directamente a ningún dispositivo (CE).

En el contexto de L3VPN basadas en CE, un dispositivo **(PE)** puede ser un router, LSR, u otro dispositivo que no tiene ninguna funcionalidad VPN específica. Se acopla a través de un circuito de acceso a uno o más dispositivos de (CE).

En las VPNs basadas en CEs, el enrutamiento en la red del cliente trata de los túneles de capa 2 como enlaces. El CE es un encaminador (o LSR) con túneles que van a los CE de la misma VPN.

En la figura 6.58 se recoge un escenario donde se da servicio a un único abonado, conectando dos de sus redes locales mediante una L3VPN.

Por supuesto, la utilización de L2VPN y L3VPN no es excluyente, sino todo lo contrario, es posible (y frecuente) utilizar soluciones mixtas para proporcionar dichos servicios.

Vemos en el ejemplo de la figura 6.59 que estar conectado al mismo puente virtual no implica que deba haber conexión directa entre CE1 y

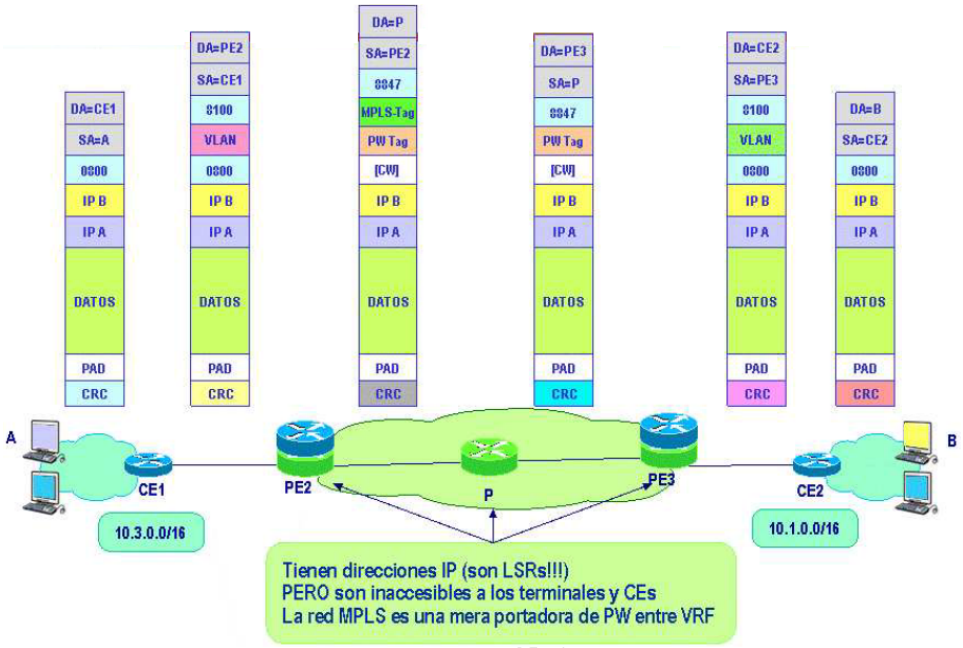

Figura 6.58: L3VPN Visión con un sólo abonado

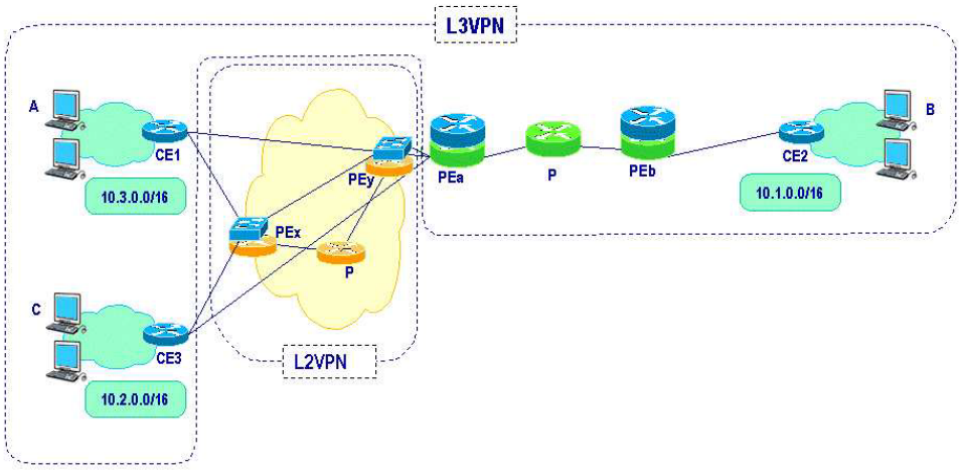

Figura 6.59: Escenario Mixto L2VPN/L3VPN

CE3, sin pasar por PEa. Así, entre cada CE y su VRF en PEa puede haber un pseudocable distinto, como entre un puente real y cada CE podría haber dos VLAN diferentes.

6.3.3. IEEE: Ethernet para Operador (Carrier Ethernet) (II)

Los puentes, comparados con los equipos MPLS son menos flexibles y, cuando hay cambios topológicos se reconfiguran algo más despacio (si se usa RSTP) pero tienen a favor que son bastante más baratos que los equipos MPLS.

Los problemas de escalabilidad y explosión de caché se pueden resolver separando los espacios de direcciones MAC de abonados y operador.

Por tanto, se define **802.1ah PBB Provider Backbone Bridge**, también conocido como conocido como Mac-in-Mac o MinM, como solución a estos problemas, pudiendo utilizar Ethernet como red de transporte para el operador. Para ello PBB define una arquitectura y un conjunto de protocolos de enrutamiento a través de la red de un proveedor, permitiendo la interconexión de varias redes de clientes sin que cada cliente pierda sus VLAN definidas individualmente.

La idea esencial consiste en realizar una separación del espacio de direcciones MAC+VLAN del cliente del espacio de direcciones del proveedor. Las tramas de cliente van enteras sobre tramas de la operadora y se añaden etiquetas adicionales, como ilustra la figura 6.60.

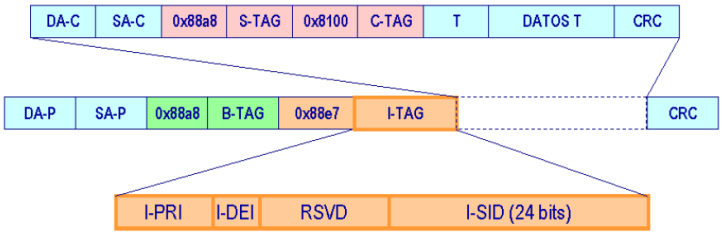

Figura 6.60: Etiquetas 802.1ah PBB Provider Backbone Bridge (Mac-in-Mac)

El formato de la B-TAG es el mismo de S-TAG (TAG/VID/VLAN). Se define un nuevo formato de etiqueta I-TAG, identificador de servicio (I-SID) con mayor rango de etiquetado.

En la figura 6.61 se recoge un escenario donde se interpreta el espacio de direcciones de la 802.1ah, donde debemos tener en cuenta los siguientes detalles a considerar:

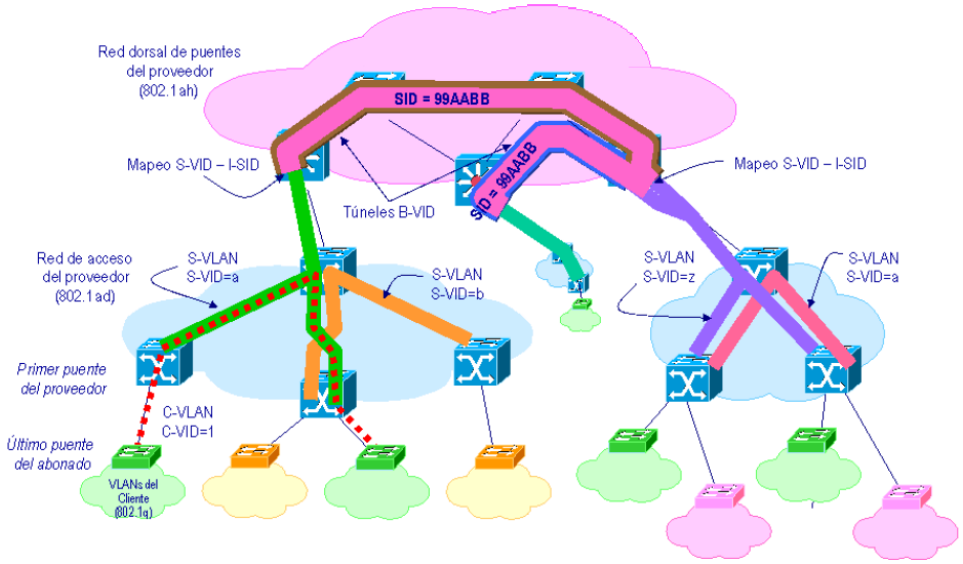

Figura 6.61: Interpretación física 802.1ah PBB Provider Backbone Bridge (Mac-in-Mac)

- La etiqueta B-VID identifica el túnel sobre el que se transportan las VLAN de Servicio sobre la dorsal.
- La S-VID tiene significado local a su red 802.1ad.
- I-SID identifica al cliente en la dorsal del proveedor, por lo tanto *no es una etiqueta de nivel de enlace.* El I-SID tiene un significado local a la red 802.1ah, pero identifica globalmente a uno de los clientes del proveedor.

El sistema MinM tiene como mayor ventaja que no es necesario realizar un aprendizaje de las MAC del cliente, únicamente es necesario el I-SID, pero tiene una serie de limitaciones como:

- Cada puente dorsal de operador consume una dirección MAC, por lo que presenta poca escalabilidad en servicios donde el usuario demanda multidifusión y además hay que encapsular en una trama MAC distinta para cada puente de operador destino.
- Mayor sobrecarga de transmisión.

Recogemos en la tabla 6.7 las diferencias principales entre las tecnologías MPLS y QinQ/MinM.

Para finalizar este apartado, se lanzan una serie de preguntas al lector para afianzar ideas sobre estas tecnologías:

	MPLS	**IEEE (QinQ/MinM)**
Capa Física	No definida	802.3
Plano de Control	LDP,RSVP-TE	No
Dirección Origen	No viaja	Viaja en la trama(SA)

Tabla 6.7: Diferencias MPLS - IEEE (QinQ/MinM)

- *¿ Puede la trama MinM transportarse sobre MPLS ?*
- *¿ Puede usarse L3 para comunicar SIDs (OSPF/IS-IS ...) ?*

6.3.4. Servicios de triple oferta y Acceso residencial basado en Ethernet

Red de Acceso basada en Ethernet

Hemos estudiado la existencia de una red dorsal Ethernet para dar soporte de VPN a clientes empresariales o corporativos. Dado que la tecnología es lo suficientemente estable, **¿ por qué no utilizarla para dar soporte a clientes residenciales, agregando DSLAMs ?**

Este enfoque tiene una serie de características importantes en su implementación que pasamos a comentar:

- Elimina la necesidad de las capas ATM/SDH.
- Incompatible con desagregación del bucle de abonado por acceso indirecto.
- Calidades: sustituir VC/VP por VLAN-ID.
- Seguridad: obligatoria segregación VLAN-ID.

Encontramos dos alternativas (tipos de equipos) para el acceso residencial basado en Ethernet:

- **DSLAM Ethernet:** agregación de un puerto Ethernet 1 Gb/s (1 GbE). Puede coexistir con el puerto ATM, así los usuarios son servidos según proveedor. A la entrada al DSLAM, la operadora identifica a cada proveedor por el VCI/VPI, si corresponde al puerto 1 GbE, desencapsula la trama ethernet y escoge VLAN-ID según proceda. Si corresponde al puerto ATM, asigna VPI/VCI nuevo y conmuta su PAI.
- **DSLAM IP:** agregación a un puerto Ethernet 1 GbE. Puede coexistir con el puerto ATM, así los usuarios son servidos según proveedor. A la entrada al DSLAM, la operadora identifica a cada proveedor por

VPI/VCI. Si corresponde al puerto 1 GbE, desencapsula el paquete IP y escoge VLAN-ID según proceda (Salida: IP sobre VLAN-ID que proceda). Si corresponde al puerto ATM, asigna su VPI/VCI nuevo y conmuta su PAI.

El DSLAM IP implementa unas funciones adicionales, como la terminación DHCP y terminación PPP.

Por supuesto, las alternativas no son excluyentes y se puede funcionar de las dos (tres) formas simultáneamente.

En estos sistemas existe una motivación para el uso de IP sobre PPP sobre ATM, y es que es bueno para gestión de usuarios en servicios IP (Authenticatio, Authorization and Accounting, AAA) y es bueno también para agregación sobre L2TP a la salida del DSLAM. Sin embargo, no es buena solución para soporte de tráfico multidifusión, necesaria para el servicio IPTV, ya que es necesario mantener una sesión PPP por usuario en conexiones que además son punto a punto.

En la figura 6.62, donde en la parte superior de la figura vemos el acceso ya estudiado mediante DSLAMs clásicos y en la inferior la nueva arquitectura propuesta, donde se hace uso de DSLAMs IP ó Ethernet.

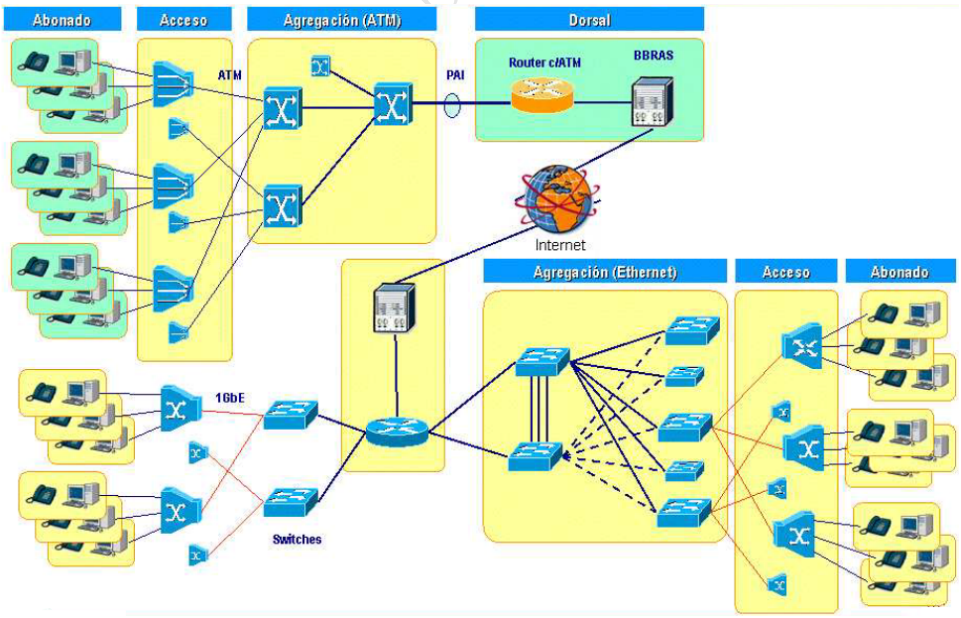

Figura 6.62: Estructura general agregación Ethernet

En la agregación Ethernet, la duplicidad de enlaces aparece por motivos

de redundancia en caso de error, no para ofrecer balanceo.

Como vemos en la figura 6.63, el acceso y la agregación se colapsan en una red IP de cobertura metropolitana.

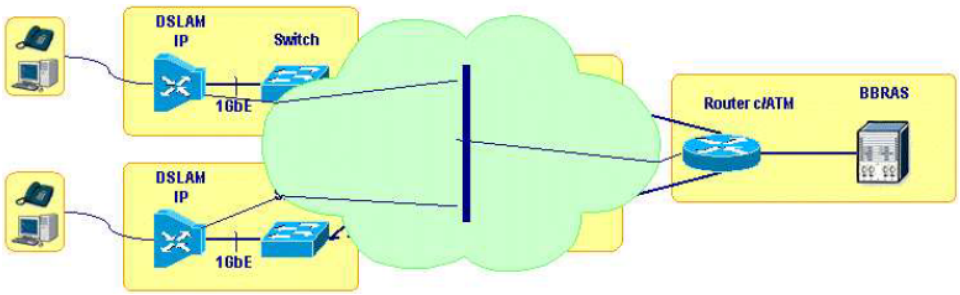

Figura 6.63: Acceso y agregación mediante red IP

Esta configuración permite la posibilidad de usar servicios L2VPN, en vez de switches convencionales, logrando así un mejor aprovechamiento de la robustez de MPLS (reencaminamiento rápido) y una reconfiguración más rápida que con STP.

Servicios de triple oferta

Todo el despliegue técnico explicado hasta ahora se ha materializado en forma comercial en lo que se conoce como servicio Triple-Play o de Triple Oferta, en el que las nuevas modalidades DSL en el bucle permiten ofrecer al abonado un servicio conjunto de Televisión, Telefonía y Acceso a Internet de Alta Velocidad, haciendo competencia directa a los operadores de cable.

Existe una doble motivación en la implementación de estos servicios. En primer lugar la motivación económica, incrementando el ARPU[13], rentabilizando aún más las instalaciones de bucle de abonado sobre pares y por otro lugar la motivación estratégica, logrando retener un mayor número de clientes.

Aparte de la justificación económica y estratégica, para el proveedor de servicios es mejor si se integra todo en la misma red de acceso y agregación que los servicios corporativos.

Como vemos en la figura 6.64, la arquitectura general es bastante similar a la de las redes híbridas de fibra y cable.

[13] ARPU: Average Revenue Per User o ingresos medios por usuario.

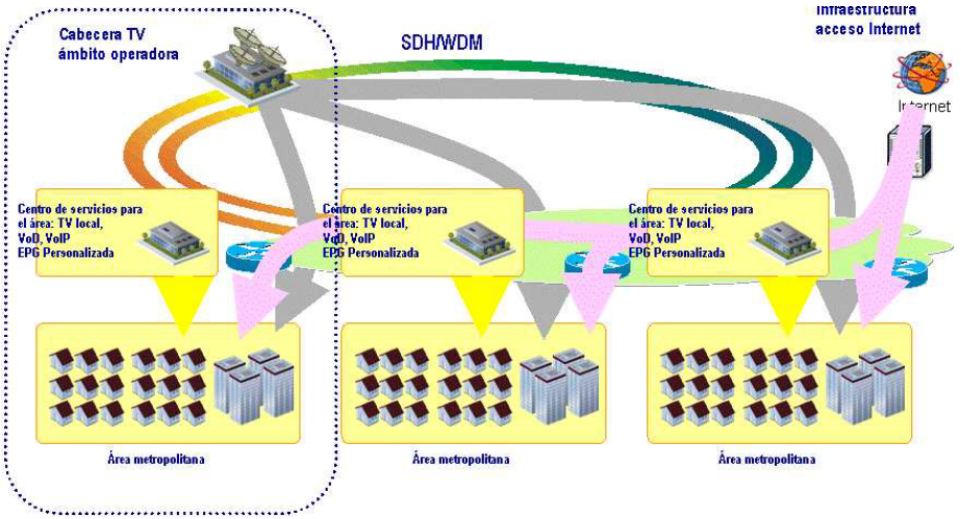

Figura 6.64: Arquitectura general servicios triple oferta (I)

Encontramos una cabecera, muy similar en cuanto a funciones a las estudiadas en los sistemas de CATV que se conecta a un anillo de fibra SDH/WDM. Con un funcionamiento similar a los nodos primarios, encontramos los Centros de Servicios para un área metropolitana, donde se introducen las TV locales, servicios de VoD, VoIP y se genera la EPG personalizada.

En la figura 6.65 nos centramos en la red de agregación, que puede ser Ethernet o VPLS, así como las pasarelas para acceso a Internet, servicios de VoD o servicios corporativos.

Es interesante conocer el vocabulario típico asociado a estos servicios. Destacamos:

- *Difusión de televisión (Broadcast TV, BTV):* emisión de programación prefijada de forma simultánea a una multiplicidad de usuarios sin posibilidad de interactuar sobre el servicio. Equivalente al servicio tradicional de difusión de televisión.
- *Control de reproducción (Time Shifted TV):* el usuario puede detener, rebobinar (limitadamente), repetir y avanzar en el contenido, incluso hasta alcanzar el instante real difundido. Las necesidades de memoria para estas funciones se pueden implementar en el dispositivo reproductor o bien en la red.
- *Vídeo a demanda (Video On Demand, VoD):* acceso individual a un contenido audiovisual en el momento deseado por el abonado con control de reproducción. Para el servicio de compra de películas por ejemplo.

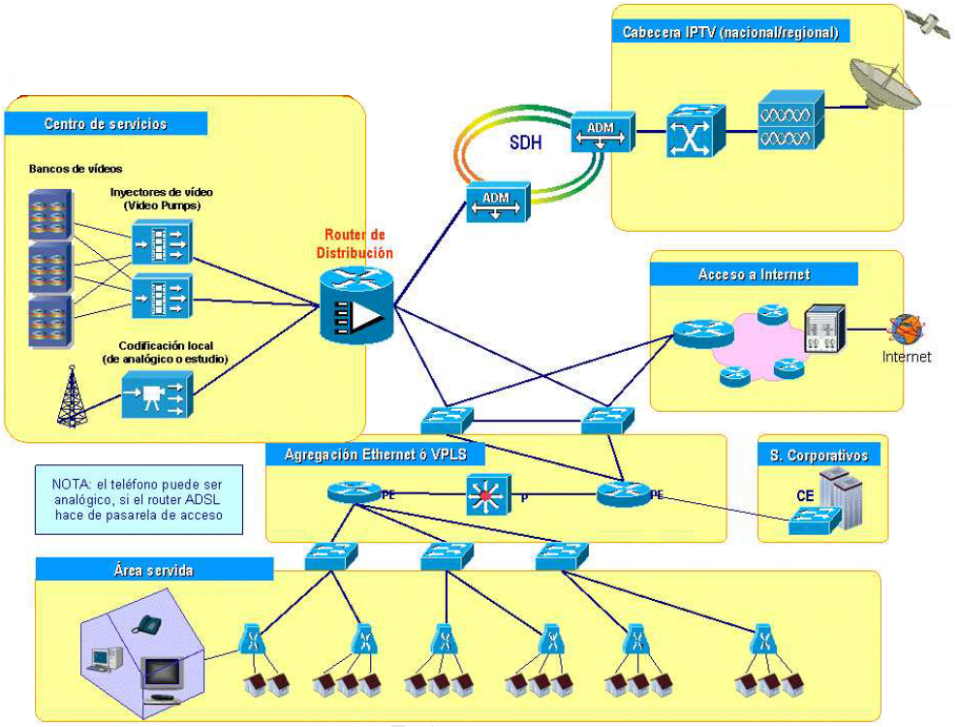

Figura 6.65: Arquitectura general servicios triple oferta (II)

- *Contenido audiovisual:* películas, noticias, documentales, eventos deportivos, ...
- *Vídeo a la carta (nVoD, PPV):* difusión de un contenido audiovisual en el que el usuario accede al programa deseado en el momento prefijado por la red, con control de reproducción. Suele acompañarse de la difusión del mismo contenido desplazado temporalmente en otro canal. Por ejemplo para el servicio de compra de eventos deportivos.
- *Multigrabadora personal en red (PVR, nPVR):* grabadora digital por el abonado en la red.
- *Guía de Programación (Electronic Program Guide, EPG):* proporciona información personalizada, es decir según el abonado y lo que tenga contratado, de la programación disponible. Se genera una por cada usuario.

Es importante también realizar una serie de consideraciones sobre el plan de direccionamiento IP:

- En el acceso a internet, el abonado necesitará al menos una dirección IP pública, para poder hacer NAT (Network Address Translation).

- Para el acceso a contenidos a demanda el uso de direcciones IP públicas no es aconsejable, por su ámbito, por eficiencia de uso del espacio de direcciones y por seguridad (las direcciones pueden reutilizarse en cada área de servicio).
- Para el acceso a contenidos BTV es conveniente utilizar direcciones IP multicast.
- Para el acceso al servicio de telefonía IP, la dirección IP asociada al teléfono no tiene por qué ser pública, sino que basta con que sea alcanzable por proxys y pasarelas. Dichos proxys y pasarelas no tienen por qué ubicarse por área de servicio, además el dimensionado de los servidores de vídeo no tiene por qué coincidir con el de los proxys.

A continuación, introduciremos las distintas opciones de VLAN a implementar a la salida de los DSLAMs, en la red de agregación para segregar los distintos servicios a los abonados de una zona, donde veremos ventajas e inconvenientes de cada opción

- **1 VLAN por Servicio:** recogido en la figura 6.66. Se asocia un VPI/VCI por servicio, es decir, por VLAN-ID. Los router ADSL admiten hasta 3 direcciones IP y cada servicio gestiona su QoS independientemente dentro de su VLAN. Es importante destacar que un servicio es equivalente a un dominio de difusión independiente (VLAN). Permite una total independencia de servicios y ubicación de servidores.

  El principal problema es que la utilización de una VLAN por servicio y usuario no es manejable.

- **1 VLAN por DSLAM:** recogido en la figura 6.67. Requiere coordinación/coubicación de servicios para gestión de la QoS en VLAN. En este caso asociamos un DSLAM a un dominio de difusión.

- **1 VLAN por protocolo:** recogido en la figura 6.68. Distintos servicios usan distintos protocolos. Se utilizarán 1 ó 3 VP/VC por abonado y tendremos tantas VLAN como protocolos.

  Todas las opciones anteriores son vulnerables a la suplantación de identidad por MAC, requiriendo acciones en el DSLAM o en el servidor para solventarlas. Además la calidad es por VLAN-ID y por VP/VCI, no por servicio/usuario que sería lo deseable. Para solucionarlo surge la siguiente opción.

- **1 VLAN por bucle de abonado con QinQ:** recogido en la figura 6.69. Identificamos al abonado dentro del DSLAM por la etiqueta C-VID. La etiqueta S-VID identificará al DSLAM, permitiendo ofrecer

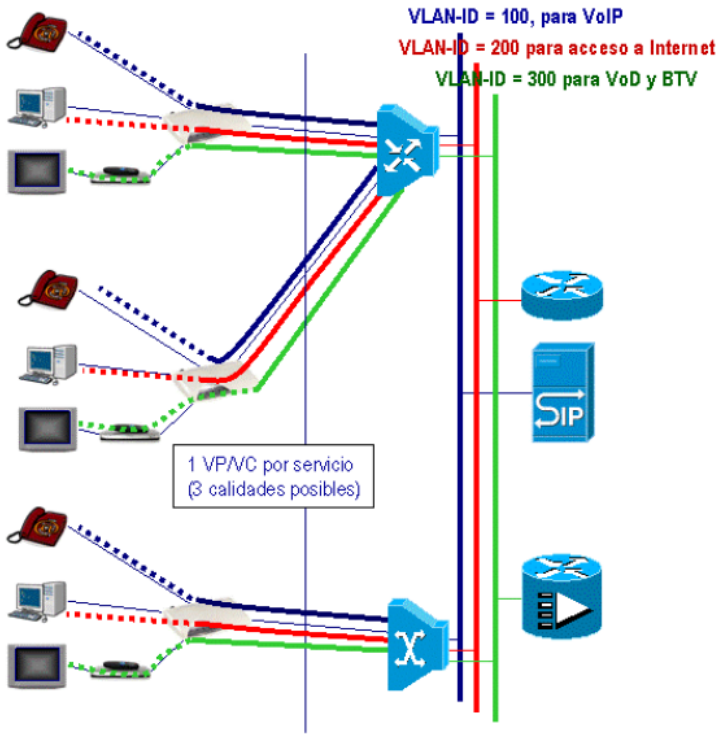

Figura 6.66: VLAN Salida DSLAM (I): VLAN por Servicio

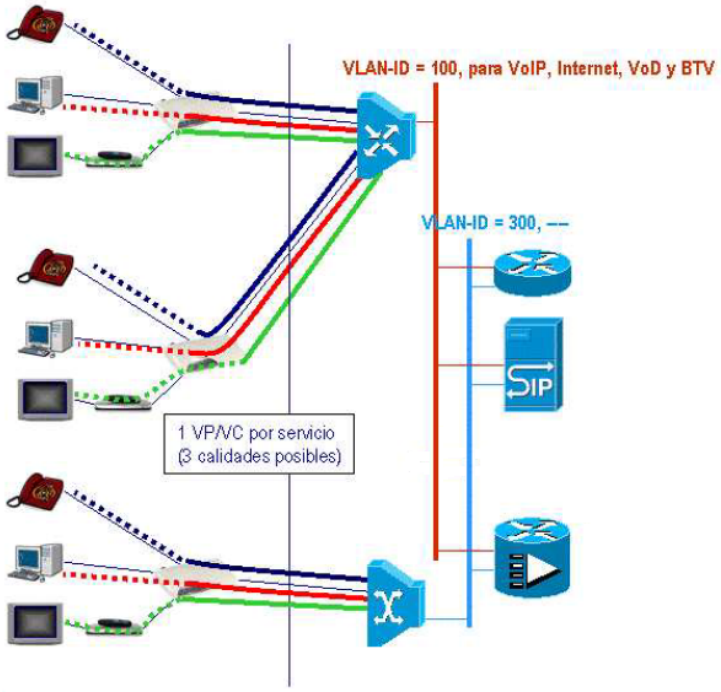

Figura 6.67: VLAN Salida DSLAM (II): VLAN por DSLAM

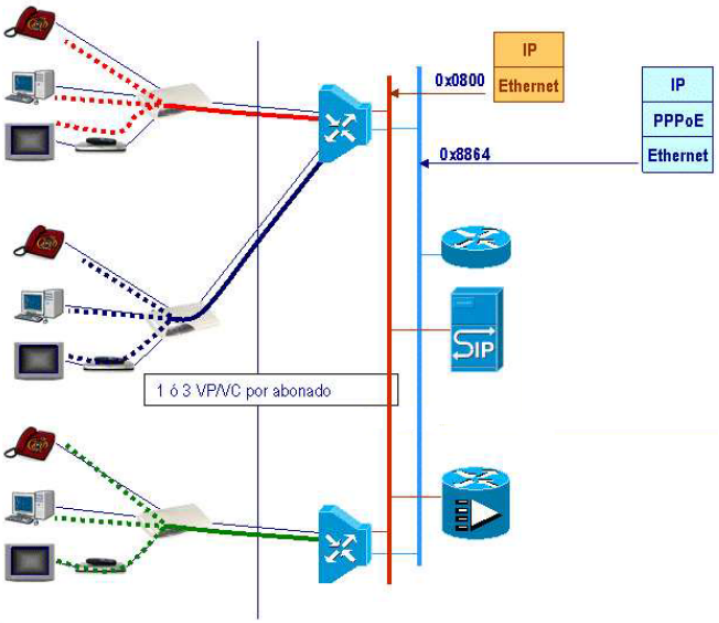

Figura 6.68: VLAN Salida DSLAM (III): VLAN por Protocolo

distintas QoS por abonado. Con QinQ se permite tener hasta 4094 x 4094 abonados por área residencial. La opción anterior multiplica el consumo de tráfico BTV/nVO/PPV ya que, por ejemplo, dos abonados del mismo DSLAM viendo el mismo canal de BTV consumen dos veces su capacidad. La misma VLAN se utiliza para VoD aunque su tasa de actividad es mucho menor.

La solución adoptada para mejorar el consumo de tráfico es utilizar 1 C-VLAN para BTV y N C-VLAN para Internet/VoIP para los N usuarios así como QinQ a la salida del DSLAM.

A todas estas opciones hay que añadir una VLAN aparte, para gestión de los distintos DSLAMs por parte del operador.

Estudiaremos ahora para finalizar el tema la transmisión de servicios de difusión de TV, es decir, el modo de funcionamiento básico para BTV y servicios como PPV o VoD. Todos estos servicios se basan en el envío de un flujo MPEG-2 SPTS, sobre RTP/UDP/IP a una dirección de multicast[14].

Por tanto, serán necesarias tantas direcciones IP multicast como programas individuales (flujos SPTS) se estén difundiendo.

[14]Ver anexo G.

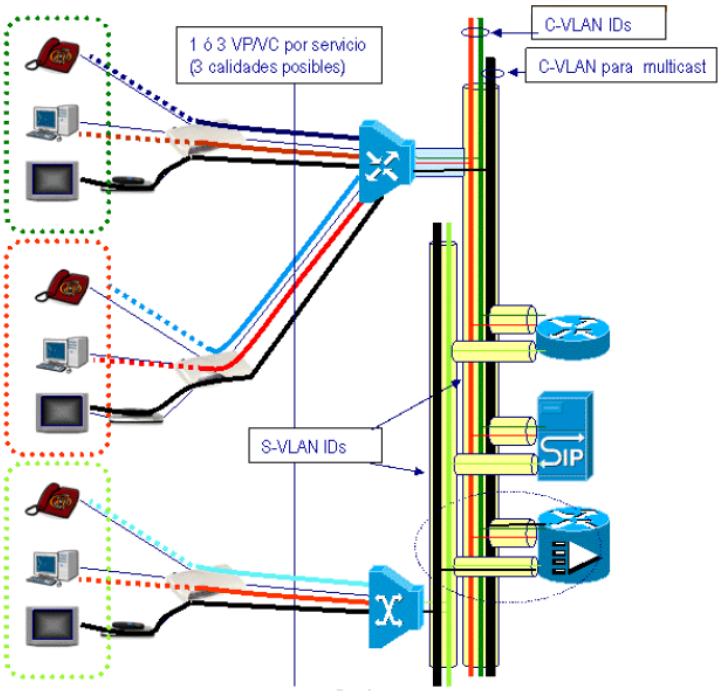

Figura 6.69: VLAN Salida DSLAM (IV): VLAN por abonado con QinQ

La conmutación entre canales se realiza mediante el protocolo IGMPv2/v3, recogido en la RFC 2236, utilizando los métodos LEAVE y JOIN. Un ejemplo básico de difusión de canales y JOIN se muestra en la figura 6.70, donde el emisor, es decir la cabecera, envía los paquetes de un canal de TV a su dirección de multicast (un único envío) siendo el router de distribución el encargado de enviar las copias a los interesados que hayan hecho JOIN a dicho canal.

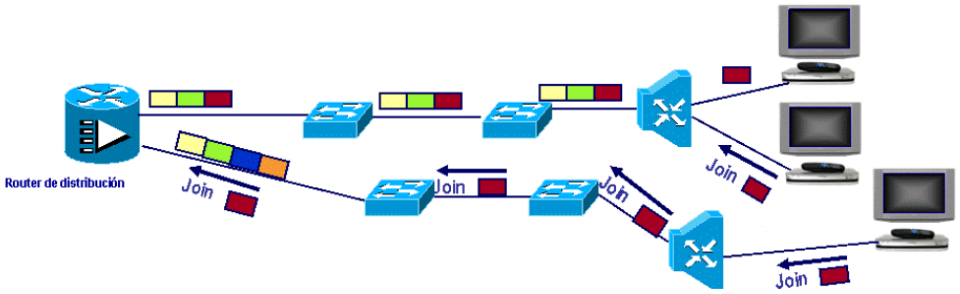

Figura 6.70: Servicio triple play: distribución de TV

Vemos que al hacer JOIN, el canal prospera hasta el equipo adecua-

do (IGMP snooping/proxy en los equipos que lo soporten). Si el canal no está disponible por falta de capacidad, no se informa al abonado.

IGMP (Internet Group Management Protocol) es un protocolo para gestión de grupos multicast. Permite a un router multicast replicar los paquetes dirigidos a destinos IP multicast por las interfaces en las que hay algún receptor interesado. Su funcionamiento es muy simple, basado en las primitivas JOIN, LEAVE y REPORT, explicadas en el Anexo G.

Para poder utilizar IGMP en aplicaciones de IPTV, es necesario realizar algunos trucos:

- *Snooping:* interpretación sigilosa de los mensajes IGMP dirigidos al router multicast. La interpretación la realiza el DSLAM IP o bien equipos de capa 2 (conmutadores de agregación o distribución). No se modifica el mensaje.
- *Proxy:* intermediación activa con el router multicast, realizada por el DSLAM IP. El proxy genera mensajes IGMP con su propia dirección IP, eliminando la del STB.
- *Efecto:* reduce el tiempo de respuesta a una orden de cambio de canal.

Para el transporte de servicios a demanda, es decir, para el funcionamiento básico de servicios como VoD/nPVR, se utiliza un flujo MPEG-2 SPTS sobre RTP/UDP/IP a una dirección unicast, concretamente a la del abonado que ha solicitado el servicio, como vemos en el ejemplo de la figura 6.71. En este caso, se parte de la ventaja estudiada del factor de concurrencia, por el que el operador sabe que no más del 20 % de los usuarios acceden simultáneamente a contenidos a demanda, lo que facilita la distribución de los mismos.

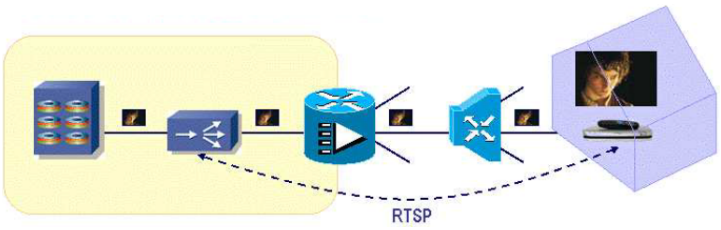

Figura 6.71: Servicio triple play: Video On Demand

Se realiza un control de la reproducción con el protocolo RTSP (Real Time Streaming Protocol), recogido en la RFC 2326. Permite el control de la reproducción de un flujo muiltimedia (adelante, atras, pausa, reproducción,

...) utilizando una sesión independiente del transporte del flujo, es decir, utiliza un puerto UDP/TCP disinto al del streaming, como vemos en la figura 6.72.

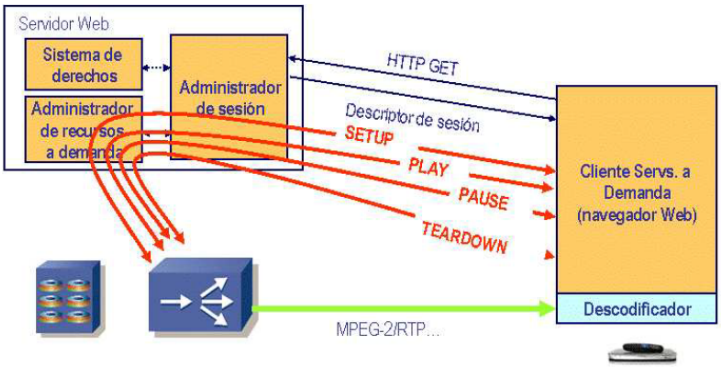

Figura 6.72: Servicio triple play: RTSP

Utiliza un formato de menajes textuales con una sintaxis similar a la de HTTP. En la figura 6.73 vemos un ejemplo de diálogo para solicitar un vídeo.

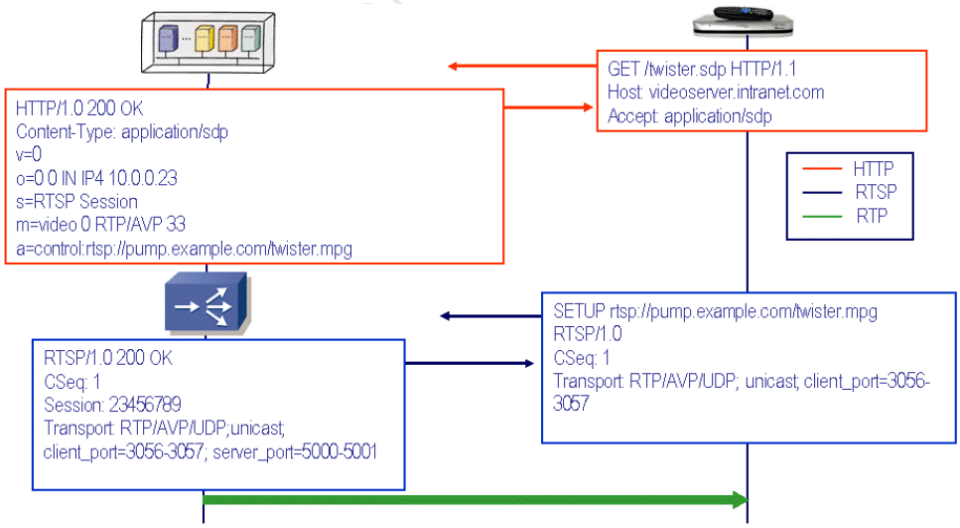

Figura 6.73: Servicio triple play: Diálogo RTSP

Concluimos el capítulo con una reflexión sobre la evolución de Ethernet. Actualmente tenemos Ethernet en el acceso, para la agregación de DSLAMs para mercado residencial y servicios VPN para mercado empresarial y utilizamos Ethernet en el transporte, para la multiplexión y transporte de los servicios anteriores.

La evolución natural del sistema es llegar a utilizar Ethernet en el bucle de abonado sobre DSL, lo que permitirá eliminar la capa ATM.

Apéndice A

Normalización [1]

Este apartado aún no está correctamente desarrollado. No obstante es muy recomendable y probablemente más que suficiente consultar el apartado 4 de la referencia [13], disponible en `http://trajano.us.es/~isabel/publicaciones/ARSS/1011/tema1.pdf`.

[1] Este capítulo está basado en los trabajos [13], [12] y [15]

Apéndice B

Recomendación I.120 (03/93)

REDES DIGITALES DE SERVICIOS INTEGRADOS

(Málaga-Torremolinos, 1984; modificada en Helsinki, 1993)

B.1. Principios de la RDSI

1.1. El concepto de RDSI se caracteriza esencialmente por el hecho de que permite una amplia gama de aplicaciones vocales y no vocales en la misma red. Un elemento clave para la integración de servicios en una RDSI, es la prestación de una gama de servicios mediante el empleo de un conjunto limitado de tipos de conexión y configuraciones de interfaz polivalente usuario-red.

1.2. Las RDSI soportan aplicaciones diversas, entre las cuales están las conexiones conmutadas y no conmutadas. Las conexiones conmutadas en una RDSI comprenden conexiones con conmutación de circuitos, conexiones con conmutación de paquetes, y sus concatenaciones.

1.3. En la medida en que sea posible en la práctica, los nuevos servicios que se introduzcan en una RDSI deberán disponerse de modo que sean compatibles con las conexiones digitales conmutadas a 64 kbit/s.

1.4. Una RDSI contendrá inteligencia para asegurar las características de servicio, y las funciones de mantenimiento y gestión de la red. Es posible que esta inteligencia no sea suficiente para algunos nuevos servicios y sea necesario suplementarla mediante inteligencia adicional dentro de la propia red o, lo que también es posible, mediante una inteligencia compatible en los terminales de usuario.

1.5. Para la especificación del acceso a una RDSI se debe utilizar una

estructura estratificada de los protocolos. El acceso de un usuario a recursos de la RDSI puede variar según el servicio requerido y el estado de la realización de las RDSI nacionales.

1.6. Se reconoce que las RDSI pueden realizarse en una diversidad de configuraciones de acuerdo con las situaciones nacionales específicas.

1.7. Las Recomendaciones de la serie I se han elaborado basándose en estos principios. La Figura 1 presenta, a grandes rasgos, la estructura de las Recomendaciones de la serie I y sus relaciones con otras Recomendaciones. Como puede verse en la Figura 1, la estructura actual de los documentos de la serie I se divide en siete partes principales. En la medida en que se haga necesario pueden añadirse otros documentos a la serie I. Además de esto, como ayuda a la realización del concepto de RDSI, se ha elaborado cierto número de Recomendaciones y se procederá a la elaboración de otras, en otras series, a cargo de los grupos de especialistas apropiados.

B.2. Evolución de las redes hacia la RDSI

2.1. Las RDSI se basan en redes digitales integradas (RDI) para telefonía y evolucionarán a partir de estas redes incorporando progresivamente funciones adicionales y características de red, incluidas las que son propias de otras redes especializadas como son las redes de datos con conmutación de circuitos y las redes de datos con conmutación de paquetes, a fin de tener en cuenta los servicios actuales y los nuevos.

2.2. La transición de una red actual a una RDSI completa puede requerir el transcurso de una o más décadas. Durante ese periodo se deben adoptar disposiciones para el interfuncionamiento de servicios ofrecidos por las RDSI y servicios ofrecidos por otras redes.

2.3. En la evolución hacia una RDSI, la conectividad de extremo a extremo se obtendrá por medio de los recursos y equipos utilizados en las redes existentes, tales como transmisión digital, conmutación múltiplex por división en el tiempo y/o conmutación múltiplex por división en el espacio. Las actuales Recomendaciones pertinentes sobre estos elementos constitutivos de una RDSI figuran en las correspondientes series de Recomendaciones del CCITT y del CCIR.

2.4. En las etapas iniciales de la evolución de las RDSI es posible que deban adoptarse disposiciones provisionales relativas a las redes de usuario a fin de facilitar, en ciertos países, una temprana penetración de capaci-

dades de servicios digitales. Las disposiciones que corresponden a variantes nacionales pueden ajustarse total o parcialmente a las Recomendaciones de la serie I. Sin embargo, se tiene el propósito de no incluirlas específicamente en la serie I.

Una RDSI en evolución puede incluir también conexiones conmutadas a velocidades binarias superiores e inferiores a 64 kbit/s. En la Recomendación I.121 figuran los aspectos de banda ancha de la RDSI.

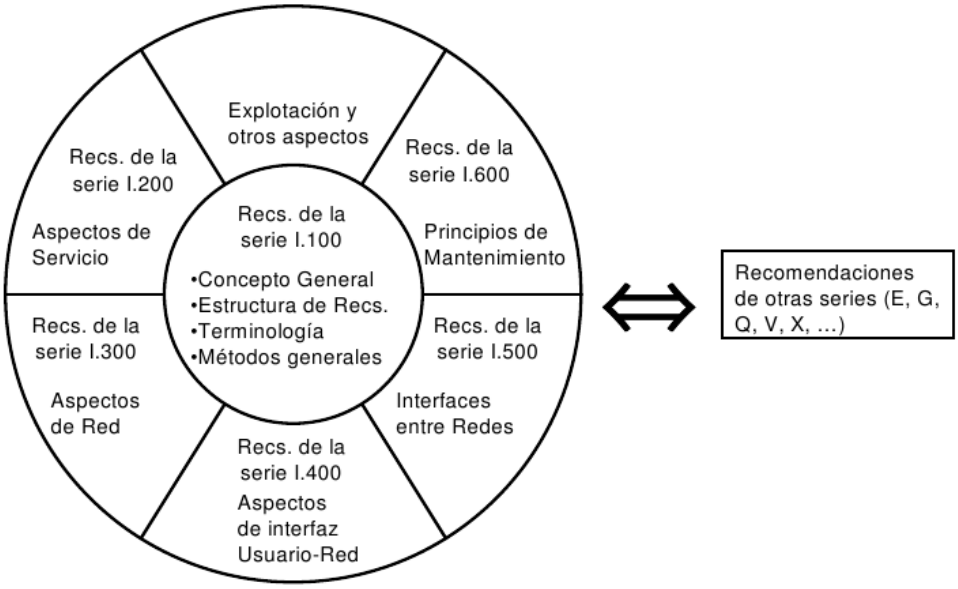

Figura B.1: Recomendaciones Serie I de la UIT-T

NOTA – En las Recomendaciones pertinentes de la serie I figuran modelos, configuraciones de referencia, instrumentos y métodos.

Apéndice C

El Modelo OSI[1]

C.1. Motivación

Históricamente, cuando el trabajo que se llevaba a cabo, constaba de un escenario con más de un computador, se debían añadir una serie de elementos extras al sistema: el hardware y el software necesario para soportar la comunicación entre los distintos equipos. El hardware de comunicaciones era/es estándar y generalmente presentaba pocos problemas.

Sin embargo, cuando la comunicación debía realizarse entre equipos heterogéneos (equipos de diferentes fabricantes o modelos), el esfuerzo en el desarrollo software se convertía en una auténtica pesadilla, ya que cada fabricante utilizaba diferentes formatos de datos o convenciones para su intercambio. Este tipo de situaciones podían darse incluso entre equipos de un mismo fabricante.

Conforme el uso de comunicaciones y redes de ordenadores iba afianzándose, empezaba a ser excesivamente costoso el desarrollo de un software específico de comunicaciones para cada escenario concreto, por lo que la única alternativa viable para los fabricantes de computadores fue implementar y adoptar un conjunto común de convenciones para datos y el intercambio de los mismos.

Para realizar este propósito, se debieron promulgar una serie de estándares internacionales por las organizaciones apropiadas para ello. Estos estándares[2] tuvieron dos efectos notables:

- Los fabricantes se sintieron alentados a implementar dichos estándares ya que sus productos sería menos atractivos en el mercado en el caso

[1] Este capítulo está basado en los trabajos [14] y [15]

[2] Es importante remarcar, que en todo este proceso fue necesario más de un único estándar.

de no implementarlos.

- Los consumidores se encontraron en posición de requerir a los fabricantes la implementación de dichos estándares para comprar y utilizar sus productos.

La labor de comunicar de forma completamente cooperativa aplicaciones en ejecución en diferentes computadores es demasiado compleja para ser manejada como un único problema. El problema debe ser descompuesto en unas partes o subproblemas más manejables, aplicando la filosofía del *divide y vencerás*. Por lo tanto, antes de desarrollar estándares, debería ser necesaria una estructura o arquitectura que define las diferentes subtareas o problemas necesarios a resolver en la tarea compleja de comunicar dos o más sistemas informáticos.

Esta línea de razonamiento llevó a la International Organization for Standardization (ISO) en 1977 a establecer un subcomité para desarrollar tal arquitectura. El resultado final fue la definición del modelo de Referencia para la Interconexión de Sistemas Abiertos (Open Systems Interconnection Reference Model), comúnmente conocido como Modelo de Referencia OSI, el cual proporciona un marco para la definición de estándares para la interconexión de computadores heterogéneos. El modelo OSI provee de las bases necesarias para la conexión de sistemas abiertos para aplicaciones distribuidas. El término abierto denota la capacidad de dos sistemas cualesquiera conformes al modelo de referencia y a los estándares definidos para su interconexión.

C.2. Conceptos

Una técnica de estructuración ampliamente aceptada, y la seleccionada finalmente por la ISO, fue la división en un modelo de capas. Las funciones de comunicación son repartidas en un conjunto vertical de capas. Cada capa realiza un subconjunto relacionado de funciones requeridas para comunicar con otro sistema. las capas se apoyan en las capas inferiores para la realización de labores de comunicación más primitivas, desentendiéndose de los detalles de dichas funciones. A su vez, las capas proporcionan servicios a las capas superiores. De una manera ideal, las capas deben ser definidas de manera que un cambio en el interior de una capa no afecte al resto de capas. De esta manera, dividiendo el problema en capas, hemos dividido el problema original de comunicaciones en varios subproblemas.

El trabajó del subcomité de la ISO fue definir un conjunto de capas y de servicios asociados a cada capa. Dicho reparto debía agrupar funciones relacionadas lógicamente y tener un número de capas suficiente, de manera

que cada capa individual fuera de un tamaño manejable pero que no sobrecargue el sistema con un número excesivo de capas.

Las características globales del modelo de capas OSI se pueden resumir:

- Cada sistema de comunicaciones se estructura en niveles o capas sucesivas.
- Cada capa utiliza los servicios de comunicaciones de la capa inmediatamente inferior y ofrece servicios a la capa inmediatamente superior. Los servicios se prestan a tráves de unos puntos de acceso al servicio (Service Access Point, SAP).
- La frontera o interfaz entre cada dos niveles, que contiene a los puntos de acceso anteriores, está perfectamente delimitada en términos de primitivas, que definen totalmente el servicio utilizado.
- Una capa se descompone en módulos especializados o entidades.
- Para ofrecer un servicio, las entidades residentes en una capa colaboran (intercambian datos) con las entidades gemelas residentes en otros sistemas.

Hemos comentado que las entidades residentes en una capa proporcionan un determinado servicio a la capa inmediatamente superior, y ese servicio se define mediante unas primitivas. La comunicación entre capas contiguas y residentes en el mismo sistema se lleva a cabo utilizando esas primitivas. Las comunicaciones suelen representarse en gráficas verticales, existiendo sólo cuatro tipos básicos de primitivas:

- *Primitiva de Petición (Request)*, mediante la cual la capa usuaria solicita o invoca una función de la capa proveedora.
- *Primitiva de Indicación (Indication)*, utilizada por la capa proveedora para invocar una función o notificar que una función ha sido invocada.
- *Primitiva de Respuesta (Response)*, utilizada por la capa usuaria para completar la función invocada mediante una primitiva de indicación previa.
- *Primitiva de Confirmación (Confirmation)*, mediante la cual la capa proveedora indica que una función invocada previamente ha sido completada.

Cualquier tipo de servicio puede definirse combinando primitivas de esos cuatro tipos básicos. Para poder abarcar todas las particularidades que pueden presentar distintos servicios, estas primitivas contienen, además, un conjunto de parámetros que dependerán del servicio concreto. La relación entre

servicio y protocolo es inmediata: para cada invocación de una primitiva en el interfaz entre la capa N y la N+1, se producirá un intercambio de una o varias PDUs de la capa N.

En este punto, podemos dar una definición de **servicio** como *aquello que ofrece una capa a la superior dentro de un sistema, a través del SAP mediante el uso de primitivas.*

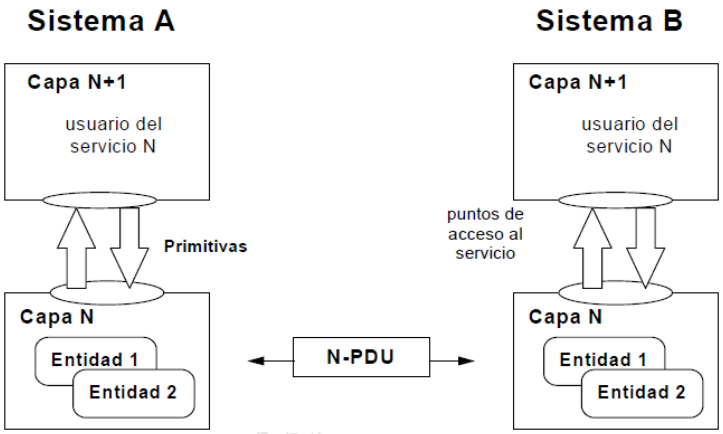

Figura C.1: Nomenclaturas y conceptos modelo OSI

La comunicación entre sistemas, se logra teniendo las correspondientes capas pares en los sistemas a comunicar[3]. Esta comunicación entre entidades pares se realiza mediante el paso de mensajes denominados Protocol Data Units (PDUs). Tanto la información a compartir como la información de control necesitan utilizar el mismo medio físico. Para ello y según la información va a travesando, en sentido descendente, las distintas capas del modelo, se van añadiendo encabezamientos sucesivos que contienen esta información de control. El conjunto resultante se transmite por el canal, que en el sistema receptor seguirá el proceso inverso.

Cada encabezamiento será utilizado sólo por la capa receptora del mismo nivel de la arquitectura y sera eliminado después. El utilizar la información de control de capas superiores constituye una violación del modelo, ya que compromete la evolución separada de las distintas capas.

Las capas pares se comunican por siguiendo un conjunto de reglas o convenciones llamadas protocolos. Se define pues un **protocolo** como el *conjunto de reglas que rige el intercambio de PDUs entre entidades pares de distintos sistemas.* Los elementos clave dentro de un protocolo son:

- *Sintaxis:* incluyendo formatos de datos y niveles de señal.

[3]Primera ley de la telemática: *las torres de protocolos deben ser simétricas.*

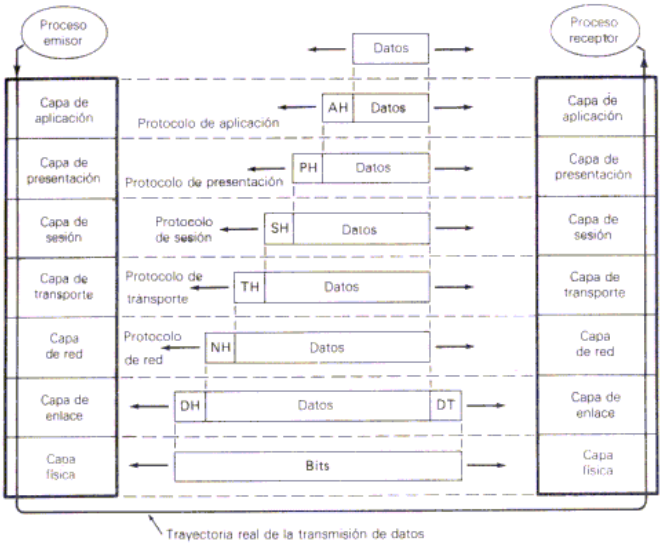

Figura C.2: Modo Operación modelo OSI

- *Semántica:* incluyendo información de control para la coordinación y el manejo de errores.
- *Sincronización:* incluyendo ajuste de velocidades y secuenciación.

La tabla C.1 recoge las 7 capas que fueron finalmente definidas y recoge en términos generales las funciones asociadas a cada capa o nivel. Por lo tanto, todo sistema que quiera intercomunicarse con otro debe implementar dichas funciones, que evidentemente también deben ser implementadas en el otro sistema.

C.3. Capas

C.3.1. Capa Física

La capa física cubre la interfaz física entre dispositivos y las reglas mediante los cuales son traspasados ente ellos. La capa física tiene cuatro características importantes:

- Mecánica.
- Eléctrica.
- Funcional.
- Procedimiento.

Capa	Definición
1. Física	Relacionado con la transmisión de un flujo de bits sin estructura sobre un enlace físico, e.d., envuelve parámetros como niveles de tensión, tiempo y detección de bits, etc. Trata con las características mecánicas y eléctricas para establecer, mantener y desactivar un enlace físico.
2. Enlace	Proporciona transferencia fiable de datos a través de un enlace físico no fiable. Envía bloques de datos (TRAMAS) encargándose de la sincronización, control de errores y control de flujo.
3. Red	Proporciona los medios funcionales y de procedimiento de transferencia de datos de longitud variable (PAQUETES) entre equipos ubicados en redes diferentes. Responsable del establecimiento, mantenimiento y terminación de conexiones.
4. Transporte	Proporciona transferencia fiable y transparente de datos (MENSAJES) entre extremos finales. Proporciona recuperación de errores extremo a extremo y control de flujo.
5. Sesión	Proporciona la estructura de control para comunicaciones entre aplicaciones. Establece, maneja y termina conexiones (sesiones) entre aplicaciones.
6. Presentación	Realiza transformaciones de datos para proporcionar una interfaz de aplicaciones estandarizada y proveer de servicios comunes de comunicaciones tales como encriptado, compresión o formateo.
7. Aplicación	Proporciona servicios a los usuarios de entornos OSI. Ejemplos: servidores de transacciones, protocolo de transferencia de ficheros o gestión de red.

Tabla C.1: Capas del Modelo OSI

Ejemplos de estándares a este nivel son RS-232-C,RS-449/422/423 y algunos aspectos de X.21.

C.3.2. Capa de Enlace de Datos

La capa física provee simplemente de un servicio de flujo bruto de datos binarios. Es sin embargo la capa de enlace, la que consigue que ese enlace físico sea fiable, a la vez que provee los mecanismos para activar, mantener y desactivar el propio enlace de datos.

El principal servicio que la capa de enlace proporciona a las capas superiores es la detección y el control de errores. Por lo tanto, con un nivel funcional de enlace de datos, las capas superiores pueden asumir que existe una transmisión libre de errores de sobre el enlace.

Si los sistemas no están directamente conectados, la situación seguirá igual, pus se tratará de una serie de enlaces fiables conectados y operando de manera independiente, liberando igual que antes a las capas superiores de cualquier responsabilidad en el control de errores.

Ejemplos de estándares a este nivel son HDLC, LAPB, LAPD y LLC.

C.3.3. Capa de Red

El servicio básico que ofrece la capa de red es proporcionar transferencia transparente de datos entre dos entidades de transporte. Libera a la capa de transporte de conocer las tecnologías de transmisión y de conmutación subyacentes utilizadas para conectar los distintos sistemas. El servicio de red es responsable de establecer, mantener y terminar conexiones a través de las facilidades de red que intervengan en el proceso.

Se encarga por tanto de hacer llegar la información suministrada por la capa superior desde un origen a su destino, atravesando tanto sistemas intermedios como subredes, y escogiendo la ruta apropiada a través de ellos si fuera necesario. El servicio puede ser orientado o no a conexión.

Las funciones básicas del nivel de red son pues el direccionamiento, encaminamiento, control de congestión e interconexión de redes.

Estas tres primeras capas ofrecen el servicio de red. Los protocolos que la implantan deberán aparecer en los nodos de la red de comunicaciones.

El mejor ejemplo de protocolo de capa 3 es el estándar X.25.

C.3.4. Capa de Transporte

El propósito de la capa 4 es proveer de un mecanismo fiable para el intercambio de datos entre procesos en diferentes sistemas. La capa de transporte asegura que las unidades de datos son entregadas libres de errores, en secuencia, sin pérdidas ni duplicidades. La capa de transporte puede responsable incluso de la optimización del uso de los servicios de red así como de ofrecer diferentes calidades de servicio a las entidades de sesión.

Por ejemplo, la entidad de sesión puede especificar una tasa de error aceptable por ella, un retraso máximo, prioridad y seguridad, de tal modo que la capa de transporte sirve como coordinador del usuario con las facilidades de comunicación.

El tamaño y la complejidad de un protocolo de transporte depende del tipo de servicio que puede obtener de la capa 3. Para una capa 3 fiable, con capacidades de circuito virtual se requiere una capa 4 mínima. Si la capa 3 no es fiable, el protocolo de capa 4 debe incluir mecanismos intensivos de detección y recuperación de errores. Acorde a esto, la ISO ha definido cinco clases de protocolos de trasporte, cada uno orientado a diferentes servicios y necesidades.

C.3.5. Capa de Sesión

La capa de sesión proporciona el mecanismo para el control de diálogos entre dos entidades de presentación. Como mínimo, la capa de sesión proporciona los medios para dos entidades de presentación puedan establecer y utilizar una conexión, llamada sesión. Además, puede proporcionar los siguientes servicios:

- Tipo diálogo: puede ser un diálogo bidireccional simultáneo, bidireccional alternativo o bien unidireccional.
- Recuperación: la capa de sesión provee un mecanismo de punto de control (checkpoint), por el que si ocurre algún error entre checkpoints, la entidad de sesión puede retransmitir todos los datos desde el último checkpoint.

C.3.6. Capa de Presentación

La capa de presentación ofrece a los procesos de aplicación un conjunto de servicios de transformación de datos. Servicios que esta capa típicamente incluye son:

- Traducción de datos: traducción de código y de conjunto de caracteres.

- Formateo: modificación de formato de datos.
- Selección de sintaxis: selección inicial y subsecuente modificación de la transformación usada.

Ejemplos de protocolos a este nivel son compresión de datos, encriptado y el protocolo de terminal virtual. El protocolo de terminal virtual convierte entre un terminal de características específicas y un modelo virtual genérico utilizado por los procesos de aplicación

C.3.7. Capa de Aplicación

Proporciona medios para que los procesos de aplicaciones puedan acceder al entorno OSI. Esta capa contiene funciones de gestión y generalmente mecanismos útiles para suportar aplicaciones distribuidas.

Ejemplos de estándares a este nivel son el protocolo de ficheros virtuales y el protocolo de transferencia y manipulación de tareas.

Para cerrar el apartado, es interesante intentar encajar algunos protocolos TCP/IP muy conocidos o extendidos ya entre todo tipo de usuarios, dentro del modelo OSI, algo que queda reflejado en la figura C.3, donde vemos como algunos protocolos encajan a la perfección con algún nivel del modelo OSI mientras que otros implementan funciones pertenecientes a diversas capas del mismo.

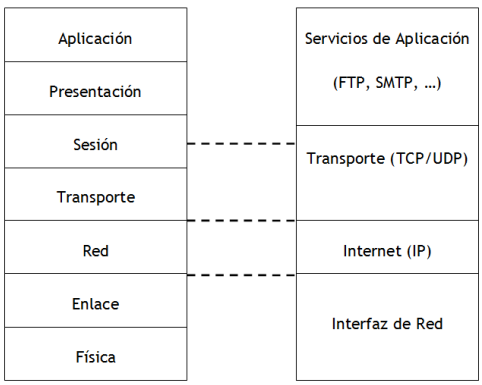

Figura C.3: Protocolos TCP/IP frente modelo OSI

C.4. Perspectivas en el modelo OSI

La figura C.4 nos muestra dos interesantes persepectivas sobre la arquitectura OSI.

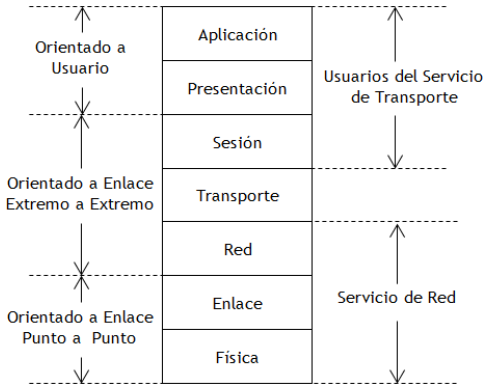

Figura C.4: Perspectivas en el modelo OSI

La notación de la parte derecha de la figura sugiere visualizar las siete capas OSI en tres partes. Las tres capas inferiores de OSI contienen la lógica para que un host pueda interaccionar con la red. Dicho host está conectado físicamente a la red, utiliza un protocolo de enlace de datos para comunicarse de manera fiable con la red y utiliza un protocolo de nivel de red para solicitar intercambio de datos con otro dispositivo conectado a la red así como para solicitar servicios o capacidades a la red, como por ejemplo prioridad. El estándar X.25 encaja en este nivel formado por las tres primeras capas OSI. Siguiendo con el análisis de esta perspectiva, el nivel de transporte proporciona una conexión fiable extremo a extremo, independientemente de las facilidades de red. Finalmente, las tres capas superiores, en conjunto, se encargan del intercambio de datos entre usuarios finales, haciendo uso de una conexión de transporte para transferencia fiable de datos.

La otra perspectiva se sugiere en la notación de la izquierda en la figura. Nuevamente, consideramos un sistema conectado a la red. Las dos capas inferiores tratan con el enlace entre el sistema final y la red. Las tres siguientes se encargan de la transferencia de datos entre distintos sistemas en la red. La capa de red hace uso de las facilidades de red para transferir datos de un sistema a otro; la capa de transporte asegura que la transferencia es fiable y la capa de sesión maneja el flujo de datos sobre una conexión lógica. Finalmente, las dos capas superiores están orientadas a las necesidades de usuario, incluyendo consideraciones a realizar por la aplicación así como a necesidades de formateo de datos.

Apéndice D

Repaso Conceptos Básicos en Telecomunicaciones[1]

Este apartado aún no está correctamente desarrollado. No obstante es muy recomendable y probablemente más que suficiente consultar la referencia [13], concretamente:

- `http://trajano.us.es/~isabel/publicaciones/ARSS/1011/tema2.pdf`
- Apartado 3 de `http://trajano.us.es/~isabel/publicaciones/ARSS/1011/tema1.pdf`.

Se recomienda también el repaso de contenidos relacionados con modelado de tráfico en redes de telecomunicaciones, que pueden encontrar en [7] o repasar los contenidos de la asignatura de quinto curso, Redes de Ordenadores, creo que algunos aún disponibles en `http://trajano.us.es/docencia/RedesDeOrdenadores`.

[1] Este capítulo está basado en los trabajos [13] y [7]

Apéndice E

Protocolos TCP/IP[1]

E.1. Introducción

La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron dos de los primeros en definirse, y que son los más utilizados de la familia.

Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como ARP (Address Resolution Protocol) para la resolución de direcciones, FTP (File Transfer Protocol) para transferencia de archivos, y SMTP (Simple Mail Transfer Protocol) y POP (Post Office Protocol) para correo electrónico, o TELNET para acceder a equipos remotos, entre otros.

TCP/IP se podria considerar la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento.

La familia de protocolos de Internet puede describirse por analogía con el

[1]Este capítulo está basado en una recopilación somera de artículos de Wikipedia. Será mejorado en posteriores revisiones.

modelo OSI (Open System Interconnection), que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel resuelve una serie de tareas relacionadas con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería.

El modelo OSI, en cambio, fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de ordenadores. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa. Sirve de ayuda entender el modelo OSI antes de conocer TCP/IP, ya que se aplican los mismos principios, pero son más fáciles de entender en el modelo OSI.

El protocolo TCP/IP es el sucesor del NCP, con el que inició la operación de ARPANET, y fue presentado por primera vez con los RFCs 791,1 7922 y 7933 en septiembre de 1981. Para noviembre del mismo año se presentó el plan definitivo de transición en el RFC 8014 , y se marcó el 1 de enero de 1983 como el Día Bandera para completar la migración.

E.2. Protocolo IP: Internet Protocol

Internet Protocol (en español Protocolo de Internet) o IP es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos, a través de una red de paquetes conmutados no fiable y de mejor entrega posible sin garantías.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por

ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir («datagramas») supera el tamaño máximo «negociado» (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de como estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en el Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits (lo cual asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670.000 millones de direcciones IP), muchas más direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

Quizás los aspectos más complejos de IP son el **direccionamiento** y el **enrutamiento**. El direccionamiento se refiere a la forma como se asigna una dirección IP y cómo se dividen y se agrupan subredes de equipos.

El **enrutamiento** consiste en encontrar un camino que conecte una red con otra y, aunque es llevado a cabo por todos los equipos, es realizado principalmente por routers, que no son más que computadoras especializadas en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos.

Una **dirección IP** es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo de Internet (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar.

El usuario al conectarse desde su hogar a Internet utiliza una dirección IP. Esta dirección puede cambiar al reconectar. A la posibilidad de cambio de dirección de la IP se denomina dirección IP dinámica. Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (IP fija o IP estática); es decir, no cambia con el tiempo. Los servidores de correo, dns, ftp públicos, servidores web, conviene que tengan una dirección IP fija o estática, ya que de esta forma se facilita su ubicación.

Las máquinas manipulan y jerarquizan la información de forma numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP. Sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar, por ello las direcciones IP pueden utilizar un sinónimo, llamado nombre de dominio (Domain Name), para convertir los nombres de dominio en direcciones IP, se utiliza la resolución de nombres de dominio DNS.

Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

En comunicaciones, el **encaminamiento** (a veces conocido por el anglicismo ruteo o enrutamiento) es el mecanismo por el que en una red los paquetes de información se hacen llegar desde su origen a su destino final, siguiendo un camino o ruta a través de la red. En una red grande o en un conjunto de redes interconectadas el camino a seguir hasta llegar al destino final puede suponer transitar por muchos nodos intermedios.

Asociado al encaminamiento existe el concepto de métrica, que es una medida de lo «bueno» que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, coste, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Si la métrica es el retardo, es mejor un camino cuyo retardo total sea menor que el de otro. Lo ideal en una red es conseguir el encaminamiento óptimo: tener caminos de distancia (o coste, o retardo, o la magnitud que sea, según la métrica) mínimos. Típicamente el encaminamiento es una función implantada en la capa 3 (capa de red) del modelo de referencia OSI.

E.3. Protocolo UDP: User Datagram Protocol

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya es-

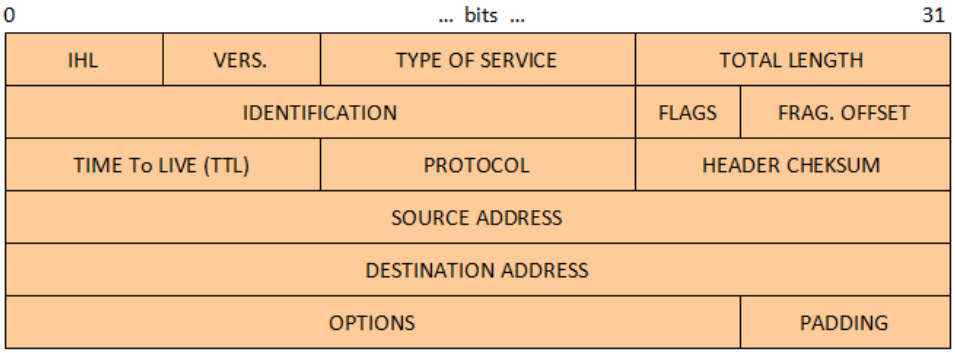

Figura E.1: Formato Cabecera IP V4

tablecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes (por lo que realmente no se debería encontrar en la capa 4) y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y la carga útil. Cualquier tipo de garantías para la transmisión de la información deben ser implementadas en capas superiores.

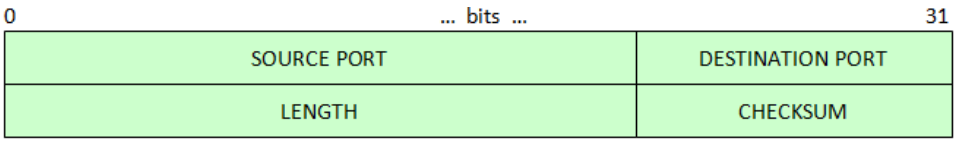

Figura E.2: Formato Cabecera UDP

La cabecera UDP consta de 4 campos de los cuales 2 son opcionales (con fondo rojo en la tabla). Los campos de los puertos fuente y destino son campos de 16 bits que identifican el proceso de origen y recepción. Ya que UDP carece de un servidor de estado y el origen UDP no solicita respuestas,

el puerto origen es opcional. En caso de no ser utilizado, el puerto origen debe ser puesto a cero. A los campos del puerto destino le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes. El campo de la cabecera restante es una suma de comprobación de 16 bits que abarca una pseudo-cabecera IP (con las IP origen y destino, el protocolo y la longitud del paquete UDP), la cabecera UDP, los datos y 0's hasta completar un múltiplo de 16. El checksum también es opcional en IPv4, aunque generalmente se utiliza en la práctica (en IPv6 su uso es obligatorio). A continuación se muestra los campos para el cálculo del checksum en IPv4, marcada en rojo la pseudo-cabecera IP.

bits	0 – 7	8 – 15	16 – 23	24 – 31
0	Dirección Origen			
32	Dirección Destino			
64	Zeros	Protocol	Longitud UDP	
96	Puerto Origen		Puerto Destino	
128	Longitud del Mensaje		Suma de verificación	
160	Datos			

Figura E.3: Checksum en UDP

El protocolo UDP se utiliza por ejemplo cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

UDP utiliza **puertos** para permitir la comunicación entre aplicaciones. El campo de puerto tiene una longitud de 16 bits, por lo que el rango de valores válidos va de 0 a 65.535. El puerto 0 está reservado, pero es un valor permitido como puerto origen si el proceso emisor no espera recibir mensajes como respuesta.
Los puertos 1 a 1023 se llaman puertos «bien conocidos» y en sistemas operativos tipo Unix enlazar con uno de estos puertos requiere acceso como superusuario.

Los puertos 1024 a 49.151 son puertos registrados. Los puertos 49.152 a 65.535 son puertos efímeros y son utilizados como puertos temporales, sobre todo por los clientes al comunicarse con los servidores.

E.4. Protocolo TCP: Transmission Control Protocol

Transmission Control Protocol (en español Protocolo de Control de Transmisión) o TCP, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn. Muchos programas dentro de una red de datos compuesta por computadoras, pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet (navegadores, intercambio de ficheros, clientes FTP, etc.) y protocolos de aplicación HTTP, SMTP, SSH y FTP.

TCP es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte, actualmente documentado por IETF en el RFC 793. Es un protocolo de capa 4 según el modelo OSI.

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe libre de errores, sin pérdidas y con seguridad.

En el nivel de transporte, los paquetes de bits que constituyen las unidades de datos de protocolo TCP se llaman *segmentos*. El formato de las cabeceras de los segmentos TCP se muestra en la figura E.4.

Las conexiones TCP se componen de tres etapas: establecimiento de conexión, transferencia de datos y fin de la conexión. Para establecer la conexión se usa el procedimiento llamado negociación en tres pasos (3-way handshake). Para la desconexión se usa una negociación en cuatro pasos (4-way handshake). Durante el establecimiento de la conexión, se configuran algunos parámetros tales como el número de secuencia con el fin de asegurar la entrega ordenada de los datos y la robustez de la comunicación.

- **Establecimiento de la conexión (negociación en tres pasos o Three-way handshake)**. Aunque es posible que un par de entidades finales comiencen una conexión entre ellas simultáneamente, normal-

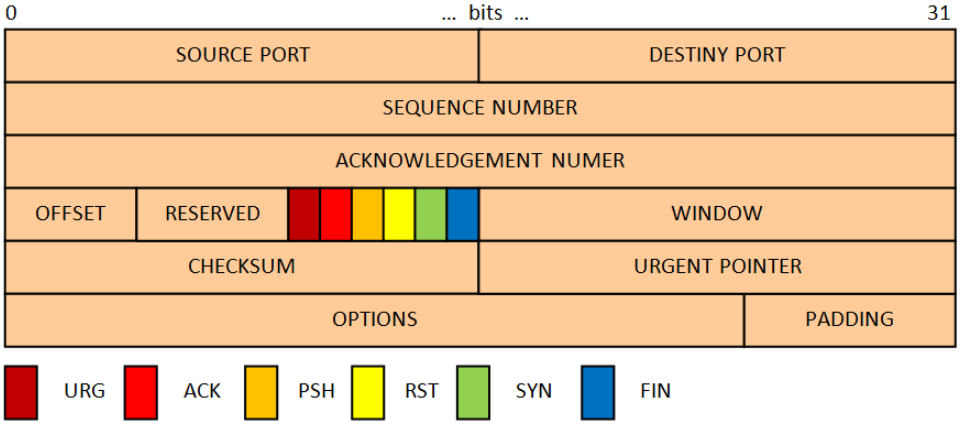

Figura E.4: Segmento TCP

mente una de ellas abre un socket en un determinado puerto TCP y se queda a la escucha de nuevas conexiones. Es común referirse a esto como apertura pasiva, y determina el lado servidor de una conexión. El lado cliente de una conexión realiza una apertura activa de un puerto enviando un paquete SYN inicial al servidor como parte de la negociación en tres pasos. En el lado del servidor se comprueba si el puerto está abierto, es decir, si existe algún proceso escuchando en ese puerto. En caso de no estarlo, se envía al cliente un paquete de respuesta con el bit RST activado, lo que significa el rechazo del intento de conexión. En caso de que sí se encuentre abierto el puerto, el lado servidor respondería a la petición SYN válida con un paquete SYN/ACK. Finalmente, el cliente debería responderle al servidor con un ACK, completando así la negociación en tres pasos (SYN, SYN/ACK y ACK) y la fase de establecimiento de conexión. Es interesante notar que existe un número de secuencia generado por cada lado, ayudando de este modo a que no se puedan establecer conexiones falseadas (spoofing).

- **Transferencia de datos.** Durante la etapa de transferencia de datos, una serie de mecanismos claves determinan la fiabilidad y robustez del protocolo. Entre ellos están incluidos el uso del número de secuencia para ordenar los segmentos TCP recibidos y detectar paquetes duplicados, checksums para detectar errores, y asentimientos y temporizadores para detectar pérdidas y retrasos.

  Durante el establecimiento de conexión TCP, los números iniciales de secuencia son intercambiados entre las dos entidades TCP. Estos números de secuencia son usados para identificar los datos dentro del

flujo de bytes, y poder identificar (y contar) los bytes de los datos de la aplicación. Siempre hay un par de números de secuencia incluidos en todo segmento TCP, referidos al número de secuencia y al número de asentimiento. Un emisor TCP se refiere a su propio número de secuencia cuando habla de número de secuencia, mientras que con el número de asentimiento se refiere al número de secuencia del receptor. Para mantener la fiabilidad, un receptor asiente los segmentos TCP indicando que ha recibido una parte del flujo continuo de bytes. Una mejora de TCP, llamada asentimiento selectivo (SACK, Selective Acknowledgement) permite a un receptor TCP asentir los datos que se han recibido de tal forma que el remitente solo retransmita los segmentos de datos que faltan.

A través del uso de números de secuencia y asentimiento, TCP puede pasar los segmentos recibidos en el orden correcto dentro del flujo de bytes a la aplicación receptora. Los números de secuencia son de 32 bits (sin signo), que vuelve a cero tras el siguiente byte después del 232-1. Una de las claves para mantener la robustez y la seguridad de las conexiones TCP es la selección del número inicial de secuencia (ISN, Initial Sequence Number).

Un checksum de 16 bits, consistente en el complemento a uno de la suma en complemento a uno del contenido de la cabecera y datos del segmento TCP, es calculado por el emisor, e incluido en la transmisión del segmento. Se usa la suma en complemento a uno porque el acarreo final de ese método puede ser calculado en cualquier múltiplo de su tamaño (16-bit, 32-bit, 64-bit...) y el resultado, una vez plegado, será el mismo. El receptor TCP recalcula el checksum sobre las cabeceras y datos recibidos. El complemento es usado para que el receptor no tenga que poner a cero el campo del checksum de la cabecera antes de hacer los cálculos, salvando en algún lugar el valor del checksum recibido; en vez de eso, el receptor simplemente calcula la suma en complemento a uno con el checksum incluido, y el resultado debe ser igual a 0. Si es así, se asume que el segmento ha llegado intacto y sin errores.

Hay que fijarse en que el checksum de TCP también cubre los 96 bit de la cabecera que contiene la dirección origen, la dirección destino, el protocolo y el tamaño TCP. Esto proporciona protección contra paquetes mal dirigidos por errores en las direcciones.

El **checksum de TCP** es una comprobación bastante débil. En niveles de enlace con una alta probabilidad de error de bit quizá requiera

una capacidad adicional de corrección/detección de errores de enlace. Si TCP fuese rediseñado hoy, muy probablemente tendría un código de redundancia cíclica (CRC) para control de errores en vez del actual checksum. La debilidad del checksum está parcialmente compensada por el extendido uso de un CRC en el nivel de enlace, bajo TCP e IP, como el usado en el PPP o en Ethernet. Sin embargo, esto no significa que el checksum de 16 bits es redundante: sorprendentemente, inspecciones sobre el tráfico de Internet han mostrado que son comunes los errores de software y hardware[cita requerida] que introducen errores en los paquetes protegidos con un CRC, y que el checksum de 16 bits de TCP detecta la mayoría de estos errores simples.

Los **asentimientos (ACKs o Acknowledgments)** de los datos enviados o la falta de ellos, son usados por los emisores para interpretar las condiciones de la red entre el emisor y receptor TCP. Unido a los temporizadores, los emisores y receptores TCP pueden alterar el comportamiento del movimiento de datos. TCP usa una serie de mecanismos para conseguir un alto rendimiento y evitar la congestión de la red (la idea es enviar tan rápido como el receptor pueda recibir). Estos mecanismos incluyen el uso de ventana deslizante, que controla que el transmisor mande información dentro de los límites del buffer del receptor, y algoritmos de control de flujo, tales como el algoritmo de Evitación de la Congestión (congestion avoidance), el de comienzo lento (Slow-start), el de retransmisión rápida, el de recuperación rápida (Fast Recovery), y otros.

El **tamaño de la ventana de recepción TCP** es la cantidad de datos recibidos (en bytes) que pueden ser metidos en el buffer de recepción durante la conexión. La entidad emisora puede enviar una cantidad determinada de datos pero antes debe esperar un asentimiento con la actualización del tamaño de ventana por parte del receptor. Un ejemplo sería el siguiente: un receptor comienza con un tamaño de ventana x y recibe y bytes, entonces su tamaño de ventana será (x - y) y el transmisor sólo podrá mandar paquetes con un tamaño máximo de datos de (x - y) bytes. Los siguientes paquetes recibidos seguirán restando tamaño a la ventana de recepción. Esta situación seguirá así hasta que la aplicación receptora recoja los datos del buffer de recepción.

Para una mayor eficiencia en redes de gran ancho de banda, debe ser usado un tamaño de ventana mayor. El campo TCP de tamaño de ventana controla el movimiento de datos y está limitado a 16 bits, es decir, a un tamaño de ventana de 65.535 bytes.

Como el campo de ventana no puede expandirse se usa un factor de escalado. **La escala de ventana TCP** (TCP window scale) es una opción usada para incrementar el máximo tamaño de ventana desde 65.535 bytes, a 1 Gigabyte. La opción de escala de ventana TCP es usada solo durante la negociación en tres pasos que constituye el comienzo de la conexión. El valor de la escala representa el número de bits desplazados a la izquierda de los 16 bits que forman el campo del tamaño de ventana. El valor de la escala puede ir desde 0 (sin desplazamiento) hasta 14. Hay que recordar que un número binario desplazado un bit a la izquierda es como multiplicarlo en base decimal por 2.

- **Cierre de una conexión según el estándar.** La fase de finalización de la conexión usa una negociación en cuatro pasos (four-way handshake), terminando la conexión desde cada lado independientemente. Cuando uno de los dos extremos de la conexión desea parar su "mitad"de conexión transmite un paquete FIN, que el otro interlocutor asentirá con un ACK. Por tanto, una desconexión típica requiere un par de segmentos FIN y ACK desde cada lado de la conexión. Una conexión puede estar "medio abierta.en el caso de que uno de los lados la finalice pero el otro no. El lado que ha dado por finalizada la conexión no puede enviar más datos pero la otra parte si podrá.

TCP usa el concepto de número de puerto para identificar a las aplicaciones emisoras y receptoras. Cada lado de la conexión TCP tiene asociado un número de puerto (de 16 bits sin signo, con lo que existen 65536 puertos posibles) asignado por la aplicación emisora o receptora. Los puertos son clasificados en tres categorías: bien conocidos, registrados y dinámicos/privados. Los puertos bien conocidos son asignados por la Internet Assigned Numbers Authority (IANA), van del 0 al 1023 y son usados normalmente por el sistema o por procesos con privilegios.

Las aplicaciones que usan este tipo de puertos son ejecutadas como servidores y se quedan a la escucha de conexiones. Algunos ejemplos son: FTP (21), SSH (22), Telnet (23), SMTP (25) y HTTP (80). Los puertos registrados son normalmente empleados por las aplicaciones de usuario de forma temporal cuando conectan con los servidores, pero también pueden representar servicios que hayan sido registrados por un tercero (rango de puertos registrados: 1024 al 49151). Los puertos dinámicos/privados también pueden ser usados por las aplicaciones de usuario, pero este caso es menos común. Los puertos dinámicos/privados no tienen significado fuera de la conexión TCP en la que fueron usados (rango de puertos dinámicos/privados: 49152 al 65535, recordemos que el rango total de 2 elevado a la potencia 16, cubre 65536 números, del 0 al 65535).

E.4.1. Desarrollo de TCP

TCP es un protocolo muy desarrollado y complejo. Sin embargo, mientras mejoras significativas han sido propuestas y llevadas a cabo a lo largo de los años, ha conservado las operaciones más básicas sin cambios desde el RFC 793, publicado en 1981. El documento RFC 1122 (Host Requirements for Internet Hosts), especifica el número de requisitos de una implementación del protocolo TCP. El RFC 2581 (Control de Congestión TCP) es uno de los más importantes documentos relativos a TCP de los últimos años, describe nuevos algoritmos para evitar la congestión excesiva. En 2001, el RFC 3168 fue escrito para describir la Notificación de Congestión Explícita (ECN), una forma de eludir la congestión con mecanismos de señalización. En los comienzos del siglo XXI, TCP es usado en el 95 % de todos los paquetes que circulan por Internet. Entre las aplicaciones más comunes que usan TCP están HTTP/HTTPS (World Wide Web), SMTP/POP3/IMAP (correo electrónico) y FTP (transferencia de ficheros). Su amplia extensión ha sido la prueba para los desarrolladores originales de que su creación estaba excepcionalmente bien hecha.

Recientemente, un nuevo algoritmo de control de congestión fue desarrollado y nombrado como FAST TCP (Fast Active queue management Scalable Transmission Control Protocol) por los científicos de Caltech (California Institute of Technology). Es similar a TCP Vegas en cuanto a que ambos detectan la congestión a partir de los retrasos en las colas que sufren los paquetes al ser enviados a su destino. Todavía hay un debate abierto sobre si éste es un síntoma apropiado para el control de la congestión.

E.5. Comparativa UDP - TCP

- **UDP:** proporciona un nivel de transporte no fiable de datagramas, ya que apenas añade la información necesaria para la comunicación extremo a extremo al paquete que envía al nivel inferior. Lo utilizan aplicaciones como NFS (Network File System) y RCP (comando para copiar ficheros entre ordenadores remotos), pero sobre todo se emplea en tareas de control y en la transmisión de audio y vídeo a través de una red. No introduce retardos para establecer una conexión, no mantiene estado de conexión alguno y no realiza seguimiento de estos parámetros.

  Así, un servidor dedicado a una aplicación particular puede soportar más clientes activos cuando la aplicación corre sobre UDP en lugar de sobre TCP.

- **TCP:** es el protocolo que proporciona un transporte fiable de flujo de bits entre aplicaciones. Está pensado para poder enviar grandes cantidades de información de forma fiable, liberando al programador de la dificultad de gestionar la fiabilidad de la conexión (retransmisiones, pérdida de paquetes, orden en el que llegan los paquetes, duplicados de paquetes...) que gestiona el propio protocolo. Pero la complejidad de la gestión de la fiabilidad tiene un coste en eficiencia, ya que para llevar a cabo las gestiones anteriores se tiene que añadir bastante información a los paquetes que enviar. Debido a que los paquetes para enviar tienen un tamaño máximo, cuanta más información añada el protocolo para su gestión, menos información que proviene de la aplicación podrá contener ese paquete (el segmento TCP tiene una sobrecarga de 20 bytes en cada segmento, mientras que UDP solo añade 8 bytes).

  Por eso, cuando es más importante la velocidad que la fiabilidad, se utiliza UDP. En cambio, TCP asegura la recepción en destino de la información para transmitir.

Apéndice F

Ethernet y VLAN 802.1q[1]

F.1. Ethernet

Una de las primeras redes de área local disponible comercialmente fue la denominada Ethernet. Su origen está en una red experimental desarrollada por la empresa Xerox en 1976. En 1980 las empresas Intel y Digital se unen a Xerox y elaboran lo que en 1981 denominarán Libro Azul de la Ethernet versión II. Esta red local es también conocida como Ethernet DXI, por las siglas de las empresas anteriores. En 1982 el grupo de estudio IEEE 802.3 adopta los trabajos de las empresas citadas como punto de partida de la red local 802.3.

La IEEE 802.3 define el subnivel MAC y la capa física de una red local, que en este caso presenta una topología lógica en bus (la topología física puede ser diferente) y un mecanismo de compartición del enlace basado en contienda con escucha y detección de colisión.

La técnica de acceso al medio utilizada es CSMA/CD, es decir, Acceso Múltiple con Escucha y Detección de Colisiones. Utiliza el formato de trama MAC 802.3 es extremadamente simple y se recoge en la figura F.1.

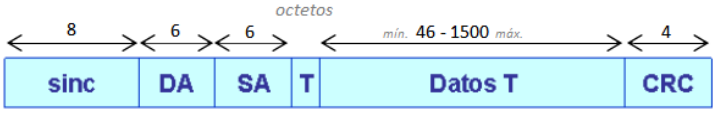

Figura F.1: Formato Trama MAC Ethernet 802.3

Donde el campo sincronismo incluye un preámbulo conocido y un delimitador de comienzo de trama. Las direcciones origen y destino (SA y DA respectivamente) siguen el formato de direcciones IEEE 802.1 de 48 bits,

[1]Este capítulo está basado en los trabajos [16] y [15]

típicamente conocidas como direcciones MAC, como por ejemplo: *00-19-B9-13-BE-D0*.

El campo T o *Ethertype*, de dos octetos de longitud se utiliza para indicar el protocolo encapsulado en la zona de carga de trama Ethernet, aunque también puede ser utilizado para indicar la longitud de los datos de usuario que vienen en el campo siguiente, donde viajan los octetos de nivel superior de forma transparente y cuyo tamaño máximo es de 1500 octetos.

La trama incluye finalmente un código de redundancia cíclica (CRC) de 32 bits para la detección de errores. El receptor sabe que los cuatro últimos octetos que se reciban corresponden al CRC que protegen a toda la parte variable de la trama.

Un **dominio de difusión** es un área lógica en una red de ordenadores en la que cualquier sistema conectado a la red puede transmitir directamente a cualquier otro en el dominio sin precisar ningún dispositivo de encaminamiento, dado que comparten el mismo segmento de red.

Extensiones mediante puentes transparentes o conmutadores permiten extender los dominios de difusión. Para ello se definieron:

- **Puentes Transparentes con Autoaprendizaje (802.1d):** dispositivos que una conectados no necesitan ninguna intervención manual y que además son capaces de transportar sin modificar información multiprotocolo de los niveles superiores al de Enlace. Tienen dos modos de funcionamiento:

  - *Funcionamiento Básico:* o modo promiscuo. Transmite el paquete de datos que le llega por todos los puertos exceptuando aquel por el que llego el paquete, sin realizar ningún tipo de filtrado en función de la dirección.
  - *Autoaprendizaje:* escuchando inicialmente en modo promiscuo, va generando una tabla en la que anota el puerto al que corresponde cada dirección MAC origen cuando recibe un paquete, así va identificando los sistemas conectados a cada puerto. Posteriormente, cuando recibe otro paquete comprueba si la dirección destino se corresponde con alguna entrada de la tabla y en caso afirmativo únicamente retransmite el paquete por el puerto correspondiente. En caso negativo retransmite en modo promiscuo.

  Posteriormente se añadió el modo de funcionamiento de árbol de Expansión Rápido (Rapid Spanning Tree).

- **Árbol de Expansión Rápido (802.1w):** los puentes funcionan bien cuando no hay bucles en la topología, por lo que se dotó a estos sistemas de capacidad para detectar de forma automática la presencia de bucles, generando de forma automática una topología libre de bucles que se denomina *árbol de expansión*. La generación del árbol de expansión se realiza intercambiando unos mensajes de configuración denominados *Configuration Bridge Protocol Data Units (CBPDU)*, que finalmente activará o desactivará algunos puertos de los puentes generando el árbol.

Así, se consiguen los primeros pasos hacia una jerarquía de red, distinguiendo puertos LAN, que determinan un segmento de red y puertos troncales, que unen los distintos puentes. Equipos más modernos permiten técnicas de balanceo de cargas y se definió también la agregación de puertos, o IEEE 802.3ad, es un término que indica el establecimiento de una red de datos que describe cómo utilizar varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, repartiendo el tráfico entre ambos, típicamente utilizado para enlaces troncales.

F.2. VLAN 802.1q

Una VLAN (acrónimo de virtual LAN, red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física.

Son útiles para segmentar el dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4).

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local.

Aunque las más habituales son las VLANs basadas en puertos (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

- **VLAN de nivel 1 (por puerto).** También conocida como *port switching*. Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos.

No permite la movilidad de los usuarios, habría que reconfigurar las VLANs si el usuario se mueve físicamente.

- **VLAN de nivel 2 por direcciones MAC.** Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.

- **VLAN de nivel 2 por tipo de protocolo.** La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...

- **VLAN de nivel 3 por direcciones de subred (subred virtual).** La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLANs.

- **VLAN de niveles superiores.** Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico... La pertencencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día...

- **VLAN por Etiquetado:** el protocolo de etiquetado **IEEE 802.1q** es el más común para el etiquetado de las VLANs. El IEEE 802.1q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde únicamente se añade una etiqueta de 4 octetos de longitud. Dicha etiqueta está compuesta por los siguientes campos:

  - **V:** de longitud 16 bits. Se codifica al valor V=0x8100, indicando así que la trama utiliza un etiquetado 802.1q.
  - **TAG:** campo de 16 bits, repartido en los subcampos:
    - **PRI:** campo de 3 bits utilizado para la asignación de hasta 8 niveles de prioridad.
    - **C:** bit de congestión. Si toma el valor 1 indica que la trama puede descartarse si existe congestión.
    - **VLAN-ID:** Identificador de VLAN. Campo de 12 bits, que permite por tanto la a priori la identificación de 4096 VLANs. Como los valores VLAN-ID=0x000 y VLAN-ID=0xFFF están reservados, tenemos pues 4094 VLANs identificables.

Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con bridges y switches sin capacidad de VLAN. Los puentes 802.1q pueden aceptar tramas sin etiquetar y añadirles etiquetas o rechazarlas.

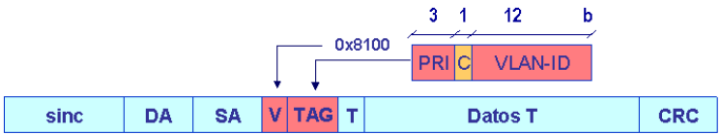

Figura F.2: Formato Trama MAC Ethernet

Se consiguen hasta 8 niveles de prioridad y 4094 VLAN distintas. Veamos como podemos usar la etiqueta 802.1q:

- Para diferenciar VLAN del mismo conmutador sin atender a puertos, protocolos o MACs (ejemplo en F.3).

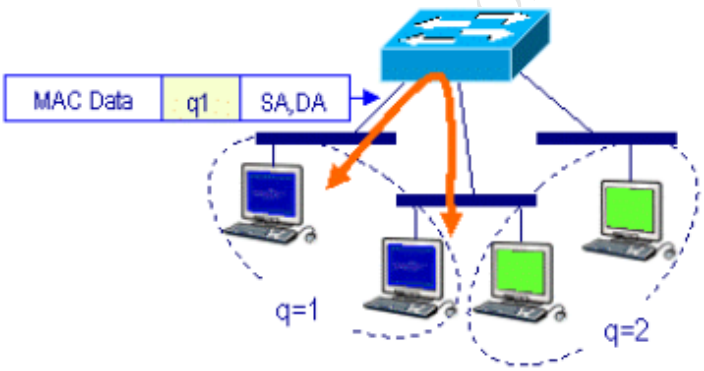

Figura F.3: Usos Etiqueta 802.1q (1)

- Se permite el apilado de etiquetas. Puede parecer MPLS pero las MAC de la trama no cambian (ejemplo en F.4).

- Para interconectar dispositivos de una misma VLAN entre conmutadores (ejemplo en F.5).

Para las comunicaciones entre puentes existen una serie de protocolos estandarizados, entre los que destacan:

- RSTP - Rapid Spanning Tree Protocol(802.1w): protocolo rápido de árbol de expansión que consigue una convergencia más rápida que el inicial STP.

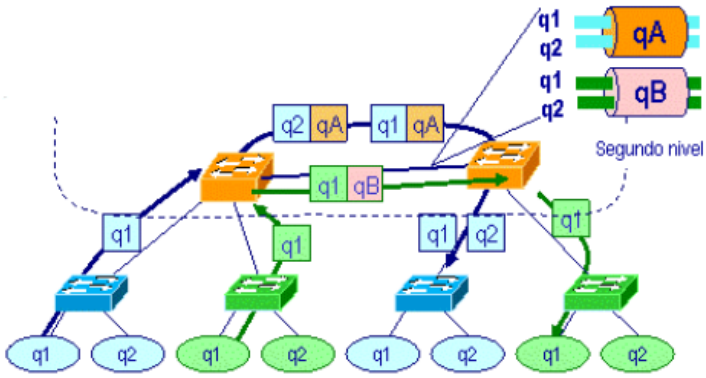

Figura F.4: Usos Etiqueta 802.1q (2)

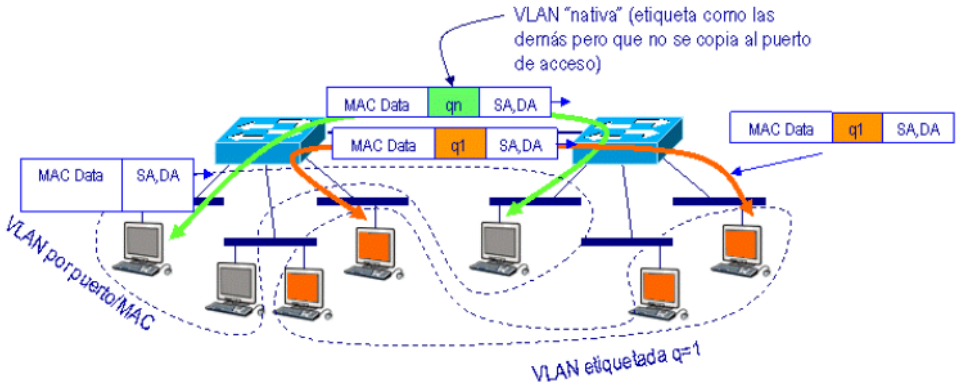

Figura F.5: Usos Etiqueta 802.1q (3)

- GVRP - Generic VLAN Registration Protocol (802.1q Sec 11): protocolo para configuración automática de VLANs. Los puentes deben colaborar para formar las VLANs y deben saber qué puertos pertenecen a cada VLAN. GVRP permite propagar la configuración de manera automática entre los puentes.
- GMRP - GARP[2] Multicast Registration Protocol (GMRP)(802.1q Sec 10): permite a los puentes registrarse y borrarse de los grupos multicast. Las tramas multicast llegarán sólo a los puertos y puentes necesarios (por VID y registro) y no a los puentes que no tengan destinatarios del grupo multicast.

Para finalizar el anexo, recogemos los agentes estandarizadores:

- IEEE: Ethernet y VLAN - `http://www.ieee.org`.
- IETF: Soprote IP - `http://www.ietf.org`.
- ITU: OAM - `http://www.itu.int`.
- MEF: Servicio - `htt://www.metroethernetforum.org`.

Y las principales normativas:

- IETF:
  - RFC 4026 Provider Provisioned Virtual Private Network (VPN) Terminology (Servicios VPN).
  - RFC 3985 Pseudo Wire EMulation Edge-to-Edge (PWE3) Architecture.
  - RFC 4664 Framework for Layer 2 Virtual Private Networks (L2VPN).
  - RFC 4110 Framework for Layer 3 Virtual Private Network (L3VPN).
- IEEE:
  - IEE 802.3 LAN/MAN CSMA/CD Access Method (Ethernet).
  - IEE 802.1q Virtual Bridged Local Area Networks (VLAN).
  - IEE 802.1ad Provider Bridges (QinQ).
  - IEE 802.1ah Provider Backbone Bridges (MinM).

[2]GARP: Generic Attribute Registration Protocol.

Apéndice G

IP Multicast[1]

G.1. Direcciones IP Multicast

IP Multicast es un método para transmitir datagramas IP a un grupo de receptores interesados. El tráfico multicast presenta las siguientes ventajas:

- Facilita el descubrimiento de recursos como por ejemplo routers en una LAN, autoconfiguración con BOOTP o DHCP.
- Se gana en eficiencia, pues se realizan copias en los routers, no en los hosts.

Es importante diferenciar entre broadcast y multicast. La difusión (broadcast) el envío es a todos los usuarios o sistemas mientras que el multicast es un envío únicamente para aquellos que explícitamente deseen recibirlo, por lo que es necesario el uso de un protocolo de gestión de grupos, como es IGMP.

Los servicios basados en multicast tienen una importancia creciente para aplicaciones multimedia, como por ejemplo, difusión de vídeo y audio en tiempo real.

En las redes locales IEEE es sencillo de implementar, pues el medio físico es compartido y se han definido una serie de direcciones especiales, la dirección de difusión (FF:FF:FF:FF:FF:FF.) y la dirección Multicast (01.XX.XX.XX.XX.XX). Inicialmente la interfaz sólo escucha en la dirección de difusión y en la individual propia, pero en cualquier momento se puede solicitar que escuche o envíe a una determinada dirección de multicast.

IP Multicast permite el envío de un datagrama a un grupo de destinos que previamente han solicitado su unión al mismo. Por tanto, para soportar IP multicast es necesario disponer de:

[1]Este capítulo está basado en el trabajo [16]

Figura G.1: Red local IEEE

- Direcciones de multicast: en IPv4 se definieron las direcciones clase D, con el rango 224.0.0.0 a la 239.255.255.255 están destinadas para ser direcciones de multicast.

Figura G.2: IPv4 Direcciones clase D

- Un protocolo de gestión de grupos. Estudiaremos IGMP pero existen otros.
- Routers con capacidad multicast.

El datagrama IP se encapsula en una trama Ethernet multicast. Se realiza una asociación de direcciones IP multicast a direcciones Ethernet multicast, teniendo en cuenta que la asociación no es única, sino que IP debe discriminar en función de las direcciones IP de los datagramas multicast.

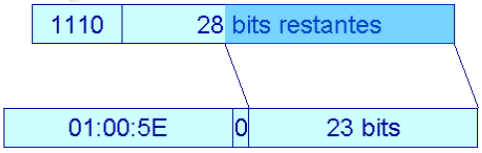

Figura G.3: IP Multicast sobre Ethernet

Se definen tres niveles, según la RFC 1112:

- Nivel 0: equipos finales incapaces de enviar o recibir multicast.
- Nivel 1: equipos finales que sólo envían multicast (asociación de direcciones multicast).
- Nivel 2: equipos finales capaces de enviar y recibir multicast (asociación de direcciones + IGMP).

Existen dos aspectos importantes a tratar para soportar multicast entre redes. Uno es la comunicación entre hosts y routers, que se realiza mediante el protocolo IGMP y por otro lado la comunicación entre routers, que se solventa utilizando protocolos de encaminamiento multicast, como DVMRP, MOSPF, PIM.

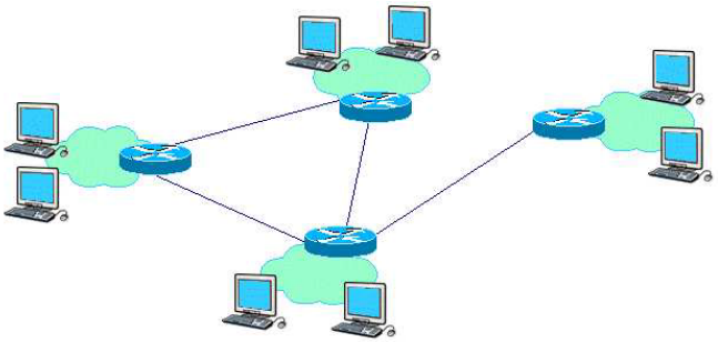

Figura G.4: Multicast entre Redes

Estudiamos finalmente el protocolo IGMP v1/2/3, recogidos en las normas RFC 1112, 2236 y 3376 respectivamente. Internet Group Managemente Protocolo (IGMP) es un protocolo de comunicación entre equipos finales y encaminadores para la gestión de grupos multicast. En los mensajes IGMP se fuerza un TTL=1, con lo cual garantizamos que nunca salimos de nuestro dominio de difusión.

Debe quedar claro que IGMP no es un protocolo de encaminamiento. Los principales mensajes IGMP, encapsulados sobre IP, son:

- JOIN: Petición al encaminador de unión al grupo.
- LEAVE: petición al encaminador de abandono del grupo.
- MEMBERSHIP QUERY: consulta del encaminador de pertenencia al grupo.
- MEMBERSHIP REPORT: respuesta al encaminador de pertenencia al grupo.

El modo de funcionamiento básico es sencillo:

- El host envía IGMP tipo 1 cuando quiere recibir de un grupo.
- El router envía IGMP tipo 2 periódicamente para mantener sus tablas de asociación a grupos.
- El host devuelve un IGMP tipo 1 por cada grupo al que está asociado.
- El host no informa cuando abandona un grupo, simplemente deja de contestar.

Respecto a los protocolos de encaminamiento multicast comentar que facilitan la comunicación entre encaminadores, permitiendo el intercambio sobre grupos y el cálculo de árboles de encaminamiento para cada grupo.

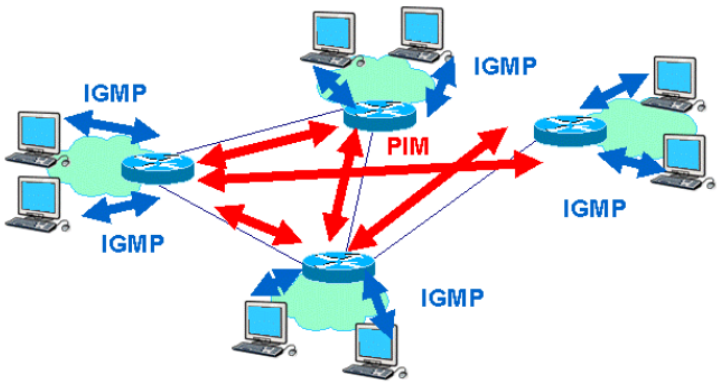

Figura G.5: Encaminamiento multicast

ACRÓNIMOS

3G	Third Generation
3GPP	Third Generation Partnership Project
ADM	Add and Drop Multiplexers
ADSL	Asymmetric Digital Subscriber Line
APON	ATM Passive Optical Network
ATM	Asynchronous Transfer Mode
ATO	Analog Turn-off
B-PON	Broadband PON
BRAN	Broadband Radio Access Network
CAMEL	Customised Applications for Mobile networks Enhanced Logic
CAP	Camel Application Part
CAS	Channel Associated Signalling
CATV	Community Antenna TV
CCS	Common Channel Signalling
CDMA	Code Division Multiple Access
CEPT	Conferencia Europea de Administraciones de Correos y Telecomunicaciones
CLEC	Competitive Local Exchange Carrier (compañías telefónicas alternativas)
CM	Cable Modem
CMTS	Cable Modem Termination System
CMT	Comisión del Mercado de Telecomunicaciones
CNAF	Cuadro Nacional de Atribución de Frecuencias
COFDM	Coded OFDM
CWDM	Coarse WDM
DCT	Discrete Cosine Transform
DOCSIS	Data over Cable System Interface Specification
DPCM	Differential Pulse Code Modulation
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Video Broadcast
DVB-RCS	DVB Return Channel by Satellite
DVD	Digital Versatile Disc
DWDM	Dense WDM
ECTA	Asociación Europea de Telecomunicaciones Competitivas
EFM	Ethernet First Mile (Ethernet en la 1ª Milla)
EPG	Electronic Program Guide
EPON	Ethernet Passive Optical Network
ES	Elementary Stream
ESCON	Enterprise System Connection

ETSI	Instituto Europeo de Estándares de Telecomunicaciones
FAW	Frame Alignment Word
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEXT	Far End Crosstalk
FFT	Fast Fourier Transform
FICON	Fiber Connectivity
FOM	Fiber Optic Modem
FR	Frame Relay
FSAN	Full Service Access Network
FSO	Free Space Optics
FTTB	Fiber to the Building
FTTC	Fiber to the Curb
FTTH	Fiber to the Home
FTTO	Fiber to the Office
FTTX	Fiber to the X
GEO	Geoestacionario
GMPCS	Global Mobile Personal Communications by Satellite
GOP	Group of Pictures
GPRS	General Packet Radio Service
HCX	Head-end Channel Switch
HDSL	High-speed Digital Subscriber Line
HEC	Header Error Control
HFC	Hybrid Fiber Coax
HFR	Hybrid Fiber Radio
HiperLAN	High Performance Radio LAN
ILEC	Incumbent Local Exchange Carrier (compañías telefónicas dominantes)
INAP	Intelligent Network Application Part
IRD	Integrated Receiver-Decoder
ISDN	Integrated Services Digital Network (RDSI)
ISUP	ISDN User Part
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LEO	Low Earth Orbit
LMDS	Local Multipoint Distribution Service
LOS	Line of Sight
MAC	Medium Access Control
MAN	Metropolitan Area Network
MDF	Main Distribution Frame
MEO	Medium Earth Orbit
MHP	Multimedia Home Platform
MFN	Multi Frequency Network
MMDS	Multichannel Multipoint Distribution Service
MPEG	Moving Picture Experts Group

MSS	Mobile Satellite Service
MTP	Message Transfer Part
NEXT	Near End Crosstalk
NLOS	Non Line of Sight
NT	Network Termination
NVoD	Near VoD
OFDM	Orthogonal Frequency Division Multiplexing
OLT	Optical Line Termination
ONT	Optical Network Termination
ONU	Optical Network Unit
PAL	Phase Alternation Line
PDH	Plesiochronous Digital Hierarchy
PES	Packetized Elementary Streams
PLC	Power Line Communications
PMD	Physical Medium Dependent
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PTNTDT	Plan Técnico Nacional de Televisión Digital Terrenal
PTR	Punto de Terminación de Red
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature-Phase-Shift Keying
RLC	Run Length Code
RPR	Resilient Packet Ring
RTC	Red Telefónica Conmutada
RDI	Red Digital Integrada
RDSI	Red Digital de Servicios Integrada
SCP	Service Control Point
SCCP	Signaling Connection Control Part
SDH	Synchronous Digital Hierarchy
SDI	Serial Digital Interface
SFN	Single Frequency Network
SHDSL	Symmetric High-speed Digital Subscriber Line
SNI	Service Node Interface
SOH	Section Overheads
SONET	Synchronous Optical Network
SPC	Stored Program Control
SRP	Spatial Reuse Protocol
STM-1	Synchronous Transport Module 1
TC	Transmission Convergence
TCAP	Transaction Capabilities Application Part
TDD	Time Division Duplex
TDT	Televisión Digital Terrestre
TRAC	Telefonía Rural de Acceso Celular

TS	Transport Stream
TU	Tributary Unit
TUP	Telephone User Part
UIT	Unión Internacional de Telecomunicaciones
UMTS	Universal Mobile Telecommunication System
UNII	Unlicensed National Information Infrastructure
UTECA	Unión de Televisiones Comerciales Asociadas
UWB	Ultra Wide Band
VC	Virtual Container
VDSL	Very high-speed Digital Subscriber Line
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
VT	Virtual Tributary
WCDMA	Wideband CDMA
WDM	Wavelength Division Multiplexing
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WLL	Wireless Local Loop
xDSL	Digital Subscriber Line

Bibliografía

[1] *Internet Request for Comments (RFC).* Internet Engineering Task Force (IETF), 2007. [Online]. Available: http://www.rfc-archive.org/

[2] P. Bhatnagar, *Engineering networks for synchronization CCS7, and ISDN: Standards, protocols, planning, and testing.* New York IEEE, 1997.

[3] M. Canalis, *MPLS Multi Protocol Label Switching: Una Arquitectura de Backbone para la Internet del Siglo XXI*, 2003. [Online]. Available: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/libmpls.PDF

[4] L. De Ghein, *MPLS Fundamentals.* Cisco Press, 2006.

[5] B. Douskalis, *IP telephony: the integration of Robust VOIP Services.* Prentice Hall, 2000.

[6] L. Dryburgh and J. Hewett, *Signaling System No. 7 (SS7/C7): protocol, architecture, and services.* Cisco Press, 2005.

[7] J. Flood, *Telecommunications switching, Traffic and Networks.* Prentice-Hall, 1999.

[8] J. Guichard and I. Pepelnjak, *MPLS and VPN architectures.* Cisco Press, 2006.

[9] G. D. Hellberg, C. and T. Boyes, *Broadband network architectures: designing and deploying triple-play services.* Prentice Hall, 2007.

[10] S. Kasera, *ATM networks: concepts and protocols.* McGraw-Hill, 2007.

[11] B. C. J. Madinabeitia, G. and Col., *Redes de acceso de banda ancha: arquitectura, prestaciones, servicios y evolución.* Madrid: Ministerio de Ciencia y Tecnología, Centro de Publicaciones, D.L., 2009.

[12] F. Redmill and A. Valdar, *SPC Digital Telephone Exchanges.* Stevenage, U. K. Peter Peregrinus, 1995.

[13] I. Román and R. Estepa, *Apuntes de la asignatura Arquitectura de Redes, Sistemas y Servicios.* Área de Ingenieríaa Telemática, Universidad de Sevilla, 2010. [Online]. Available: http://trajano.us.es/~isabel/arquitectura.html#Documentacion

[14] W. Stallings, *ISDN and broadband ISDN with frame relay and ATM.* Prentice Hall, 1995.

[15] J. Vozmediano, *Notas Complementarias de la Asignatura Redes de Ordenadores.* Área de Ingeniería Telemática, Universidad de Sevilla.

[16] J. Vozmediano and A. Lara, *Transparencias de Clase.* Área de Ingeniería Telemática, Universidad de Sevilla. [Online]. Available: http://trajano.us.es/docencia/Conmutacion/