Concepto de IP en las nuevas redes Integradas

INTEGRANTES

ING. CARDOZO F. JOEL

C.I.: 6.682.161

CARACAS, MARZO 2006

UNIVERSIDAD CENTRAL DE VENEZUELA

FACULTAD DE INGENIERIA ELECTRICA

S.C.A.D.A.(ESPECIALIZACION)

SISTEMAS DE TELECOMUNICACIONES

INDICE

OBJETIVO

El trabajo será complementario a lo visto en clase y permitirá al estudiante entender como se está comenzando aplicar el concepto de IP en las nuevas redes integradas desde el punto de vista del manejo de la voz en centros de conmutación Cx públicos y privados, hacia el nuevo concepto de redes integradas universales. Desde el punto de vista público, la tradicional red PSTN en conjunto con las redes de CxP, están siendo integradas hacia un nuevo concepto de redes de próxima generación.

INTRODUCCIÓN

Uno de los desafíos más importantes de lo que se supone constituirán la nueva generación de redes IP en esta investigación, será la provisión de servicios de multiconferencia multimedia y los diferentes protocolos a emplear. Además de la introducción de nuevos servicios, Con esta idea, aparte de tener que tratar los problemas típicos asociados a los servicios en tiempo real (como la QoS), debemos tener en cuenta la necesidad de buscar mecanismos de señalización y control que permitan un despliegue eficaz de los servicios suplementarios. Los dos enfoques más prometedores son el conjunto de protocolos que la ITU-T ha desarrollado bajo la denominación de H.323, y la propuesta del lado del IETF: el SIP. Aunque la arquitectura que proponen es muy similar, se pueden encontrar profundas diferencias en su planteamiento. H.323 es la solución más madura, y ha seguido un desarrollo orientado principalmente a la Telefonía IP (TIP), centrándose, por tanto, en la interoperabilidad con la PSTN y el soporte de los servicios suplementarios. SIP se ha desarrollado sin embargo con un objetivo mucho más amplio, centrándose en la provisión del desarrollo de nuevas funcionalidades y servicios que no se vean coartadas en el futuro, es un protocolo pensado para aplicaciones que vayan más allá de la TIP (videoconferencia, streaming de vídeo, mensajería instantánea). Parece claro que se ve venir un periodo de convivencia de ambas soluciones, de manera que nos encontramos con varias iniciativas conjuntas que persiguen un escenario donde la interoperabilidad constituirá un requisito absolutamente imprescindible; todo pensado en un entorno de Comunicación Universal e independiente del medio o dispositivo que se utilice en cada momento para acceder a los servicios.

El objetivo de la investigación es ofrecer una breve descripción de las características generales, motivación y alcance que ha tenido el desarrollo del protocolos H.323, SIP, H.248 ò (Megago), y las redes IP sobre WDM, en el ámbito de las tecnologías relacionadas con las redes y los servicios IP, en pleno escenario de convergencia tecnológica.

Durante el desarrollo de la investigación, se dará una definición de los protocolos y se indicará sobre las características, arquitectura y componentes de los protocolos antes descritos. Se dará una visión general de las posibles aplicaciones de esta tecnología en convergencia; se dará un repaso muy breve a las principales líneas de trabajo y los esfuerzos de estandarización en los frentes de interoperabilidad en un escenario de necesaria convivencia con tecnologías tradicionales.

En esta investigación, no podemos pretender abarcar todo el dinamismo de las tecnologías relacionadas, de manera que cuando se hable de tendencias o líneas de trabajo, e incluso aplicaciones o servicios de esas tecnologías, se plantearan de forma genérica con la única intención de proporcionar una visión lo más amplia posible de la tecnología y el escenario donde se presenta.

La responsabilidad es ahora de los operadores el usar sus existentes redes de fibra para satisfacer lo que el mercado necesita. Desde 1980, SONET/SDH ha cubierto estas necesidades suministrando protección.

Esto mientras soporta una mezcla transparente y flexible de protocolos de tráfico incluido IP, Fiber Channel, Ethernet y GFP. Mientras que el despliegue de las redes WDM (Múltiplexación por división de onda) durante la década siguiente sirvieron para incrementar el ancho de banda de la fibra existente, escasean severamente las capacidades de protección y de gestión inherentes a la tecnología SONET/SDH.

También el desarrollo WDM vino con un nuevo y completo conjunto de Elementos de Red (NE - Network Elements) incluidos amplificadores, conmutadores, multiplexadores y desmultiplexadores ópticos, los cuales introducen un subnivel en la red mereciendo una monitorización constante para garantizar el fallo de tráfico libre.

La meta de la OTN (Optical Transport Network), es combinar los beneficios de la tecnología SONET/SDH con el aumento del ancho de banda del WDM. En pocas palabras, OTN aplicará la funcionalidad de la Operación, Administración, Mantenimiento y Aprovisionamiento del SONET/SDH a las redes ópticas WDM. Este OTN recientemente desarrollada se especifica en la ITU-T G.709 Network Node Interface for Optical Transport Network (OTN). Esta recomendación – a veces referida como Digital Wrapper (DW) – toma la tecnología SONET/SDH de una única longitud de onda como un paso a las redes transparentes gestionables de longitud de onda de muchas longitudes de onda. El FEC (Forward Error Correction) añade una característica adicional a la OTN ofreciendo el potencial para los operadores de red para reducir el número de regeneradores usados lo que a su vez reduce los costes de la red.

CAPITULO 1

INTEGRACIÓN DE IP SOBRE CANALES WDM

1. INTEGRACIÓN DE IP SOBRE CANALES WDM.

El estudio de la integración de IP sobre redes ópticas. Estudiando la encapsulación de los distintos niveles IP sobre los distintos niveles WDM. Analizando la gestión, la funcionalidad y arquitectura de las redes ópticas.

En un principio lo que se quiere exponer el estado actual y el desarrollo futuro de equipos y redes IP, de cómo WDM propone las medidas para implementar estas funciones y mejora la funcionabilidad de las redes.

Con este trabajo se pretende introducir aspectos importantes a tener en cuenta cuando se considera la posibilidad de IP sobre WDM. Provee un buen fondo para cualquiera que trabaje en lo concerniente a la reducción de la cabecera necesaria para el transporte de paquetes IP en canales ópticos. Uno de los aspectos a tratar es la de tener una perspectiva de la capa IP. Mirar lo que está disponible en términos de funcionalidad, software y hardware en la capa IP.

IPv6 es probablemente la mejor elección en las futuras redes IP sobre WDM. Esta investigación, muestra también el desarrollo al que tienden los routers y valorar los router Gigabit, así como estos forman la base para las redes de transporte IP sobre WDM. Algunos cambios en configuraciones de hardware están también identificados, esto es necesario a la hora de hacer routers capaces de manejar paquetes de velocidades de Gigabits, como usar switch en vez de buses. Esto muestra que para clasificar los paquetes IP dentro del flujo y conmutándolos en las capas inferiores en vez de enrutarlos, mirando las tablas de enrutamiento en cada nodo puede reducir significativamente la latencia de la red.

Una técnica de la que hablaremos en particular es MPLS (*Multi Protocol Label Switching*) la cual fue propuesta por la IETF (*Internet Engineering Task Force*) y ya esta implementada en muchos routers. MPLS tiene la ventaja de aliviar el peso de las largas tablas de enrutamiento en los routers y al mismo tiempo soporta la realización de funcionalidades de la red, como VPN (*Virtual Private Network*) y CoS (*Class of Service*). Las técnicas que se necesitan para la integración de la capa IP sobre la capa WDM, dando una visión general de los diferentes métodos de encapsulamiento de los paquetes IP preparándolos para ser transportados en una longitud de onda.

En la adaptación de los paquetes IP sobre WDM se evalúa los diferentes mecanismos de encapsulación de la cantidad de cabecera necesaria para transportar los paquetes IP.

El trabajo muestra algunas de las posibilidades que WDM puede dar en términos de funcionalidad. Tres diferentes posibilidades se puede dar para soportar CoS usando longitudes de onda:

- Mejora en la capacidad de los nodos y por tanto CoS para sobre aprovisionamiento.
- Paso por los routers a través de enrutamiento de longitud de onda así como el decremento del retraso en las redes.
- Uso de longitudes de onda como etiquetas para la clasificación de CoS.

También veremos las diferentes opciones de conexión cruzada y enrutado de los flujos IP la ayuda de las longitudes de onda y por consiguiente obteniendo una menor latencia en la red. En este, se identifican las tendencias predominantes en IP sobre WDM. Estas tendencias discutidas son:

- Routers más rápidos → 2,5 Gb/s de hoy a los 10 Gb/s.
- Aumento del número de longitudes de onda → 32 sistemas de longitudes de onda a 200 sistemas de canal.
- Moviendo el enrutamiento a las capas inferiores y aminorando la latencia de las redes.
- Nuevos protocolos dedicados a adaptar IP sobre WDM.
- Menor conversión de protocolos entre las distintas partes de la red.

1.1. WDM (Múltiplexación por División de Onda).

La tecnología WDM permite transmitir múltiples longitudes de onda en una misma fibra óptica simultáneamente. El rango de longitudes de onda utilizado en la fibra puede ser dividido en varias bandas, Cada uno de estos canales, a distinta longitud de onda, puede transmitir señales de diferentes velocidades y formatos.

WDM, incrementa la capacidad de transmisión en el medio físico (fibra óptica), asignando a las señales ópticas de entrada, específicas frecuencias de luz (longitudes de onda), dentro de una banda de frecuencias inconfundible. Una manera de asemejar esta multiplexación es la transmisión de una estación de radio, en diferentes longitudes de onda sin interferir una con otra (**ver Figura # 1**),

porque cada canal es transmitido a una frecuencia diferente, la que puede seleccionarse desde un sintonizador (Tuner). Otra forma de verlo, es que cada canal corresponde a un diferente color, y varios canales forman un “arco iris”.

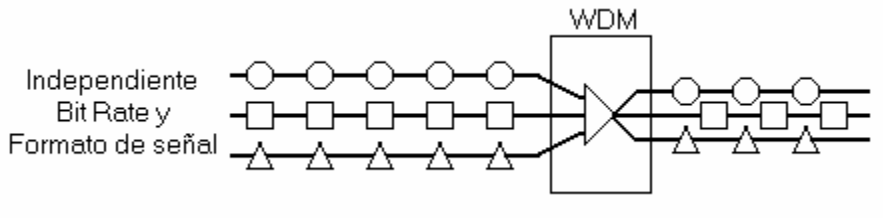


Figura # 1. Incremento de la capacidad con WDM.

En un sistema WDM, cada longitud de onda es enviada a la fibra y las señales son demultiplexadas en el receptor. En este tipo de sistema, cada señal de entrada es independiente de las otras. De esta manera, cada canal tiene su propio ancho de banda dedicado; llegando todas las señales a destino al mismo tiempo.

La gran potencia de transmisión requerida por las altas tasas de bit (Bit Rates) introduce efectos no-lineales que pueden afectar la calidad de las formas de onda de las señales.

La diferencia entre WDM y Dense WDM (DWDM) es fundamentalmente el rango. DWDM espacia las longitudes de onda más estrechamente que WDM, por lo tanto tiene una gran capacidad total. Para sistemas DWDM (Dense Wavelength Division Multiplexing) el intervalo entre canales es igual o menor que 3.2 [nm]. La ITU (International Telecommunication Union) ha estandarizado este espaciamiento, normalizando una mínima separación de longitudes de onda de 100 [GHz] (o 0.8 [nm]), también esta la posibilidad de separación de 200 [GHz] (o 1.6 [nm]) y 400 [GHz] (3.2 [nm]).

Nota: WDM y DWDM utilizan fibra mono-modo para enviar múltiples Lightwaves de diferentes frecuencias. No confundir con una transmisión multi-modo, en la cual la luz es introducida en una fibra a diferentes ángulos, resultando diferentes “modos” de luz. Una sola longitud de onda es usada en transmisión multi-modo.

La principal ventaja de DWDM es que ofrece una capacidad de transmisión prácticamente ilimitada. Aparte del ancho de banda, DWDM ofrece otras ventajas:

- Transparencia. Debido a que DWDM es una arquitectura de capa física, puede soportar transparencia en el formato de señal, tales como ATM, GbE (Gigabit

Ethernet), ESCON, TDM, IP y Fibre Channel, con interfaces abiertas sobre una capa física común. Por lo mismo, puede soportar distintos Bit Rates.

- Escalabilidad. DWDM puede apalancar la abundancia de fibra oscura en redes metropolitanas y empresariales, para rápidamente satisfacer la demanda de capacidad en enlaces punto-a-punto y en tramos de anillos ya existentes.

- Iniciación dinámica. Rápida, simple y abastecimiento dinámico en las conexiones de redes, dada la habilidad de proveedores de proveer servicios de alto ancho de banda en días, antes que en meses.

El auge de la fibra óptica está estrechamente ligado al uso de una región específica del espectro óptico donde la atenuación óptica es baja. Estas regiones, llamadas ventanas, se ubican en áreas de alta absorción. Los primeros sistemas en ser desarrollados operan alrededor de los 850 [nm], la primera ventana en fibra óptica basada en Silica. Una segunda ventana (Banda S), a 1310 [nm], se comprobó que era superior, por el hecho de tener menor atenuación. La tercera ventana (Banda C), a 1550 [nm], posee la menor pérdida óptica de manera uniforme. Hoy en día, una cuarta ventana (Banda L), cerca de los 1625 [nm], está en bajo desarrollo y en sus primeros usos. Estas cuatro ventanas se pueden observar en el espectro electromagnético mostrado en la **Figura C.2.**

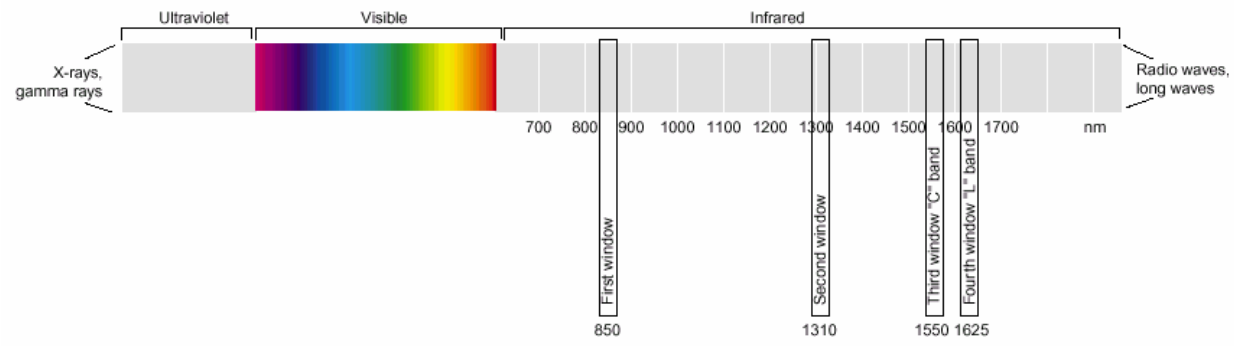


Figura C.2. Espectro Electromagnético.

1.2 Evolución de la tecnología DWDM.

Los primeros comienzos de WDM, a fines de la década de los 80's, utilizaban dos longitudes de onda ampliamente espaciadas en las regiones de los 1310 [nm] y 1550 [nm] (o 850 [nm] y 1310 [nm]), algunas veces llamadas WDM banda ancha (Wideband WDM). A comienzos de los 90's floreció una segunda generación de WDM, algunas veces llamada WDM Banda estrecha (Narrowband WDM), en la cual se

utilizaban entre dos a ocho canales, que estaban separados a intervalos de aproximadamente 400 [GHz] en la ventana de los 1550 [nm]. A mediados de los 90's, emergieron los sistemas DWDM con 16 a 40 canales con una separación entre ellos de 100 [GHz] y 200 [GHz]. A fines de los 90's, los sistemas DWDM evolucionaros, a tal punto que eran capaz de utilizar de 64 a 160 canales paralelos, empaquetados densamente a intervalos de 50 [GHz] y 25 [GHz]. **La Figura C.3** muestra la evolución de esta tecnología, que puede ser vista como un incremento en el número de longitudes de onda acompañada de una disminución en el espaciamiento entre las mismas. Con el crecimiento en la densidad de longitudes de onda, los sistemas también avanzaron en la flexibilidad de configuración, por medio de funciones de subida/bajada (Add/Drop) y capacidades de administración.

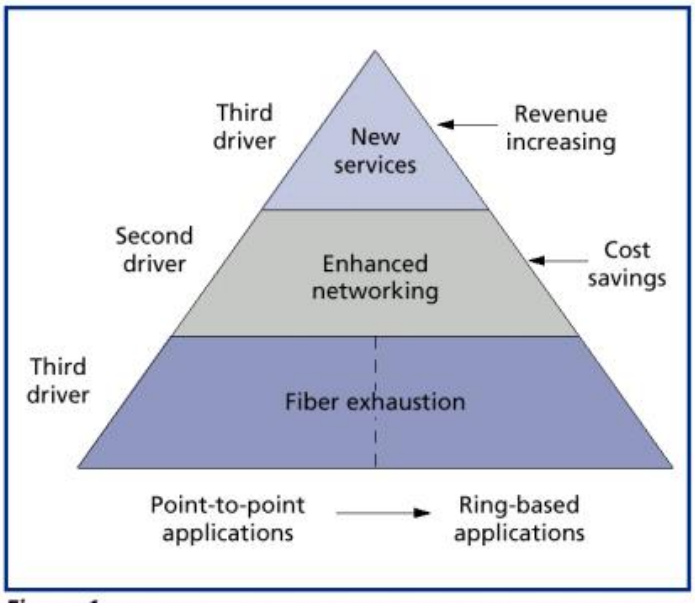


Figura C.3. Evolución de sistemas DWDM.

El incremento de la densidad de canales, como resultado de la tecnología DWDM, tuvo un impacto dramático en la capacidad de transmisión en la fibra. En 1995, cuando los primeros sistemas a 10 [Gbps] fueron demostrados, la tasa de incremento de la capacidad fue de un múltiplo lineal de cuatro cada cuatro años a cuatro cada año (ver Figura C.4).

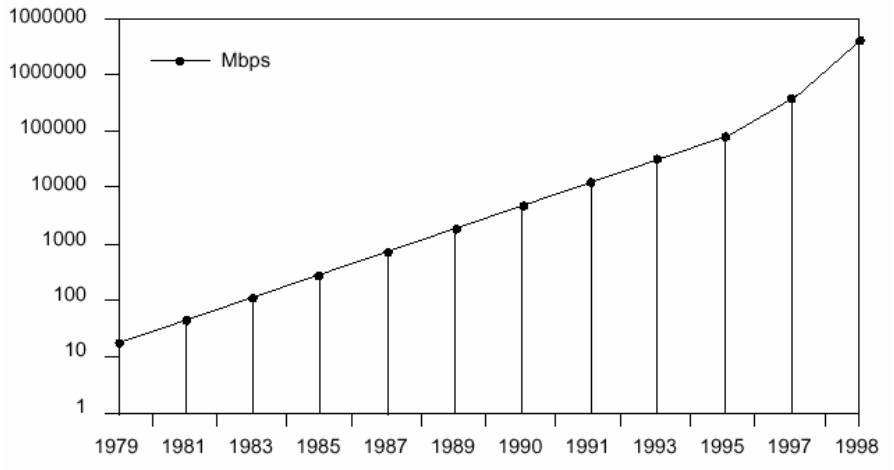


Figura C.4. Crecimiento de la capacidad en la fibra.

"Investigaciones de laboratorio han podido realizar experimentos para transmitir 1022 λ en una misma fibra, sistema denominado Ultra Dense Wavelength Division Multiplexing (UDWDM), con una separación entre canales de 10 [GHz]".

1.3 Funcionamiento de un sistema DWDM.

En su núcleo, DWDM involucra un pequeño número de funciones de capa física. Estas son bosquejadas en la Figura C.5, la que muestra un sistema DWDM de cuatro canales. Cada canal óptico ocupa su propia longitud de onda.

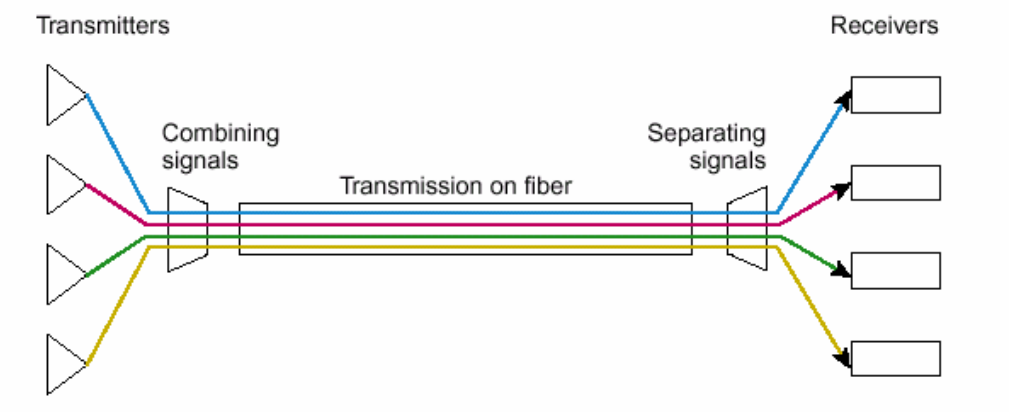


Figura C.5. Esquema funcional DWDM.

El sistema ejecuta las siguientes funciones principales:

- Generación de la señal. La fuente, un láser de estado sólido, puede proveer luz estable con un específico ancho de banda estrecho, que transmite la información digital, modulada por una señal análoga.

- Combinación de señales. Modernos sistemas DWDM emplean multiplexores para combinar las señales. Existe una pérdida asociada con multiplexión y demultiplexión. Esta pérdida es dependiente del número de canales, pero puede ser disminuida con el uso de amplificadores ópticos, los que amplifican todas las longitudes de onda directamente, sin conversión eléctrica.

- Transmisión de señales. Los efectos de Crosstalk y degradación de señal óptica o pérdida pueden ser calculados en una transmisión óptica. Estos efectos pueden ser minimizados controlando algunas variables, tales como: espaciamiento de canales, tolerancia de longitudes de onda, y niveles de potencia del láser. Sobre un enlace de transmisión, la señal puede necesitar ser amplificada ópticamente.

- Separación de señales recibidas. En el receptor, las señales multiplexadas tienen que ser separadas. Aunque esta tarea podría parecer el caso opuesto a la combinación de señales, ésta es hoy, en día, difícil técnicamente.

- Recepción de señales. La señal demultiplexada es recibida por un fotodetector.

Además de estas funciones, un sistema DWDM podría ser equipado con una interfaz Cliente-Equipo para recibir la señal de entrada. Esta función es desempeñada por transpondedores.

1.4 Cambios en la transmisión.

La transmisión de luz en una fibra óptica presenta varios cambios que originan los efectos que se enumeran a continuación:

- Atenuación. Decaimiento de la potencia de la señal, o pérdida en la potencia luminosa, con la propagación de la señal en la fibra.

- Dispersión Cromática. Esparcimiento del pulso luminoso cuando éste viaja por la fibra.

- No-Linealidades. Efectos acumulados por la interacción de la luz con el material a través del cual ésta viaja, resultando en cambios en el lightwave y en interacciones entre lightwaves.

Cada uno de estos efectos se puede deber a una serie de causas, no todas las cuales afectan DWDM. Un estudio detallado de estos fenómenos se realiza en el anexo A: “Conceptos Básicos”.

1.5 Transpondedor, interfaz clave en sistemas DWDM.

Dentro de un sistema DWDM, un transpondedor convierte la señal óptica del equipo terminal en señal eléctrica y desempeña la función 3R (**ver Figura C.6**). Esta señal eléctrica es, por consiguiente, usada para dirigir un láser WDM. Cada transpondedor dentro de un sistema WDM, convierte está señal “cliente” en una longitud de onda levemente diferente. Las longitudes de onda provenientes desde todos los transpondedores de un sistema son entonces multiplexadas ópticamente.

En la dirección del receptor se efectúa el proceso inverso. Las longitudes de onda individuales son filtradas desde la fibra multiplexada y alimentan a un transpondedor individual, el cual convierte la señal óptica en eléctrica y conduce una interfaz estándar hacia el “cliente”.

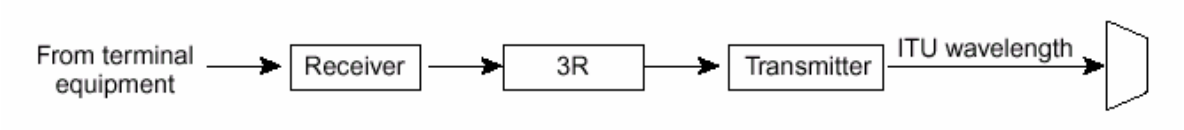


Figura C.6. Función de un transpondedor.

Diseños futuros incluyen interfaces pasivas, las cuales aceptan los estándares de luz de la ITU directamente de un switch o router incluido, con una interfaz óptica.

La operación de un sistema basado en transpondedores se puede explicar considerando la Figura C.7

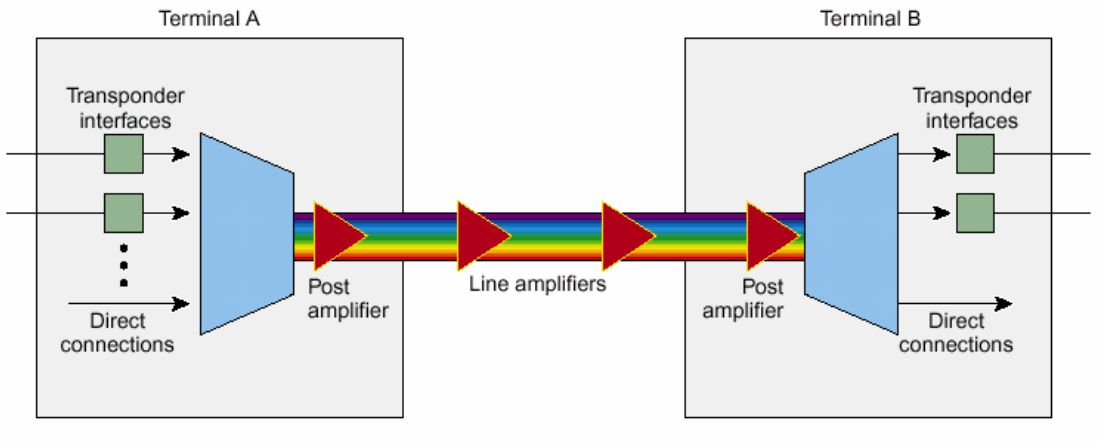


Figura C.7. Esquema de un sistema DWDM.

Los siguientes pasos explican el sistema mostrado en la Figura C.7.

1. El transpondedor acepta entradas en la forma estándar de láser mono-modo o multi-modo. La entrada puede llegar desde diferentes medios físicos, de distintos protocolos y tipos de tráfico.

2. La longitud de onda de cada señal de entrada es identificada a una longitud de onda DWDM.

3. Las longitudes de onda DWDM provenientes del transpondedor son multiplexadas dentro de una sola señal óptica y lanzadas dentro de la fibra. El sistema puede también incluir la habilidad de aceptar señales ópticas directas para ser multiplexadas; tales señales podrían llegar, por ejemplo, de un nodo satelital.

4. Un post-amplificador amplifica la potencia de la señal óptica, del mismo modo que emigra el sistema (opcional).

5. Amplificadores ópticos son utilizados cada cierta distancia de enlace, de ser necesarios (opcional).

6. Un pre-amplificador amplifica la señal antes de que ésta entre en el nodo receptor (opcional).

7. La señal recibida es demultiplexada en lambdas individuales DWDM (o longitudes de onda).

8. Las longitudes de onda individuales DWDM son identificadas para el tipo de salida requerido (por ejemplo, 2.5 [Gbps] fibra mono-modo) y enviadas a través del transpondedor.

1.6 Topologías y esquemas de protección para DWDM.

Las arquitecturas de redes están basadas en muchos factores, incluyendo tipos de aplicaciones y protocolos, distancia, utilización y estructura de acceso, y toplogías de redes anteriores. En el mercado metropolitano, por ejemplo, topologías punto-a-punto pueden ser usadas para conectar puntos de empresas, topología de anillo para

conectar instalaciones Inter.-oficinas (IOFs) y para acceso residencial, y topologías de malla pueden ser usadas para conexiones Inter-POP (Inter Punto-a-punto) y en backbones. En efecto, la capa óptica puede ser capaz de soportar muchas topologías y, puesto al desarrollo impredecible en esta área, estas topologías pueden ser flexibles.

Hoy en día, las principales topologías en uso son la punto-a-punto y anillo.

1.6.1 Topología punto-a punto.

La topología punto-a-punto puede ser implementada con o sin OADMs. Estas redes están caracterizadas por velocidades de canales ultra rápidos (10 a 40 [Gbps]), alta integridad y confiabilidad de la señal, y rápida restauración de trayectoria. En redes long-haul (larga distancia), la distancia entre transmisor y receptor puede ser varios cientos de kilómetros, y el número de amplificadores requeridos entre ambos puntos, es típicamente menor que 10. En redes MANs, los amplificadores no son necesarios frecuentemente.

La protección en topologías punto-a-punto puede ser proveída en una pareja de caminos. En los equipos de primera generación, la redundancia es un nivel del sistema. Líneas paralelas conectan sistemas redundantes a ambos extremos.

En los equipos de segunda generación, la redundancia es al nivel de tarjeta. Líneas paralelas conectan un solo sistema en ambos extremos que contienen transpondedores, multiplexores y CPUs redundantes.

Un esquema de este tipo de topología se puede observar en la Figura C.8

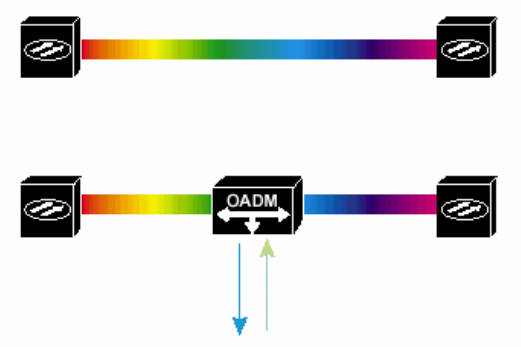


Figura C.8. Topología punto-a-punto.

1.6.2 Topología de anillo.

Los anillos son las arquitecturas más comunes encontradas en áreas metropolitanas y en tramos de unas pocas decenas de kilómetros. La fibra anillo puede contener sólo cuatro canales de longitudes de onda, y típicamente menos nodos que canales. El Bit Rate está en el rango de los 622 [Mbps] a los 10 [Gbps] por canal.

Con el uso de OADMs, los que bajan y suben longitudes de onda en forma transparente, es decir que las otras no se ven afectadas, las arquitecturas de anillo permiten a los nodos tener acceso a los elementos de red, tales como routers, switches y servidores, con la subida y bajada de canales de longitudes de onda en el dominio óptico. Con el incremento en el número de OADMs, la señal está sujeta a pérdidas y se pueden requerir amplificadores.

Para la protección en esta topología se utiliza el esquema 1+1. Se tiene dos líneas de conexión, la información se envía por una de ellas. Si este anillo falla, se switchea la trayectoria al otro anillo. Un esquema de esta topología se puede observar en la Figura C.9.

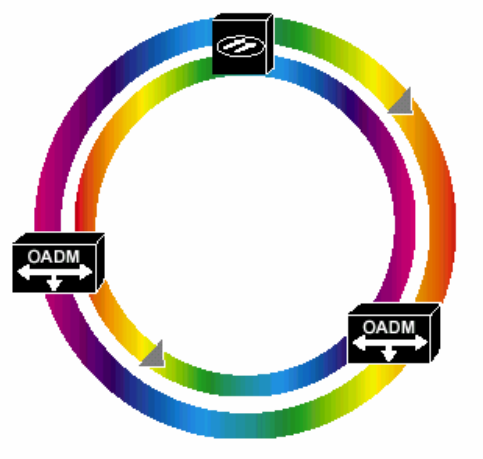


Figura C.9. Topología anillo.

1.6.3 Topología de malla.

La arquitectura de malla es el futuro de redes ópticas. Como las redes evolucionan, las arquitecturas de anillo y punto-a-punto tendrían un lugar, pero la malla sería la topología más robusta. Este desarrollo sería habilitado por la introducción de los OxCs (Optical Cross-Connects) y switches configurables, que en algunos casos reemplazarían, y en otros suplementarian, a los dispositivos DWDM fijos.

A partir del punto de vista del diseño, hay una airosa trayectoria evolutiva de topologías de punto-a-punto y malla. Al comienzo de enlaces punto-a-punto, dotados de nodos OADM al principio para flexibilidad, y posteriormente en las interconexiones, la red puede evolucionar en una malla sin un rediseño completo. Adicionalmente, las topologías de anillo y malla pueden ser conectadas a enlaces punto-a-punto (ver Figura C.10).

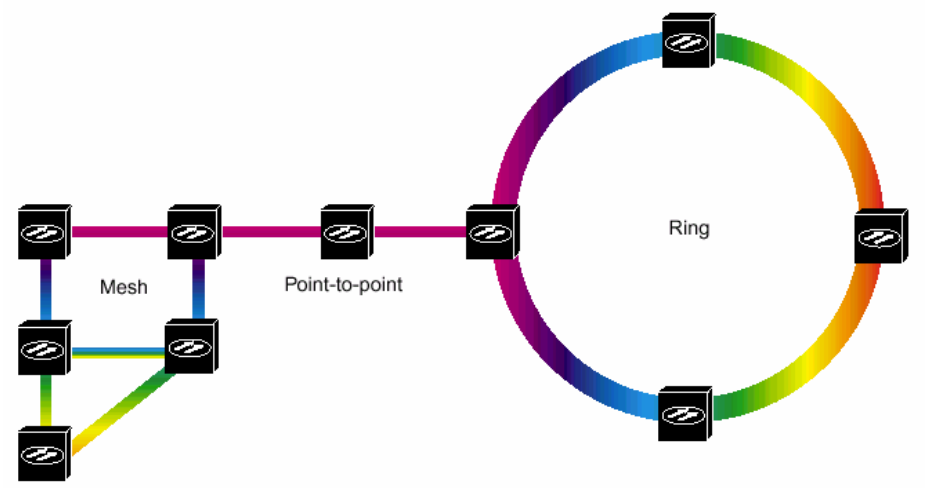


Figura C.10. Arquitecturas malla, punto-a-punto y anillo.

Las redes DWDM tipo malla, consistiendo en nodos totalmente ópticos interconectados, necesitarían de la próxima generación de protección. Donde los esquemas de protección previos están basados en redundancia del sistema, de tarjeta, o al nivel de fibra, la redundancia ocurriría al nivel de longitud de onda. De esta forma, entre otras cosas, un canal de datos podría cambiar de longitud de onda a medida que viaja a través de la red, debido a una falla en el ruteo o switcheo.

Las redes tipo malla, por lo tanto, requerirían de un alto grado de inteligencia para realizar las funciones de protección y administración de ancho de banda, incluyendo a la fibra y al switcheo de longitud de onda. Los beneficios en flexibilidad y eficiencia, realmente, son potencialmente grandes. El uso de fibra, el cual puede ser

bajo en soluciones anillo puesto que requieren de protección de fibra en cada anillo, puede ser mejorado en un diseño de malla. La protección y restauración pueden estar basadas en caminos compartidos, por esta razón se requiere de pocos pares de fibra para la misma cantidad de tráfico y no desperdiciar longitudes de onda sin usar.

1.7.- Descripción y funcionamiento de la WDM.

La multiplexación por división de longitud de onda (WDM), nace para aprovechar de una manera más eficiente y económica los medios ya existentes. La capacidad de transmisión de información se incrementa usando una sola fibra. Con WDM, todos los canales transmiten simultáneamente y utilizan cada uno de ellos todo el ancho de banda del medio de transmisión. Se les asigna una longitud de onda en particular, por medio de un modulador electro – óptico, el cual convierte la señal eléctrica en energía luminosa, con una longitud de onda específica, que se distribuye en forma simultánea en toda la fibra óptica. Para alimentar la energía luminosa a la fibra, se utilizan dispositivos que se les llama distribuidores selectivos de longitudes de onda, éstos tienen aplicación en sistemas de distancias cortas y enlace sin repetidores. Un sistema completo se muestra a continuación

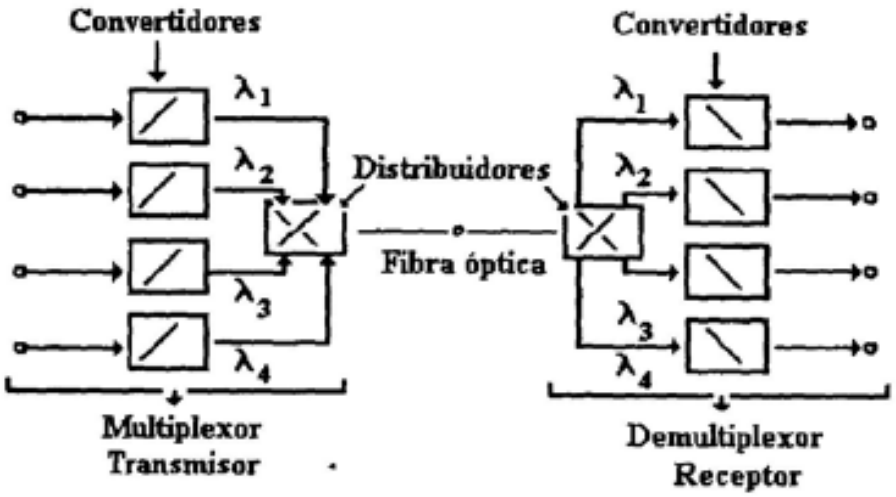


Figura 18.Sistema de transmisión de fibra óptica con WDM

Fuente: Jardón. Sistemas de Comunicaciones por Fibras Ópticas. 1995 Los multiplexores de este tipo pueden ser unidireccionales o bidireccionales. En los WDM unidireccionales, las señales se transmiten en una misma dirección con varios portadores ópticos con diferentes longitudes de onda. Los WDM bidireccionales transmiten la información en dos sentidos sobre la misma fibra, utilizando diferente

longitud de onda en cada sentido. Cada uno de los dispositivos WDM combina señales con una determinada longitud de onda para transmitirlas sobre la fibra, desde luego, también en el receptor se requieren dispositivos que separen estas señales.

Este tipo de sistemas básicamente se forman con:

- Fuentes ópticas: Convierten la señal eléctrica en energía luminosa y la emiten con diferentes longitudes de onda.
- Multiplexores ópticos: combinan la energía luminosa emitida por las fuentes ópticas para alimentar la fibra.
- Medio de transmisión: Esta es la fibra óptica, debe tener una baja atenuación para las longitudes de onda de interés.
- Demultiplexores ópticos: Dispositivos que separan la energía luminosa que le llega a través de la fibra por medio de la longitud de onda.
- Fotodetectores: Este es el elemento que se encarga de hacer la conversión de energía óptica a señal eléctrica. Para esta técnica, básicamente existen tres tipos de multiplexores, los cuales son:
- Los de rejilla de difracción.
- Los de filtros de interferencia
- Los de prisma

Siendo las siguientes las características más importantes que estos dispositivos deben cubrir:

- Bajas pérdidas por inserción
- Baja diafonía
- Facilidad de fabricación
- Fácil adaptación de conectores, para tener una transmisión directa.
- Tamaño pequeño
- Alta confiabilidad

Los más utilizados son los de rejilla y los de interferencia, ya que tienen menor costo y menores pérdidas que los de prisma. La separación de los canales depende del tipo de fuente óptica. Con los LED se tiene una separación de 400 nm y con los láser es de 4 a 50 nm. También se debe de tomar en cuenta la atenuación introducida en los distribuidores, que es normalmente de 0.8 a 1 dB.

1.8. Utilización.

Los sistemas WDM se utilizan en redes locales, en telecomunicaciones de larga distancia (entre troncales), en telecomunicaciones de banda ancha, tales como videoteléfono, video conferencia, TV, audio y otros. Una red de telecomunicaciones que utiliza WDM de tres canales se muestra a continuación.

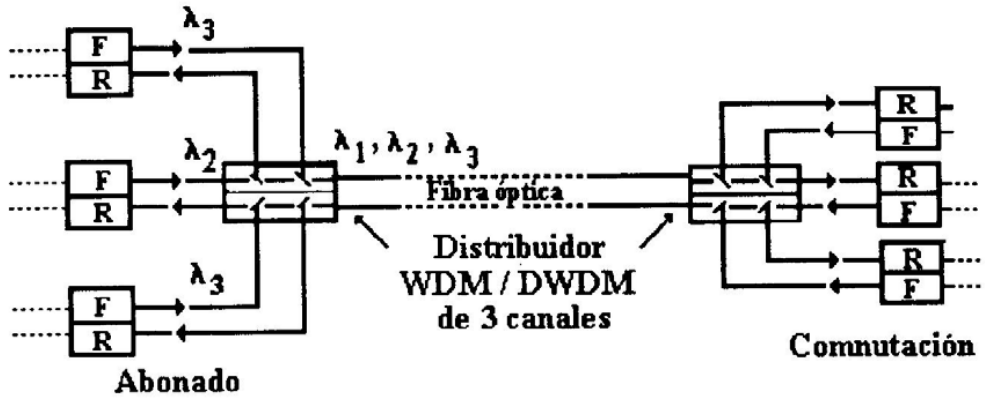


Figura 19.Red de telecomunicaciones de banda ancha que utiliza distribuidores WDM de tres canales

Fuente: Jardón. Sistemas de Comunicaciones por Fibras Ópticas. 1995 A principios de los 90, se denominó transmisión WDM en banda ancha a la transmisión de una señal a 1550nm y otra de retorno a 1310nm. Más tarde, a mitad de los 90, el desarrollo WDM permitía espaciamientos más cortos, implementando transporte bidireccional de 2x2 y 4x4 canales a 1550 nm, alcanzando velocidades de 2,5 Gbps en enlaces punto a punto. Finalmente, a finales de los 90, los sistemas densos (DWDM) llegaron a ser una realidad cuando gran número de servicios y multitud de longitudes de onda comenzaron a coexistir en la misma fibra, llegando a enviar 32/40/64/80/96 longitudes de onda a 2,5 Gbps y 10Gb/s. Aún así, pronto veremos los sistemas ultra-densos (UDWDM) con transmisión de 128 y 256 longitudes de onda a 10Gbps y 40 Gbps por canal, ya que la infraestructura actual de fibra óptica no será suficiente para cubrir la demanda.

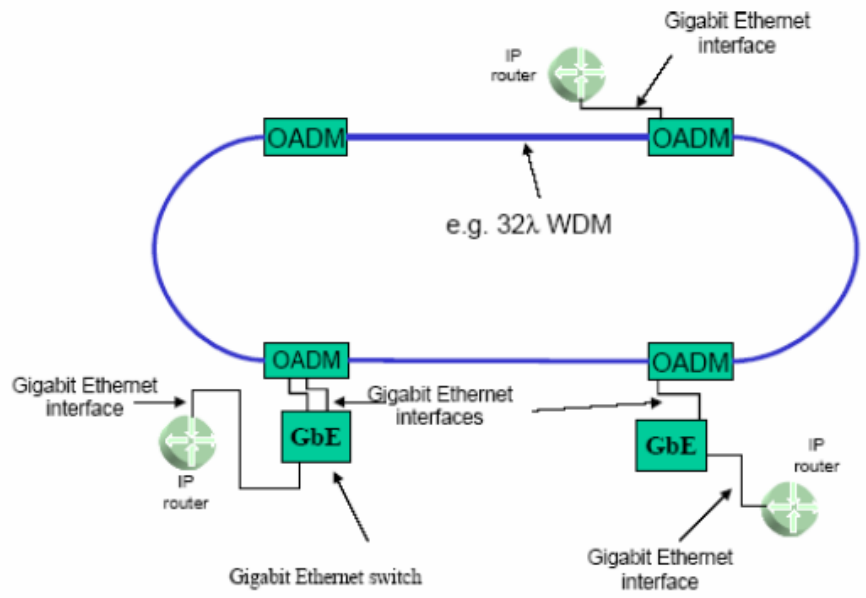


Figura 55. Ejemplo de IP siendo transportada por un anillo WDM

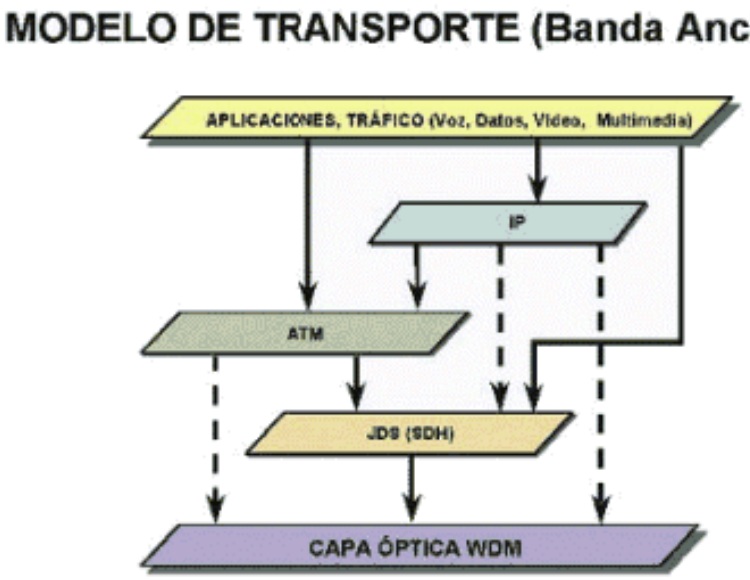
La figura 55 muestra un servicio IP transportado en una red tipo anillo WDM con interfaces de Ethernet de alta velocidad y con amplificadores ópticos (OADM). En un futuro se espera que las redes WDM pasen a ser UDWDM por la amplia demanda de ancho de banda. Se mencionarán a continuación algunas tendencias para WDM y sus variantes.

- IP sobre ATM sobre SDH para transmisiones WDM
- IP sobre ATM directamente en WDM
- IP sobre SDH, Paquetes sobre SONET (POS)
- IP sobre SDL directamente sobre WDM

1.9. CARACTERÍSTICAS GENERALES DE LA WDM.

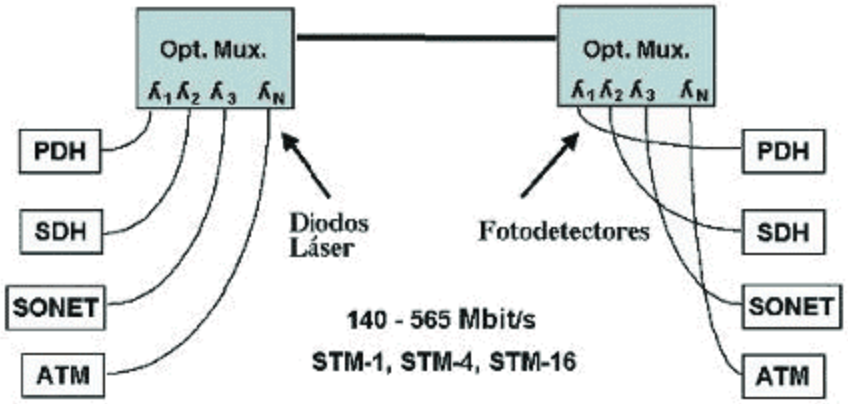
Los sistemas de comunicación que utilizan como medio de transmisión una fibra óptica se basan en inyectar en un extremo de la misma la señal a transmitir (previamente la señal eléctrica procedente del emisor se ha convertido en óptica mediante un LED o L áser y ha modulado una portadora) que llega al extremo receptor, atenuada y, probablemente con alguna distorsión debido a la dispersión cromática propia de la fibra, donde recibe en un fotodetector, es decodificada y convertida en eléctrica para su lectura por el receptor, que se emplea con los sistemas de fibra óptica depende de una serie de factores, y algunas fuentes de luz se adaptan mejor a unos tipos que a otros. As LED, con un amplio espectro en el haz luminoso, admiten muy bien la modulación en intensidad, mientras que el láser -un haz de luz coherente adapta mejor a la modulación en frecuencia y en fase. Los dos métodos

tradicionales para la multiplexación de señales en un sistema de fibra óptica que utiliza luz coherente (láser) han sido TDM (Time Division Multiplexing) y FDM (Frequency Division Multiplexing), al que se viene a WDM. Al contrario que las otras t WDM suministra cada señal en una frecuencia láser diferente, de tal manera que puede ser filtrada ópticamente en el receptor. En distancias cortas, como es en el entorno de una oficina, la atenuación de la fibra (mínima para una longitud de onda de 1,55 (mm) y la dispersión (mínima para 1,3 (mm) no presenta un gran problema, pero a distancias mayores, como las que se requieren en los enlaces de comunicaciones a larga distancia, realmente lo es y se requiere el uso de amplificadores/repetidores que regeneren la señal cada cierta distancia. Por ejemplo:



cable trasatlánticos se colocan repetidores cada 75 km que, primero, convierten la señal óptica degradada en eléctrica, la amplifican y la vuelven a convertir en óptica mediante un diodo láser, para inyectarla de fibra óptica, todo un proceso complejo y que introduce retardos debido a los dispositivos electrónicos por los que ha de pasar la señal. Este inconveniente se evitaría si todo el camino pudiese ser óptico (all-optical), algo que ya es posible gracias a los resultados obtenidos, hace ya más de una década, por investigadores de la Universidad de Southampton, que descubrieron la manera de amplificar una señal óptica en una longitud de onda de 1,55 mm haciéndola pasar por una fibra de 3 metros de longitud dopada con iones erbio e inyectando en ella una luz de láser a 650 mm (fenómeno que se conoce como bombeo o pumping).

WDM: MULTIPLEXACIÓN EN LONGITUD DE ONDA



Los iones de erbio, que reciben la energía del láser, se excitan cediendo su energía mediante un proceso de emisión estimulada, lo que proporciona la amplificación de la señal, consiguiéndose de esta manera hasta 125 dB de ganancia. Dependiendo de la distancia y del tipo de fibra se pueden requerir amplificadores ó unir dos sistemas WDM, que son las piezas clave en esta tecnología Los sistemas amplificadores comerciales actuales (EDFA/ Erbium Doped Fiber Amplifier) utilizan, típicamente, un láser con una longitud de onda de 980 o 1.480 (m, en lugar de los 650 mm de las primeras pruebas de laboratorio y la inyección de la radiación diodo láser DFB) en el núcleo de la fibra se hace mediante un acoplador dicróico (beam -splitter), viajando ambas señales juntas por el núcleo, necesitándose muy poca potencia debido a las reducidas dimensiones de éste, pero que ha de ser bombeado a lo largo de toda él para evitar resonancias debido a la absorción por átomos de erbio no excitados. Cada receptor lleva un filtro óptico constituido por dos espejos que forman una cavidad resonante (DBR) en la que se puede seleccionar la longitud de onda, lo que sirve para sintonizarlo con la frecuencia que se desea separar.

1.10. MODELOS DE REFERENCIA ÓPTICO OTN.

1.10.1. La Visión OTN – Propiedades de la OTN.

La meta de la OTN es poder hacer el transporte multiservicio de paquetes basado en el tráfico de datos y antiguo, mientras que la tecnología DW (Digital Wrapper) acomoda la gestión no intrusiva y la monitorización de cada canal óptico asignado a una determinada longitud de onda. Por tanto la cabecera "wrapped " (OH) haría posible la gestión y el control de la información de la señal. La figura 1 ilustra como las capacidades de gestión de la OTN se realizan con la adición de cabeceras en varias posiciones durante el transporte de la señal cliente.

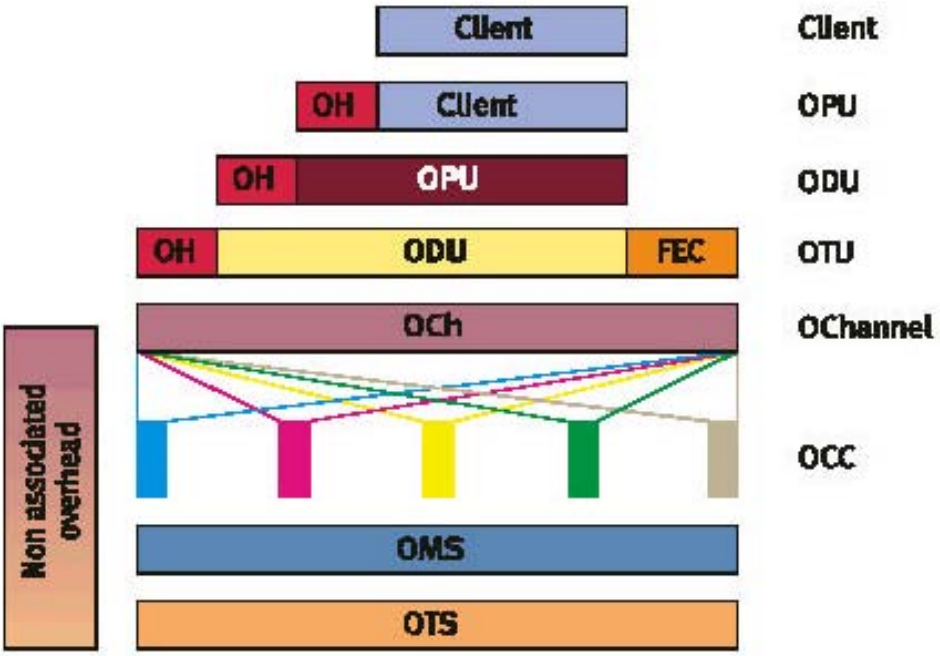


Figure1: Basic transport structure of an OTN

Se añaden varias secciones de cabecera a la señal cliente que juntas con el FEC forman la OTU (Optical Transport Unit). Entonces esto es transportado por una longitud de ondacomo un Canal Óptico (OCh). Si se transportan múltiples longitudes de onda sobre la OTN, se debe añadir una cabecera a cada una de ellas para poder tener la funcionalidad de gestión de la OTN.

Las secciones Multiplexación Óptica y las secciones Transmisión Óptica se construyen usando la cabecera adicional junto con los OCh.

La OTN presenta muchas ventajas a los operadores de la red incluyendo:

– Transparencia de protocolo

– Compatibilidad hacia atrás de los protocolos existentes

– Empleo de codificación FEC

– Reducción de regeneración 3R (a través de diseños flexibles ópticos de la red)

El último punto es de particular significación en cuanto minimiza la complejidad de la red que nos lleva a una reducción de costes.

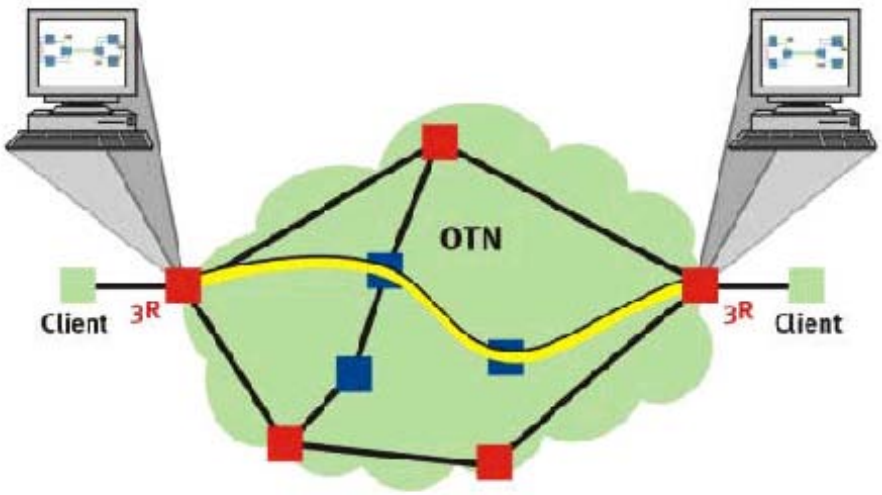


Figure 2: OTN network

La figure 2 ilustra la regeneración 3R que hay en un IrDI (Inter-domain Interface) de entrada a una OTN. El transporte a través de la red puede tener lugar solamente en el dominio óptico. Sin embargo un punto a resaltar es que en la actualidad no hay capacidades de gestión para negociar con las señales ópticas que no se hayan convertido al formato digital. En contraste a la red transparente, la red opaca realiza regeneración 3R en cada nodo de la red.

1.10.2. Los estándares ITU-T G.709 para la OTN.

El estándar ITU-T G.709, Network Node Interface para la OTN (Optical Transport Network) define la IrDI (inter-domain interface) de OTN de la manera siguiente:

– Funcionalidad de la cabecera en preparar la red óptica multilongitud de onda.
– Estructura de la trama OTU (Optical Transport Unit).
– Velocidades y formatos permitidos para el mapeo de los clientes.

Se describen dos tipos de interfaces en la recomendación ITU-T G.872 Architecture of the Optical Transport Networks , las ubicaciones de las cuales se ilustran en la figura 3 .

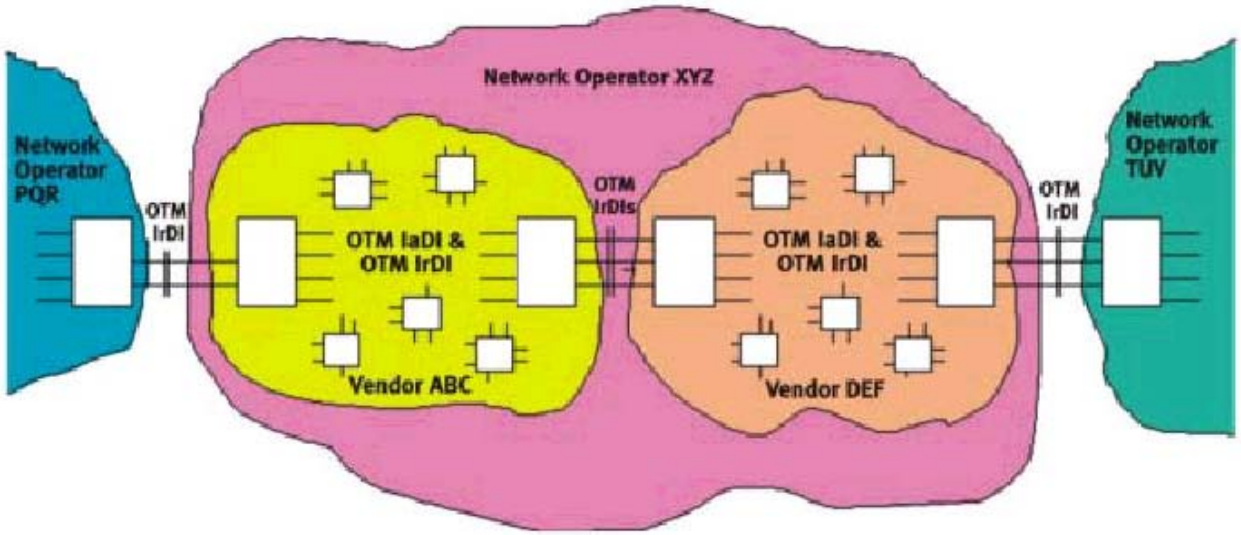


Figure 3. Network interfaces as defined in ITU-T G.872

1.10.3. Inter-Domain Interfaces (IrDI).

Estas definen:

– la ubicación entre las redes de dos operadores
– la ubicación entre las subredes de dos fabricantes en el mismo dominio del operador.
– la ubicación dentro de la subred de un fabricante.

1.10.4. Intra-Domain Interfaces (IaDI).

Estas definen:

– la ubicación entre el equipo de la subred de un fabricante individual Como en SONET/SDH, la OTN tiene un diseño estructurado en niveles.

Los niveles básicos de la OTN son visibles en la estructura del transporte OTN y consta de Canales Ópticos (OCh), Optical Multiplex Section (OMS) y Optical Transmission Section (OTS) como se ve en la figura 4. El transporte de una señal cliente en la OTN sigue el procedimiento indicado a continuación:

– Se añade la cabecera a la señal cliente para formar la OPU (Optical Channel
– Payload Unit)
– Entonces se añade una cabecera a la OPU formando así la ODU (Optical
– Channel Data Unit)
– Se añade una cabecera adicional más el FEC para formar la OTU (Optical
– Channel Transport Unit)
– Añadiendo más cabeceras se crea un OCh que es transportado por un color
– Se puede añadir cabeceras adicionales al OCh para poder gestionar múltiples.
– colores en la OTN. Entones se construyen el OMS y el OTS

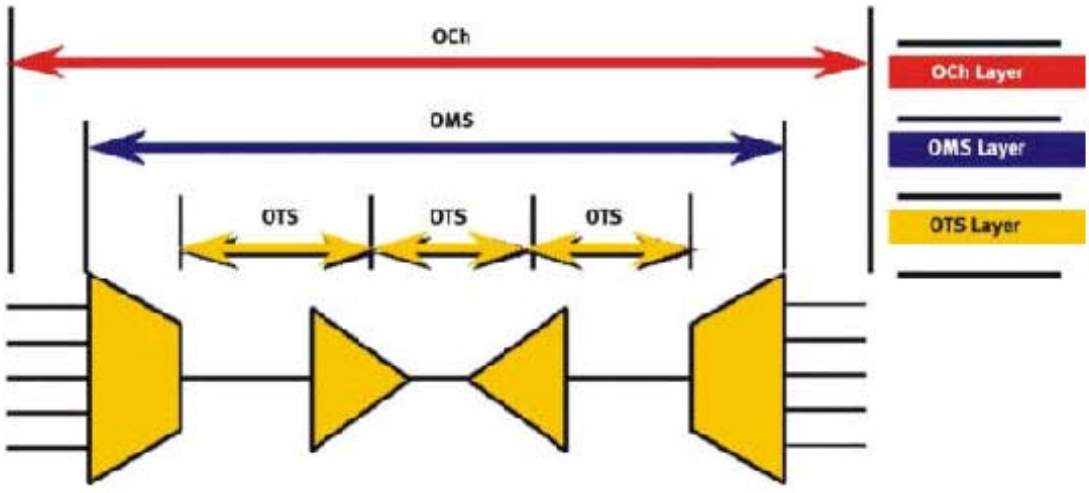


Figure 4. OTN layer structure

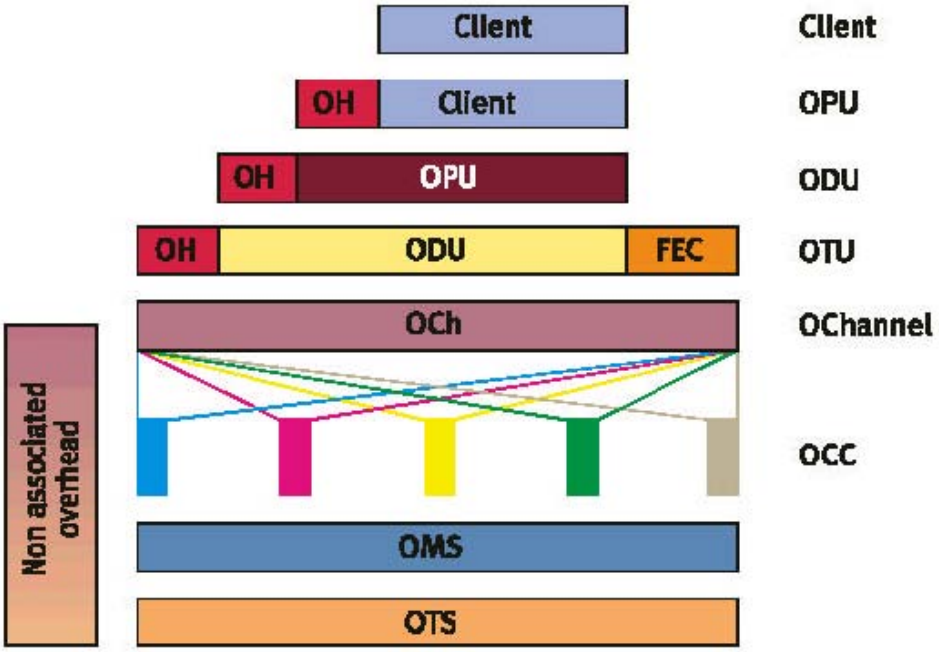


Figure 5. Basic OTN transport structure

El resultado es un canal óptico (OCh) que comprende una sección OH, una señal cliente y un segmento FEC.

Figure 6: Optical channel structure consisting of OH bytes, client and FEC.

La cabecera de OCh que ofrece la funcionalidad de gestión OTN, contiene 4 subestructuras: OPU (Optical Channel Payload Unit), ODU (Optical Channel.

Data Unit), OTU (Optical Channel Transport Unit) y FAS (Frame Alignment Signal).

La señal cliente - o los datos actuales a ser transportados – podía ser de cualquier protocolo existente p.e.; SONET/SDH, GFP, IP, GbE.

Figure 7: Client in an Optical Channel

La cabecera del OPU (Optical Channel Payload Unit) se añade a los datos del OPU y se usa para soportar las distintas señales cliente. Regula el mapeo de muchas señales cliente y suministra información sobre el tipo de señal transportada. Habitualmente la ITU-T G.709 soporta mapeo asíncrono y síncrono de las señales cliente en los datos.

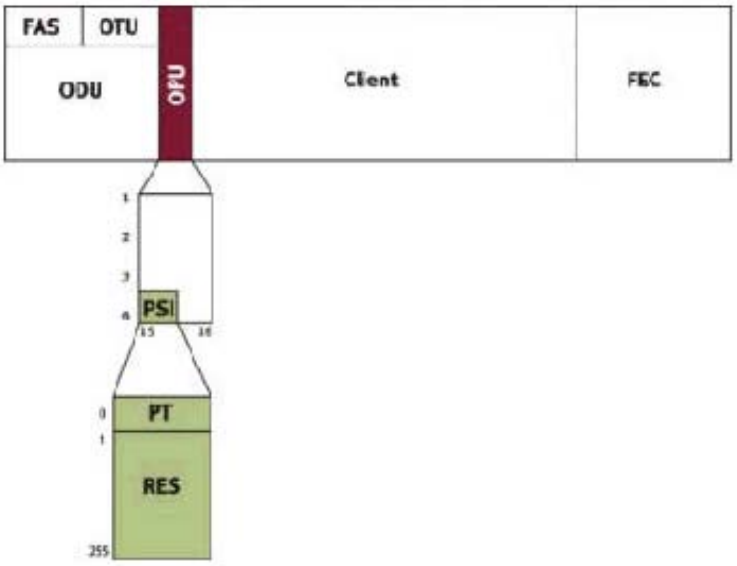


Figure 8: Overhead of OPU

La cabecera del OPU consta del PSI (Payload Structure Indentifier) que incluye el PT (Payload Type) y los bits de cabecera asociados con el mapeo de las señales cliente en los datos, como por ejemplo los bits de justificación requeridos para los mapeos asíncronos. Entonces la cabecera del OPU termina en el punto donde el OPU es ensamblado y desensamblado.

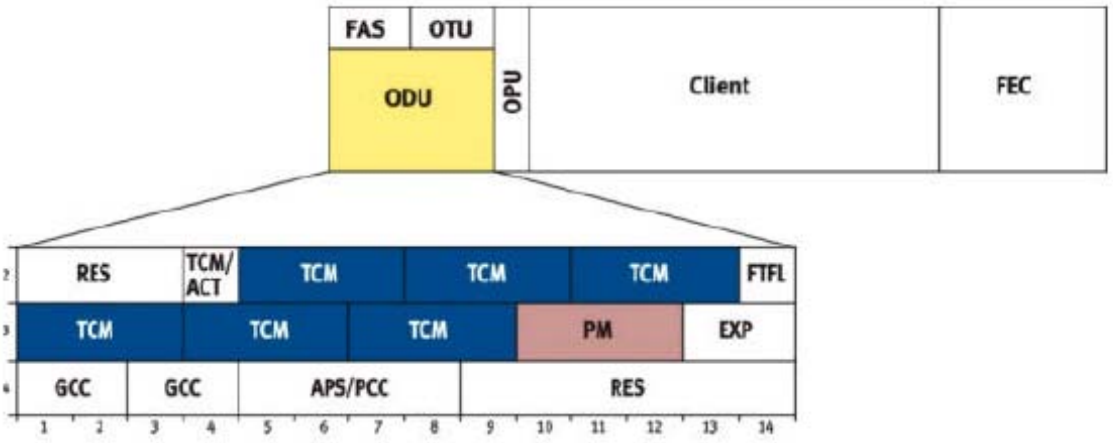


Figure 9: Overhead structure of ODU

256 octetos alineados con la multitrama ODU. PSI contiene el tipo de datos (PT) identificando los datos a ser transportados. El PT (Payload Type) de OPU es un único octeto definido dentro del PSI para indicar la composición de la señal OPU, o en otras palabras, el tipo de datos a ser transportados en el OPU.

La cabecera del ODU (Optical Channel Data Unit) permite al usuario soportar TCM (Tandem Connection Monitoring), PM (Path Monitoring) y APS. También es posible la supervisión del camino extremo a extremo y la adaptación del cliente via el OPU (como se ha descrito previamente).

La cabecera del ODU suministra dos importantes cabeceras: la cabecera PM (Path Monitoring) y la cabecera TCM.

La cabecera PM (Path Monitoring) de ODU permite la monitorización de secciones determinadas dentro de la red así como la localización del fallo en la red vía los octetos de la cabecera descritos en la cabecera PM.

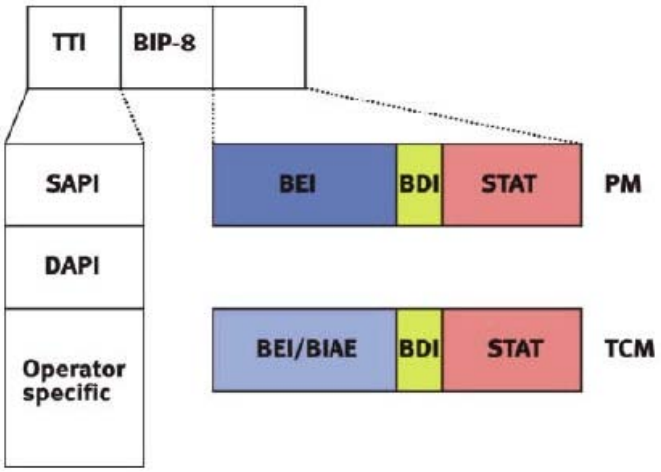


Figure 10: TCM and PM overhead structures

La cabecera PM está configurada en la fila 3, columnas 10 a 12 para soportar la monitorización del camino. La estructura del campo PM contiene los siguientes subcampos:

– TTI (Trail Trace Identifier). El TTI es similar al octeto J0 en SONET/SDH. Se usa para identificar la señal del origen al destino dentro de la red. El TTI contiene los Identificadores de Punto de Acceso (API - Access Point Identifiers) que se usan para especificar el Identificador de Punto de Acceso Origen (SAPI) y el Identificador del Punto de Acceso Destino (DAPI). Los APIs contienen información del país de origen, del operador de la red y otros detalles administrativos.

- BIP-8 (Bit Interleaved Parity). Este es un octeto que se usa para Detección de Error. El octeto BIP-8 provee “bit interleaved parity – 8 code”. El BIP-8 computa todo el OPU y se inserta en el BIP-8 SM dos tramas más tarde.
- BDI (Backward Defect Indication). Este es un único bit que lleva información en cuanto a fallo de la señal en la dirección ascendente.
- BEI (Backward Error Indication) y BIAE (Backward Incoming Alignment Error). Estas señales llevan información sobre los bloques “interleaved-bit” detectados con error en la dirección ascendente. También se usan para llevar errores de alineación de entrada (IAE
- Incoming Alignment Errors) en la dirección ascendente.
- Bits de estado para la señal de indicación y mantenimiento (STAT - Status bits). Estos tres bits indican la presencia de señales de mantenimiento.

1.10.5. Cabecera TDM (Tandem Connection Monitoring) del ODU .

Una determinada función implementada en las redes SONET/SDH es TCM (Tandem Connection Monitoring), una funcionalidad que permite la gestión de la señal a través de múltiples redes. La comprobación jerárquica de errores usando los octetos de paridad es otra función que se puede realizar. Además de esto, también el G.709 permite las funciones de gestión de la señal tales como las encontradas por ejemplo en los servicios al por mayor de longitud de onda.

Los octetos de la cabecera TCM están definidos en la cabecera de la fila 2, columnas 5 a 13 así como en la fila 3, columnas 1 a 9 en la cabecera del ODU. Cada campo TCM contiene los subcampos - como ya se describió en Path Monitoring – con BIAE adicional. La funcionalidad TCM implementada en el OTN es capaz de monitorizar hasta 6 “tandem connections” independientemente. TCM permite el anidamiento y el solape de las conexiones de monitorización ODU.

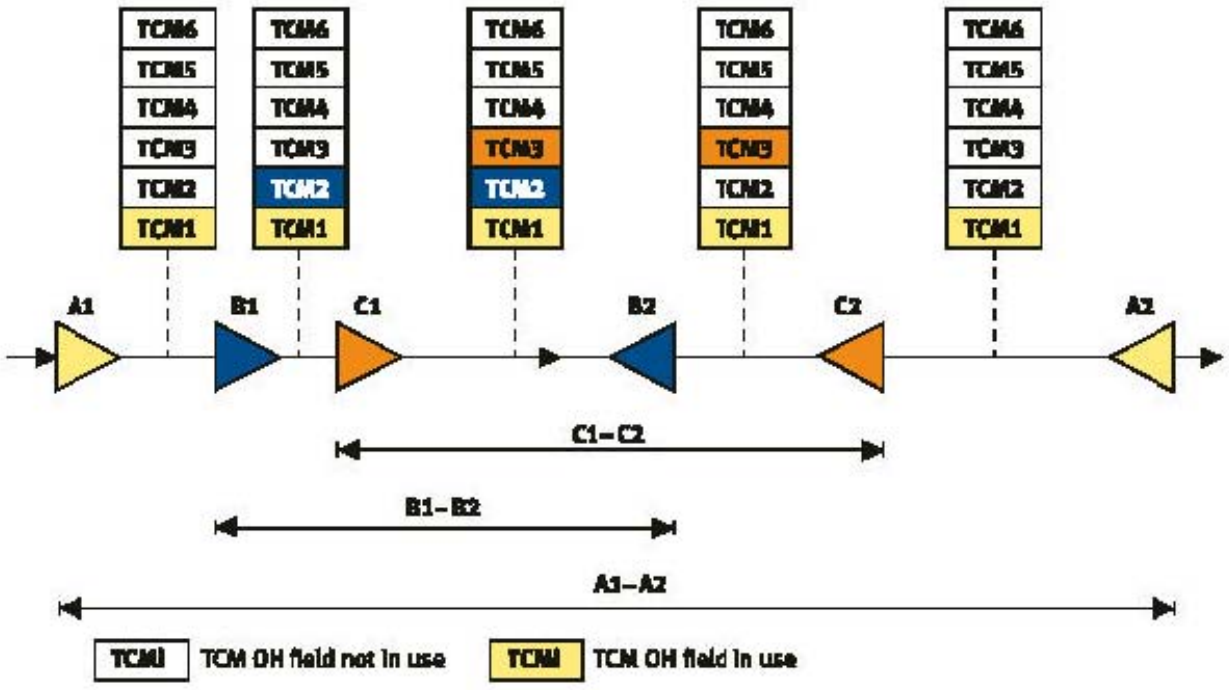


Figure 11: Possible TCM structure in an OTN.

Como se ilustra en la figura 11, es posible la monitorización entre A1-A2, B1-B2 y C1-C2 en modo anidado. Con B1-B2, solo es posible en modo cascada. Potencialmente estas funcionalidades se pueden usar por carriers para el mantenimiento de sus propios SLAs (Service Level Agreements) dentro de sus redes. Los octetos adicionales de cabecera del ODU se describen más abajo.

- RES. Estos octetos están reservados para la futura estandarización internacional. Todos los octetos están a cero ya que habitualmente no se usan.
- TCM/ACT. Este campo de un octeto se usa para la activación y desactivación de los campos TCM. En la actualidad, estos campos aún están en estudio.
- EXP. Estos octetos están reservados para futuros usos experimentales.
- General communication channels (GCC1,GCC2). Estos dos campos permiten la comunicación entre dos elementos de la red con acceso a la estructura de trama ODU.
- Automatic Protection Switching y Protection Communication Channel (APS/PCC). Es posible la conmutación APS en uno o más niveles.
- Fault Type y Fault Location channel (FTFL). Se reserva un octeto en la cabecera del ODU para el mensaje FTFL. Este octeto provee información del estado de fallo incluyendo información en cuanto al tipo y ubicación del fallo. El FTFL está relacionado con el tramo TCM.

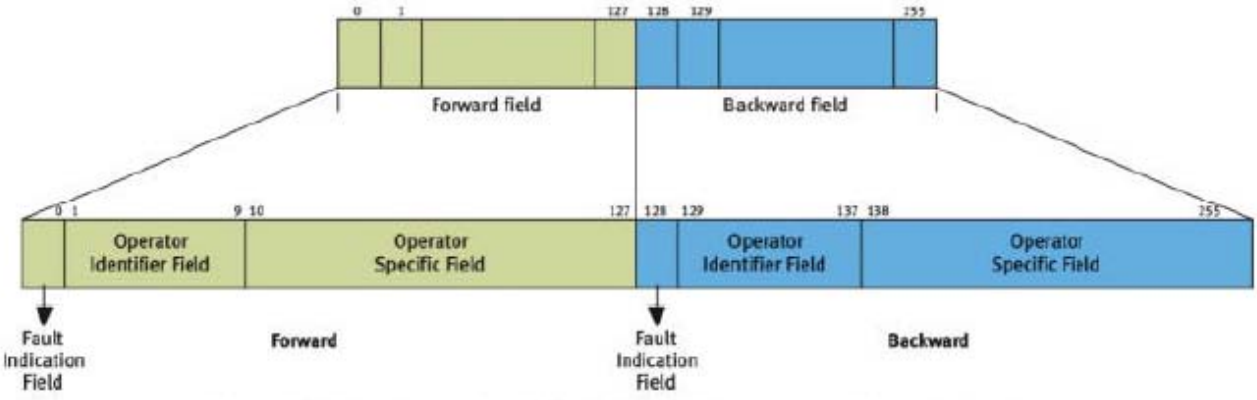


Figure 12: Structure of the FTFL field with its corresponding substructure

La subestructura contiene: campos de indicación de fallo hacia adelante y hacia atrás, campos de identificación del operador anterior y posterior, y campos específicos del operador anterior y posterior que realiza las funciones siguientes:

- **Campo de Indicación del Tipo de Fallo.**

Los códigos especificados indican las situaciones siguientes:

  - Sin Fallo
  - Fallo de la Señal
  - Degradación de la Señal

Los octetos adicionales en el campo del mensaje FTFL están reservados para la futura estandarización internacional.

- **Campo Identificador del Operador .**

Este campo especifica el origen geográfico del operador e incluye un campo de segmento nacional

- **Campo Específico del Operador.**

Estos campos no están estandarizados por las recomendaciones ITU-T G.709

- **Cabecera del OTU (Optical Channel Transport Unit) y Alineación de la Trama.**

El OTU se usa en la OTN para soportar el transporte vía una o más conexiones de canal óptico. También especifica la Alineación de Trama y el FEC.

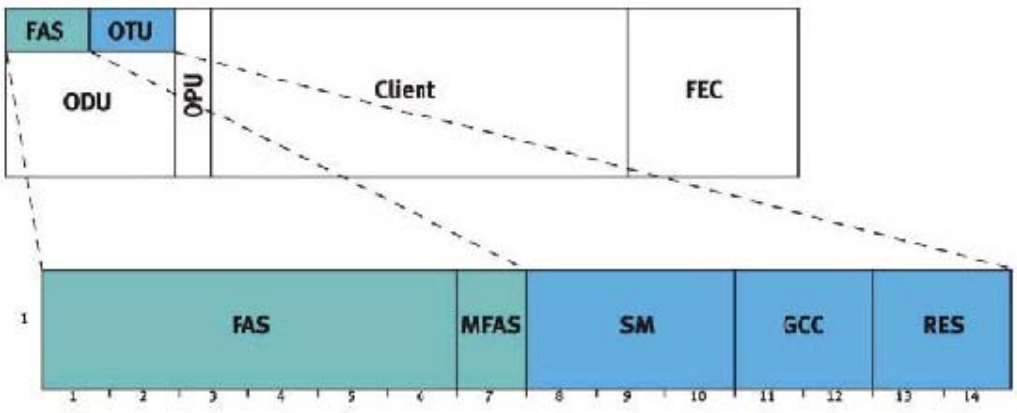


Figure 13: Frame Alignment and OTU OH structure

La cabecera de la Alineación de Trama es parte de la cabecera del OTU. Se sitúa en la fila 1, columnas 1 a 6 del OTU en que se define una Señal de Alineación de Trama (FAS

-Frame Alignment Signal) (figura 13). Como las tramas OTU y ODU pueden abarcar múltiple tramas OTU, se define una señal de cabecera estructurada multitrama. La Señal de Alineación Multitrama (MFAS - Multi Frame Alignment Signal) se define en la fila 1, columna 7 de la cabecera OTU/ODU. El valor del octeto MFAS se incrementa con cada trama OTU/ODU.

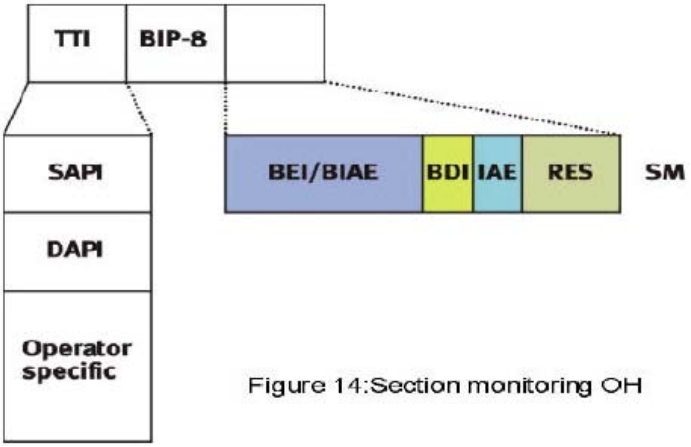


Figure 14:Section monitoring OH

La cabecera de la Sección de Monitorización consta de los subcampos descritos para la cabecera de la monitorización del camino, con excepción del bit de Error de Alineación de Entrada (IAE - Incoming Alignment Error).

Este bit permite al punto de entrada informar al punto de salida de que ha sido detectado un error de alineación en la señal de entrada. IAE se pone a “1 ” cuando ocurre el error, de otra forma es puesto a “0”.

General Communication Channel 0 (GCC0) se usa como un canal de comunicación entre puntos de terminación del OTU.

1.10.6. Forward Error Correction (FEC).

Junto con la cabecera del OCh del “Digital Wrapper Envelope”, se añade un ancho de banda adicional – en este caso el FEC. El algoritmo implementado/FEC permite la corrección y detección de errores en un enlace óptico.

Figure 15: FEC structure of the OCh

FEC ya es ampliamente usado por los operadores de cable submarino en varios diseños. También hay varios algoritmos/códigos que se pueden usar para realizar la corrección del error.

La implementación FEC definida en la recomendación G.709 usa el llamado Código Reed-Solomon RS(255/239). Aquí una fila OTU se divide en 16 subfilas cada una de ellas conteniendo 255 octetos. Las subfilas están formadas por “byte interleaved”, significando que la primera subfila consta del primer octeto de la cabecera y el primer octeto de los datos. El primer octeto FEC se inserta en el octeto 240 de la primera subfila. Esto es verdad para todas las 16 subfilas.

De estos 255 octetos, 239 se usan para calcular la comprobación de paridad del FEC, el resultado del cual se transmite en los octetos 240 a 255 de la misma subfila.

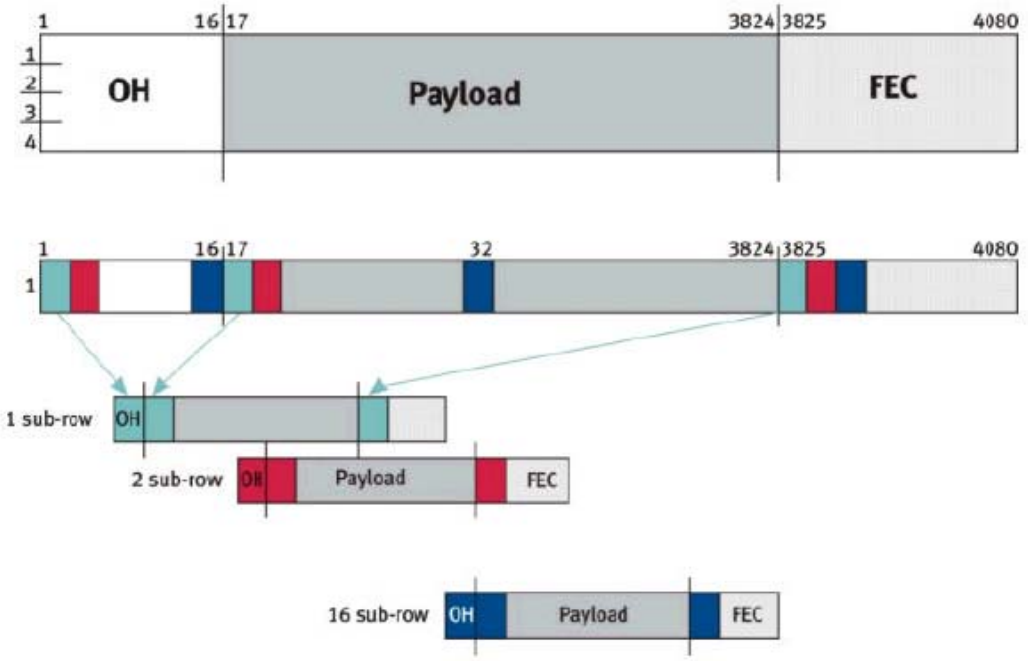


Figure 16: Illustration of Reed-Solomon coding in the G.709 recommendation

El código Reed-Solomon detecta errores de 16 bits o corrige errores de 8 bits en una subfila. El FEC RS (255,239) se especifica para la interfaz plenamente estandarizada IrDI. Otras interfaces OTUkV (p.e.; IaDI)– que solo están funcionalmente estandarizadas.

– pueden usar otros códigos FEC.

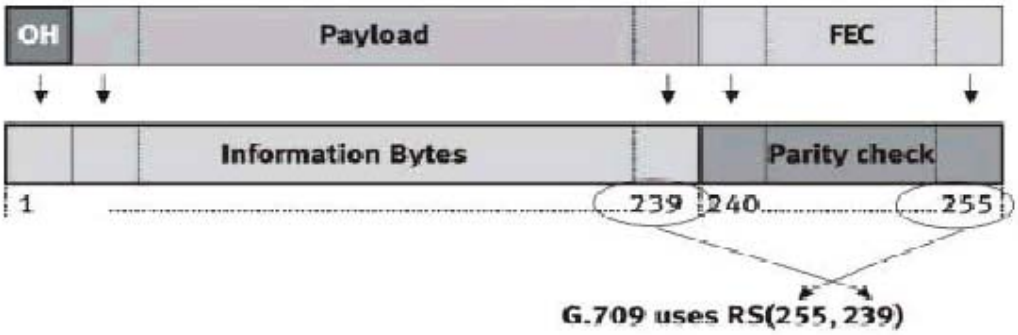


Figure 17. Forming of parity check

- **El caso de uso de FEC en redes ópticas.**

FEC permite la detección y la corrección de errores de bits causados por fallos físicos en el medio de transmisión. Estos fallos se pueden clasificar en efectos lineales (atenuación, ruido y dispersión) y no lineales (four wave mixing, self phase modulation, cross phase modulation).

Cuando se usa FEC en un enlace de red, el operador de red puede aceptar una señal de calidad más baja en el enlace ya que estos errores potenciales se pueden corregir.

En el cuadro se ilustra el efecto de un aumento de la calidad de la señal en tres casos. En un caso, no se usa FEC. En los restantes dos casos, se utiliza FEC pero con diferentes algoritmos de codificación.

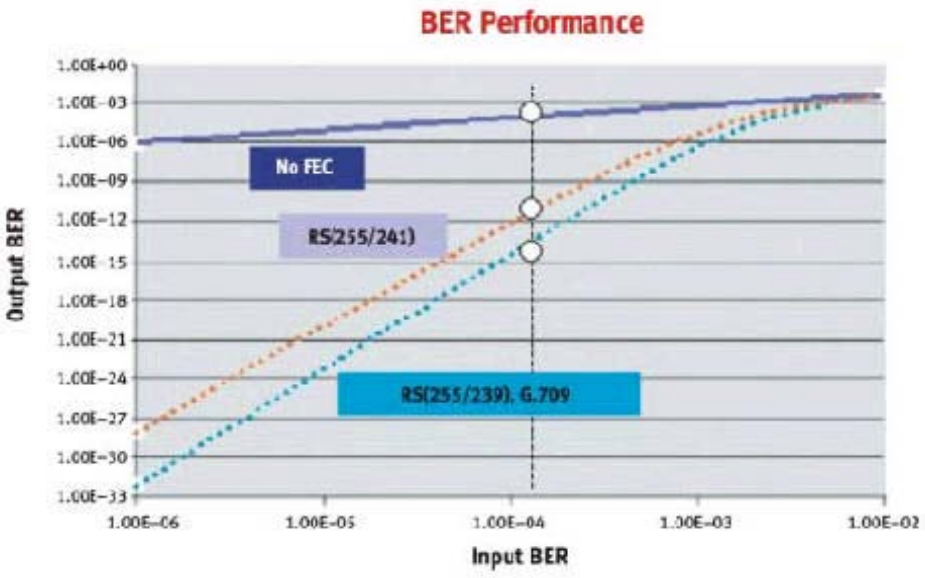


Figure 18: Effect of using FEC with various algorithms.

En este ejemplo un BER (Bit Error Rate) de entrada de aproximadamente 10^{-4}, se puede mejorar a un BER de salida de aproximadamente 10^{-15} en el mejor de los casos. Sin embargo el BER de salida no demuestra mejora cuando no se usa un algoritmo FEC.

- **Los beneficios del FEC en las redes ópticas.**

La mejora del potencial en la calidad de la señal en un enlace óptico ofrece muchas ventajas incluyendo:

– ganancia en nivel de potencia de aproximadamente 5 dB. Esto se consigue cuando se usa 7% FEC. (correlacionando a una expansión de enlace de aproximadamente 20km).
– reducción en el uso de regeneradores 3R. Esto permite incrementar la distancia entre enlaces.
– uso de los enlaces existentes de 2.5Gbit para transportar tráfico de 10Gbit. Esto ha sido intentado y puede ser posible dado que el FEC permite la corrección de una calidad de señal más baja.
– posibilidades de aviso anticipado. Algunos Elementos de la Red (NE) monitorizan los errores corregidos en los enlaces. Este parámetro se puede usar sucesivamente como una herramienta de aviso anticipado mediante el cual la cantidad de errores corregidos en un enlace puede significar el debilitamiento de un componente del propio enlace.

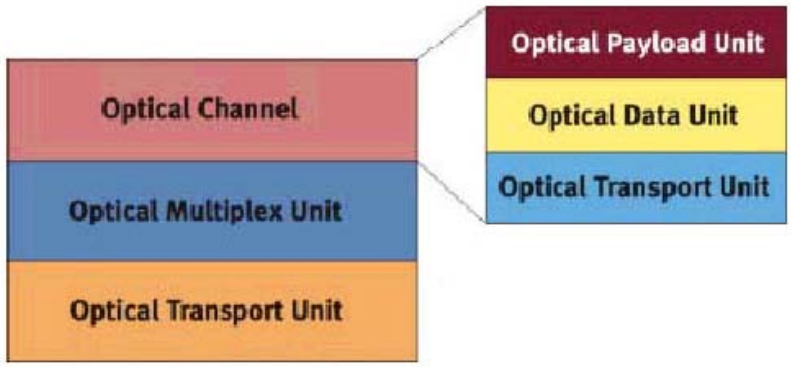


Figure 19: OCh substructure and basic OTN structure.

Una vez se ha formado el canal óptico, se añade una cabecera adicional no asociada a las longitudes de onda individuales del OCh, que forman entonces las Secciones deMultiplexación Ópticas (OMS) y las Secciones de Transmisión Ópticas (OTS).

En el nivel de la Sección de Multiplexación Óptica (OMS), se trnsportan tanto los datos OMS y como la cabecera no asociada. Los datos OMS constan de OChs multiplexados. La cabecera del OMS, aunque sin definir en este punto, intenta soportar la monitorización de la conexión y asistir a los proveedores de servicio en sus problemas y el aislamientode los fallos de la OTN.. El nivel de la Sección de Transmisión Óptica (OTS) transporta los datos OTS así como la cabecera de OTS. Similar al OMS, el OTS transporta las secciones multiplexadas ópticamente descritas anteriormente. La cabecera del OTS -sin embargo no completamente definida -se usa para funciones de mantenimiento y operación. El nivel OTS permite al operador de la red realizar tareas de monitorización y mantenimiento entre los elementos de la red que incluyen; OADMs, multiplexadores, desmultiplexadores y conmutadores ópticos..

- **Aplicaciones de medida del FEC.**

La OTN provee extensiva funcionalidad OAM&P para múltiples longitudes de onda y así requiere una extensa cabecera. Para garantizar la disponibilidad de ancho de banda y la calidad de la transmisión de la red, los octetos de la cabecera necesitan ser monitorizados. Además de monitorizar el estado de estos octetos de cabecera, el sistema necesita ser verificado bajo presión. Este procedimiento ejecuta principalmente por la introducción de alarmas y errores en el sistema y a continuación medir su efecto en la transmisión.

La tecnología DW (Digital Wrapper) y el FEC implementado en la OTN son tecnologías relativamente nuevas ofreciendo aplicaciones relacionadas al uso del R&D. Las aplicaciones de medición en producción e instalación ya están o en uso o planificadas en un futuro.

– Las pruebas en R&D, producción e instalación son principalmente funcionales y cubren:
– la verificación de la integridad de la señal (potencia óptica, posibilidad del DUT para sincronizar la trama, y otros parámetros)
– la prueba de señales de mantenimiento – prueba de alarmas (p.e. LOS, AIS, etc.)
– inserción de error en la señal de prueba
– pruebas de mapeo del OTUk (p.e. mapeo de una estructura SONET/SDH en el OTUk)

– pruebas de multiplexación del OTUk (p.e. multiplexación de un ODM1 en un ODU2)
– pruebas de la cabecera G.709 (p.e. pruebas de la sección de monitorización, de la monitorización del camino y FTFL)
– interoperabilidad, en donde se requiere pruebas de TCM
– pruebas de error del FEC
– estimulación de los Elementos de Red con anomalías (p.e. alarmas y errores).

1.10.7. Pruebas de Estímulos.

Un estímulo se envía al DUT y la señal devuelta se monitoriza en el equipo de medida. La señal recibida se debe correlacionar con el estímulo. La dos señales no deberían ser iguales, entonces el usuario recibe la información en el DUT permitiendo que posteriormente se puedan llevar a cabo más investigaciones.

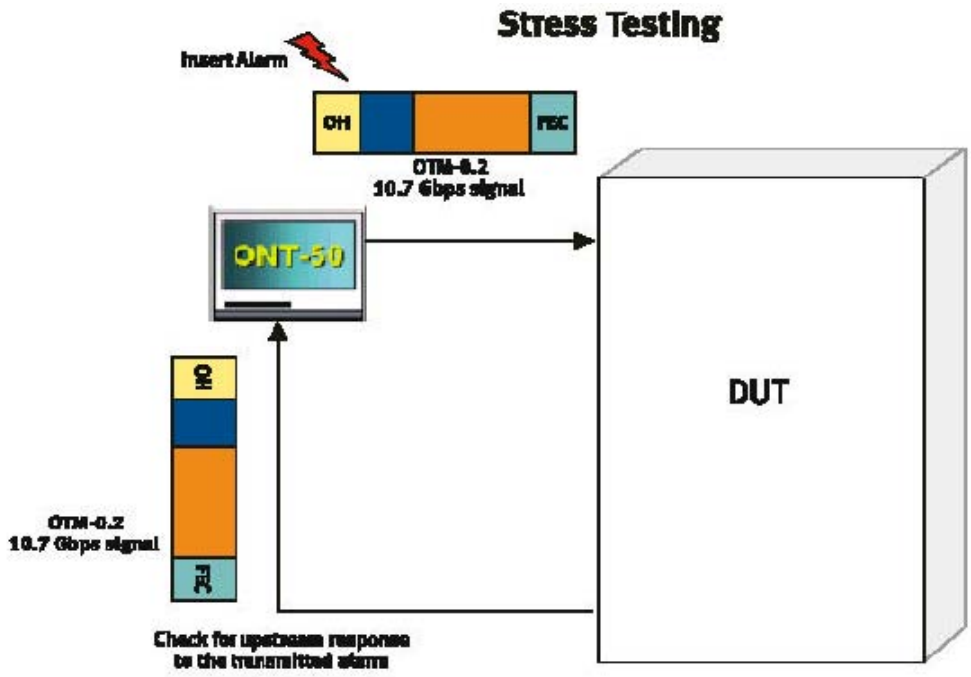


Figure 20: Setup for stimulus testing

Los posibles estímulos podrían incluir los errores y alarmas estándar del OTN como se definen en las recomendaciones G.709.

1.10.8. Mapeo y desmapeo de las señales cliente.

La estructura de las tramas de OTN hacen posible el mapeo de varios tipos de tráfico en las OPUs. Esto incluye por ejemplo; SONET/SDH (STM-256) en OPU3, mapeo de celdas ATM en el OPU y el mapeo de tramas Generic Frame Procedure (GFP) en el OPU. Por supuesto las diferencias de velocidad entre el cliente y el OPU necesitan ser ajustadas. También esta prueba es extremadamente útil ya que se requieren mapeos síncronos o asíncronos para los distintos mapeos del cliente. Con el fin de realizar esta medida, entonces se debe transmitir una señal de rango variable para su mapeo en el OPU por el DUT. Entonces el receptor puede detectar si el cliente ha sido mapeado apropiadamente en el OPU.

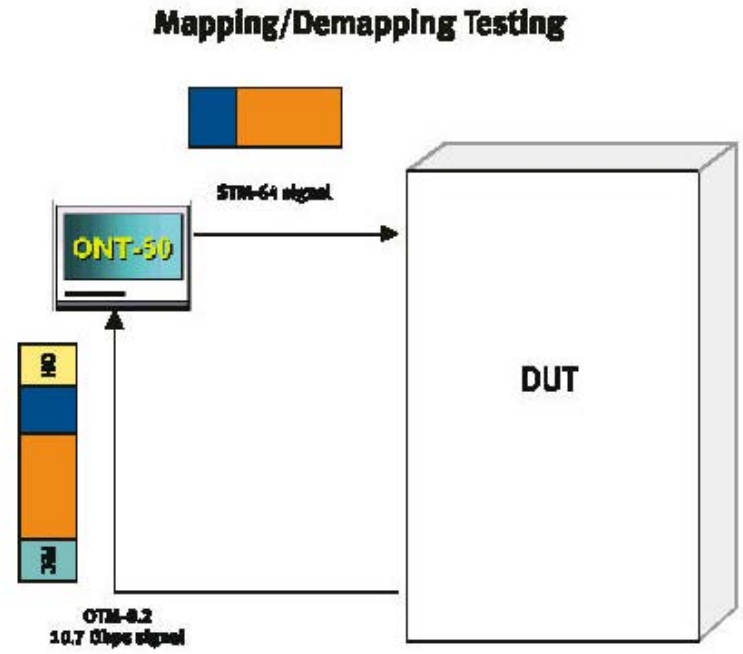


Figure 21: Mapping and demapping testing

1.10.9. Pruebas del FEC.

Con el fin de hacer una comprobación completa del FEC, se inserta un error en el OCh y entonces se transmite a través de los Elementos de la Red OTN.

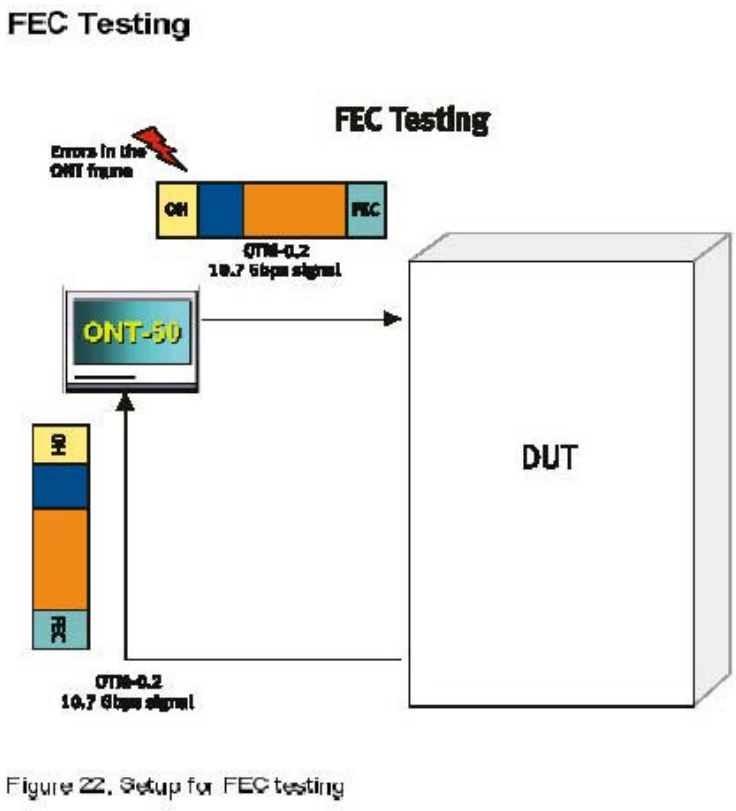


Figure 22. Setup for FEC testing

En el extremo receptor, se comprueba el OCh para determinar si el error fue corregido por el DUT. Esta prueba se realiza insertando distintas cantidades de errores y permitiendo al usuario comprobar sucesivamente la capacidad de corrección de error de su Elemento de Red. Si el número de errores insertados excede la capacidad de corrección del Elemento de Red, el equipo de medida lo reflejará como error o errores incorregibles.

CAPITULO 2

PROTOCOLOS DE SEÑALIZACIÒN

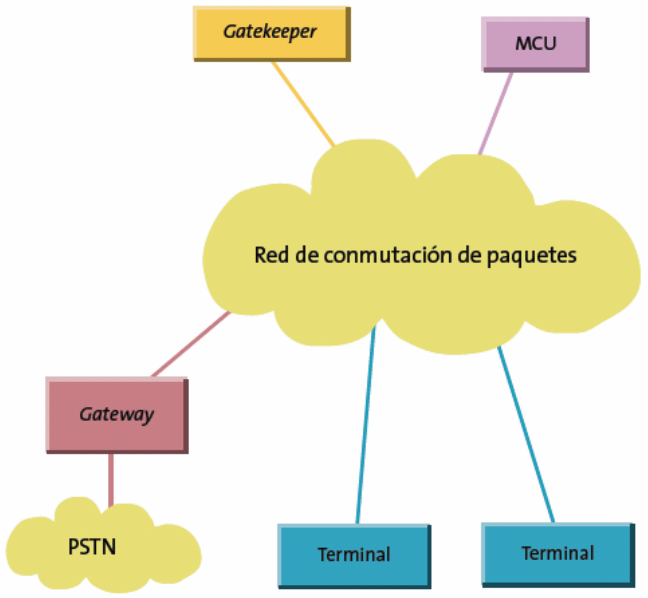
2.- PROTOCOLO H.323.

H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para vídeo-conferencias y aplicaciones en tiempo real, entre otras variantes.

El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

2.1. COMPONENTES H.323.

Este estándar define un ámplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define los siguientes componente más relevantes como se muestra en la siguiente figura:



- **Entidad:**

La especificación H.323 define el término genérico entidad como cualquier componente que cumpla con el estándar.

- **Extremo**:

  Un extremo H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

- **Terminal:**

  Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

  Las funciones de control que realizan los terminales son las siguientes:

  - H.245 para negociación del canal.
  - H.225.0 (Q.931) para señalización y control de llamada.
  - H.225.0 (RAS) para comunicación con el gatekeeper.

  También implementan los protocolos RTP/RTCP para el manejo de los flujos de audio y video.

- **Gatekeeper:**

  El gatekeeper (GK) es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas. El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN. El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

Las funciones que debe desarrollar un gatekeeper son las siguientes:

• Control de la señalización.

• Control de acceso y administración de recursos, autorización de llamadas.

• Traducción de direcciones de transporte entre direcciones IP y alias.

• gestión del ancho de banda.

• gestión de llamadas(concesión de permisos...)

• gestión del ancho de banda.

Para desarrollar estas funciones , entre el gatekeeper y el endpoint se emplea el protocolo RAS (Registration /Admission /Status) sobre UDP.

Un gatekeeper y sus endpoints definen una zona H.323, de manera que en entornos LAN's es suficiente un gatekeeper, pero en entornos como Internet, son necesarios varios de ellos, cada uno definiendo una zona H.323.

Lógicamente, entre gatekeepers se requerirá comunicación, por lo que actúa como el punto central para todas las llamadas en una zona, comportándose como un conmutador virtual.

Si bien el gatekeeper no es obligatorio, su empleo en un entorno H.323 sí posibilita emplear más eficientemente la plataforma, por ejemplo mediante el enrutamiento de llamadas a su través.

Los gatekeepers son entidades funcionales separadas de los endpoints H.323, pero es posible incluir funcionalidades gatekeepers en los gateways y las MCU's.

- **Gateway:**

Un gateway H.323 (GW) es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. los gateways, son los sistemas encargados de permitir que los equipos H.323 puedan operar con otras redes. Desarrollan la traducción de la señalización, información de control e información de usuario, posibilitando así

interoperabilidad entre redes, terminales y servicios, haciendo viable la integración de servicios aún con plataformas dispares, llámese PSTN y redes IP.

Una diferencia respecto a los gatekeepers, es que los gateways sí cursan información de usuario, soportada en RTP/UDP/IP.

- Funciones de los gateways:
- transcodificación de audio y vídeo.
- traducción de procedimientos de comunicación.
- traducción de formatos de transmisión.

Evidentemente, dada su funcionalidad, los gateways son elementos opcionales en entornos H.323, y sólo son necesarios cuando se requiere una interconexión entre entornos H.323 y entornos no H.323:

- **MCU (Multipoint Control Units):**

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

La comunicación bajo H.323 contempla las señales de audio y vídeo. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo el estándar T.120 que permite la compartición de aplicaciones en conferencias punto a punto y multipunto.

Dado el jitter, que sufren los paquetes IP en la red, y las consecuencias negativas de esto para el tráfico de audio y vídeo, en el terminal H.323 se requiere un buffer de recepción para absorber, en la medida de lo posible, estas fluctuaciones en la demora de los paquetes IP, anulando o reduciendo el efecto negativo que el jitter puede producir en flujos de información de usuario con requerimientos de tiempo real.

Los protocolos de control comprendidos en H.323, unos se encapsulan en UDP (protocolos H.225.0 (RAS, Registration Admisión Status), que se desarrolla entre el gatekeeper y los endpoints) y otros en TCP (H.225.0 (Q.931), para el control de la llamada y H.245 para el control del canal.

2.2. FLUJO DE LLAMADAS.

El establecimiento de la llamada en H.323 se lleva a cabo en tres fases:

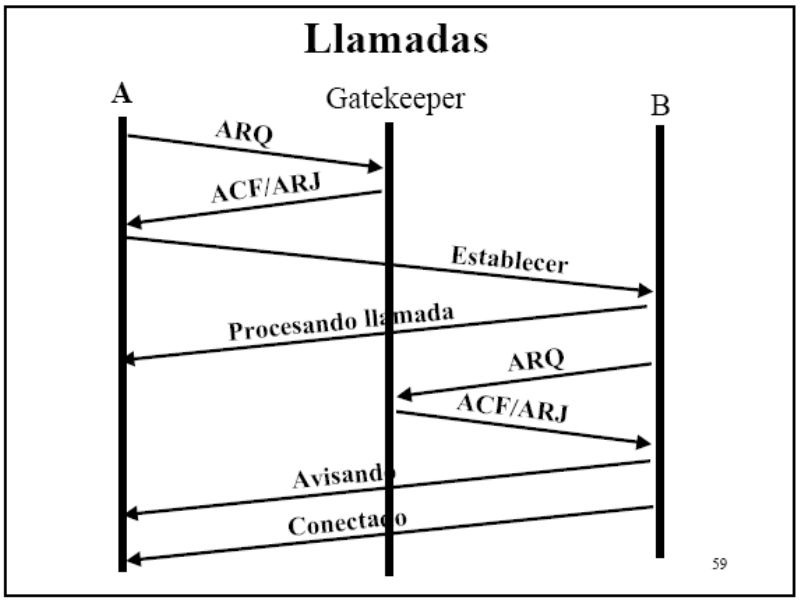
- Fase RAS: intercambio de mensajes entre el gatekeeper y el endpoint., para la traducción de direcciones , autorización de llamadas y gestión del ancho de banda.
- Fase Q.931: intercambio de mensajes entre endpoints para el establecimiento de conexiones lógicas.
- Fase H.245: intercambio de mensajes entre endpoints para acordar en intercambio de información de usuario.

Dependiendo del papel que juegue el gatekeeper en las llamadas H.323 podremos hablar de dos modelos:

- modelo de llamada H.323 directa (direct routed model)
- modelo de llamada H.323 indirecta (gatekker routed model)

A continuación de estas tres fases de establecimiento de llamada, se lleva a cabo la transferencia de información de usuario por medio de los protocolos RTP/RTCP, según lo acordado en la fase H.245, previa apertura de los canales lógicos en los endpoints. Estos canales lógicos son unidireccionales, por lo que para una comunicación bidireccional se requiere abrir uno en cada dirección de transmisión. En la transferencia de medios no interviene el gatekeeper, pues es solo una entidad de señalización, sino que se lleva a cabo directamente entre os endpoints.

Hasta la fecha, el estandar H.323 ha evolucionado desde la primera versión H.323v1, hasta la última versión H323v4, mejorando la primera versión en cuestiones como seguridad, servicios suplementarios, identificación de llamadas, conexión rápida.....etc.



2.3. CARACTERISTICAS Y RECOMENDACIONES DEL PROTOCOLO H.323

El estándar H.323 especifica los componentes, protocolos y procedimientos que proveen los servicios de comunicación multimedia sobre redes de paquetes sin garantía de calidad de servicio, tanto para sesiones multipunto como punto a punto. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol). Además, H.323 también define la señalización necesaria para comunicaciones multimedia sobre redes IP (entre otras). Para el transporte de medios utiliza los protocolos RTP/RTCP.Los terminales y equipos H.323 soportan aplicaciones con requerimientos de tiempo real (voz y vídeo), así como aplicaciones de datos y combinaciones de ellas (videotelefonía, etc). Los terminales H.323 pueden ser terminales explícitamente diseñados a este fin o pueden estar integrados en PC's.

El estándar H.323 incluye entre otras las siguientes recomendaciones:

- H.225.0: paquetización, sincronización y señalización.
- H.245: control del canal.
- G.711, G.722, G.723.1, G.728, G.729: codificación audio.
- Además también define recomendaciones sobre conferencias de datos en tiempo real y seguridad.

H.323 define una serie de entidades en una red H.323 con una serie de funcionalidades:

- **Direccionamiento:**

1. RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.
2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

- **Señalización**:

1. Q.931 Señalización inicial de llamada
2. H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz
3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

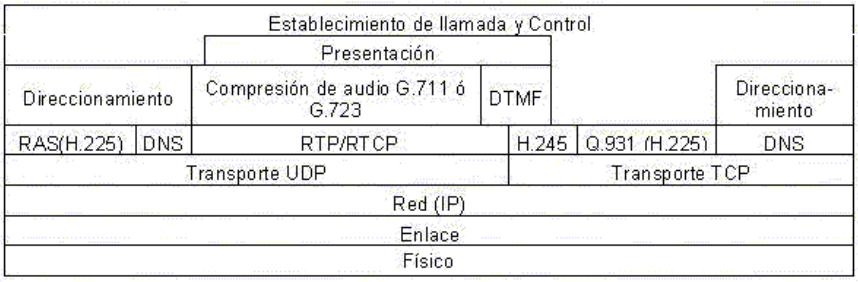
- **Compresión de voz:**

1. Requerido: G.711
2. Opcionales: G.728, G.729 y G.723

- **Transmisión de voz:**

1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP. UDP provee a los usuarios acceso a los servicios IP. Los paquetes UDP son entregados como paquetes IP no orientados a conexión, los cuales pueden ser descartados antes de alcanzar su objetivo.

2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

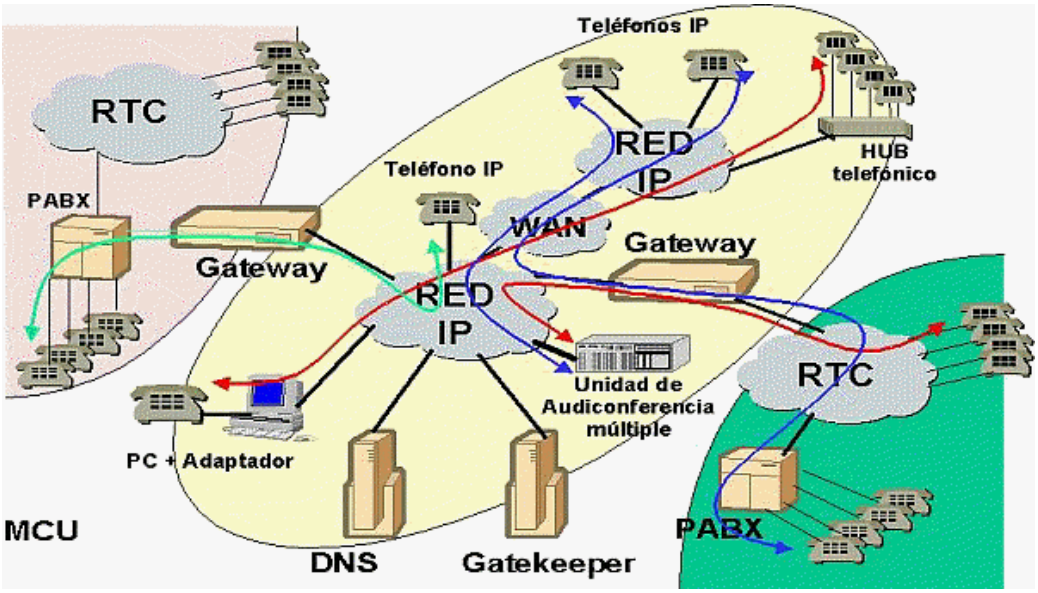


- **Control de la transmisión:**

1. RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras. Actualmente se puede partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, permitirán construir las aplicaciones VoIP. Estos elementos son:

   - Teléfonos IP.
   - Adaptadores para PC.
   - Hubs telefónicos.
   - Gateways (pasarelas RTC / IP).
   - Gatekeeper.
   - Unidades de audioconferencia múltiple. (MCU voz)

- Servicios de directorio.



2.4. ARQUITECTURA DEL PROTOCOLO H.323.

En una arquitectura H.323 (como la que se muestra en la Figura 1) se integran como componentes básicos los Terminales, Gateways (para interconexión con resursos PSTN/IN), Gatekeepers (Control de admisión, registro y ancho de banda) y MCUs (Multiconference Control Units). Dentro de H.323 se incluyen todo un conjunto de protocolos perfectamente integrados (en la Figura 2 se ilustra la pila de protocolos H.323) que toman parte en el establecimiento y mantenimiento de conferencias multimedia: Q.931 para el establecimiento de llamada, H.225 para la señalización, H.245 para la negociación de capacidades y el establecimiento de canales, H.450.x para la definición de servicios suplementarios (Call Park, Call Pickup, Call Hold, Call Transfer, Call Diversion, MWI, ...), RAS para el registro de terminales y el control de admisión, RTP/RTCP para el transporte y secuenciación de los flujos multimedia, G.711/G.712 para la especificación de los codecs, T.120 para colaboración y “dataconferencia”... Esto da una idea muy clara de una de las características menos agradables de este protocolo, y que siempre han argumentado sus detractores: su excesiva complejidad, frente a la sencillez del modelo Internet en que se basa SIP. De hecho SIP se podría comparar, grosso modo, con las partes de Q.931 y H.225 de H.323.

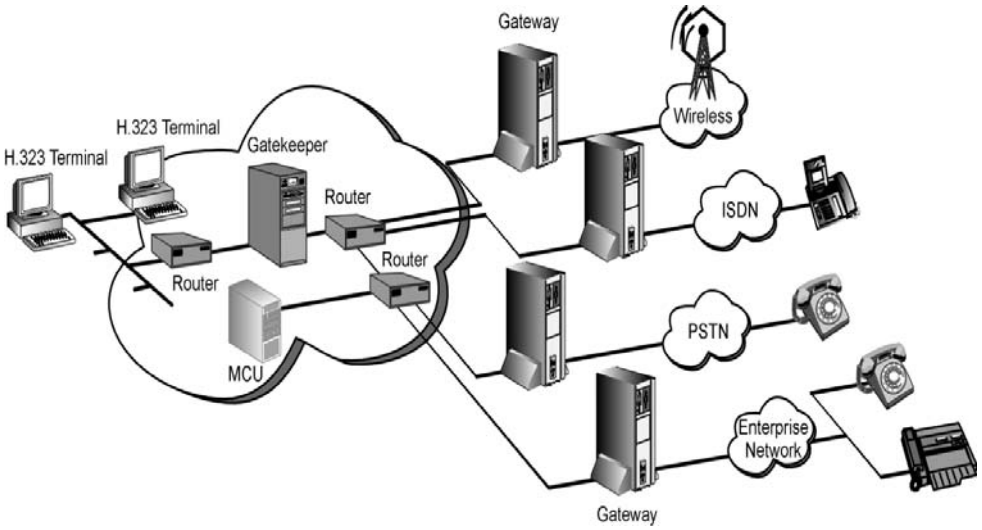


Figura 1

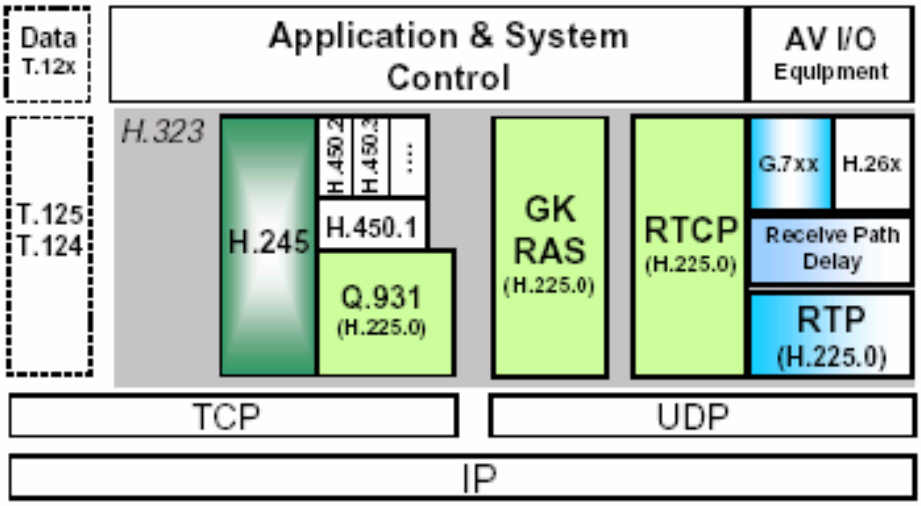


Figura 2

2.5. DEFINICIÒN DE PROTOCOLO SIP.

El protocolo “Session Initiation Protocol” (SIP) es un estándar emergente para establecer, enrutar y modificar sesiones de comunicaciones a través de redes Internet Protocol (IP). Utiliza el modelo de Internet y lo convierte al mundo de las telecomunicaciones, utilizando protocolos Internet existentes tales como HTTP y SMTP (Simple Mail Transfer Protocol). También usa una estructura de dirección URL. Usa estas direcciones de tipo correo electrónico para identificar a los usuarios en lugar de los dispositivos que los utilizan. De esta forma SIP no depende del dispositivo y no hace distinción alguna entre voz y datos, teléfono u ordenador. Como se describe a continuación, SIP es usado mas para el manejo de servicios, mientras que H.323 se usa prácticamente para la conversión del número telefónico en paquetes IP.

2.6. CARACTERÍSTICAS BÁSICAS DEL PROTOCOLO SIP.

Se trata de un protocolo para el establecimiento de sesiones sobre una red IP. Una sesión que puede soportar desde una llamada telefónica hasta una multiconferencia multimedia con elementos de colaboaración. Está siendo desarrollado por el SIPWG del IETF (RFC 2543, 2543bis), con la misma filosofía de sencillez y mínimo esfuerzo de siempre. SIP está pensado como un mecanismo para el establecimiento, la terminación y la modificación de sesiones. Se trata de un protocolo basado en el paradigma de petición/respuesta (request-response), al igual que HTTP o SMTP.

SIP maneja mensajes de petición: [que se estructuran en tres bloques] Request Line + Cabecera + Cuerpo, y mensajes de respuesta: Status Line + Cabecera + Cuerpo. En ambos casos el cuerpo es independiente de SIP y puede contener cualquier cosa. A efectos de estandarización se definen métodos para describir las áreas de especificación; SIP define los siguientes métodos: invite, bye, options, ack, register, cancel, info (rfc 2976), comet, prack, subscribe/, notify/, message.

En la Figura 3 se ilustra un mensaje tipo, con los campos más importantes de la cabecera y el cuerpo rellenos de forma genérica.

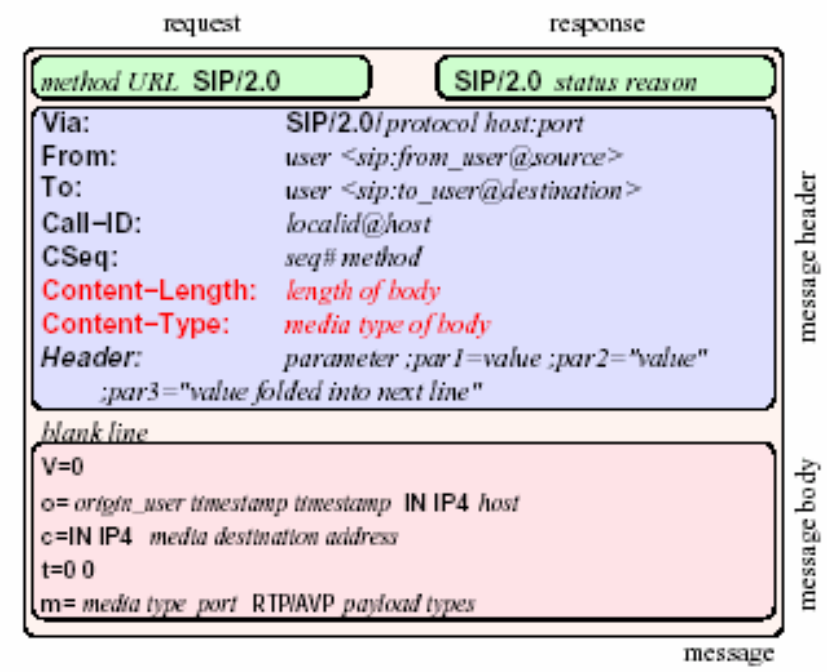


Figura 3

Las respuestas son del tipo HTTP:

1xx	Informational (100 Trying, 180 Ringing, 181 Call is being forwarded)
2xx	Successful (200 OK, 202 Accepted)
3xx	Redirection (300 Multiple choices, 301 Moved Permanently, 302 Moved Temporarily)
4xx	Client Error (400 Bad Request, 404 Not Found, 482 Loop Detected, 486 Busy here)
5xx	Server Failure (500 Server Internal Error, 501 Not Implemented)
6xx	Global Failure (600 Busy Everywhere, 603 Decline).

SIP se puede definir como un protocolo de control, pensado para la creación, modificación y terminación de sesiones, con uno o más participantes. Esas sesiones pueden comprender conferencias multimedia, llamadas telefónicas sobre Internet (o cualquier otra red IP), distribución de contenidos multimedia... Las sesiones pueden realizarse en multicast o en unicast; los participantes pueden negociar los contenidos y capacidades que van a utilizar; soporta movilidad de los usuarios, mediante utilización de proxies.

Las funcionalidades que se le exigen a un protocolo de estas características, son básicamente: La traducción de nombres y las ubicación de usuarios, la negociación de capacidades de cada usuario, la gestión de los usuarios que toman parte en una conferencia (sesión) y la gestión de los cambios en las capacidades de cada participante.

SIP propone la utilización de un direccionamiento análogo al que se usa para el servicio de correo electrónico (e.g. sip:paco@bbva.com). Para la descripción de contenidos, puede utilizar MIME, estándar de facto en Internet; aunque el IETF sugiere, para la descripción de la propia sesión, la utilización de SDP (Session Description Protocol), que no es un protocolo propiamente dicho, sino un formato [de texto plano] para describir los flujos multimedia que se intercambian en una sesión. Al igual que el servicio de correo, utiliza DNS para encontrar el servidor adecuado al que se le debe pasar una determinada petición. Está pensado para ser independiente de los niveles inferiores; sólo necesita un servicio de datagramas no fiable, con lo cual se puede montar sobre UDP o TCP. Sobre ese servicio no fiable se monta un transporte con RTP/RTCP.

La Figura 4 pretende ponernos un poco en situación, representando los protocolos implicados en los aspectos de señalización (H.323, SIP, RTCP), provisión de calidad de servicio (RTCP, RSVP), transporte y encapsulación de contenidos multimedia y/o de medios múltiples (H.261, MPEG/RTP) que aparecen en escena cuando se aborda el problema del establecimiento, control y transporte de sesiones, que soportan comunicaciones multimedia entre varios participantes.

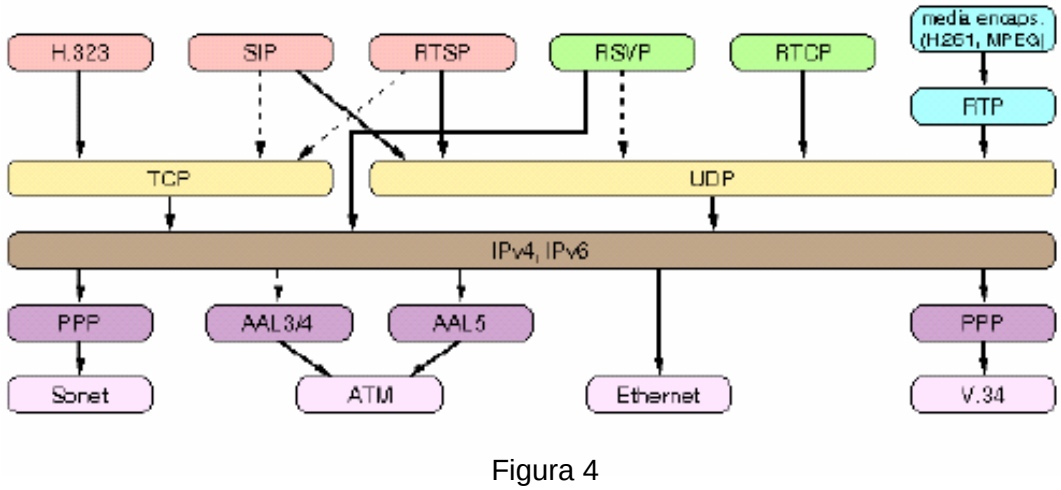


Figura 4

2.7. ARQUITECTURA DEL PROTOCOLO SIP.

SIP necesita dos componentes básicos: un agente de usuario (UA, User Agent) y un servidor (NS, Network Server). El agente de usuario, comprende un elemento cliente (UAC, User Agent Client) y un elemento servidor (UAS, User Agent Server). El cliente inicia las llamadas, y el servidor las responde: la idea es realizar llamadas (establecer sesiones 'peer-to-peer', P2P) con un protocolo Cliente/Servidor.

Las funciones principales de los servidores SIP son la resolución de nombres y la ubicación de usuarios. Se comunican con otros servidores pasándose mensajes en base a protocolos NHR. Los servidores pueden guardar o no información de estado, dando lugar a dos modos de funcionamiento ('statefull' o 'stateless' respectivamente para los anglosajones). Los servidores sin estado constituirían lo que se podría denominar el 'backbone' de una infraestructura SIP, mientras que los servidores con estado serían los dispositivos más cercanos alos agentes de usuario, que se encargarían del control de los dominios de usuarios.

Otras funcionalidades importantes de los servidores son la redirección (de una petición) y la "distribución" (pueden pasar una llamada a un grupo de usuarios, apropiándose de la sesión el primero que conteste).

Con esos componentes, UAC, UAS y NS, se puede montar una infraestructura básica de SIP; sobre la cual se pueden montar servidores de aplicaciones que podrían alojar módulos de servicio: de mensajería instantánea, de presencia, de control de llamada, perfiles de usuario... Al mismo nivel se supone que interaccionarían con otros servidores de contenidos en una arquitectura distribuida que integraría el balanceo de carga y soportaría la interfaz de gestión.

En el Diagrama 1 se pretende ilustrar el establecimiento de una llamada para mostrar cómo interactúan los elementos básicos que hemos mencionado más arriba.

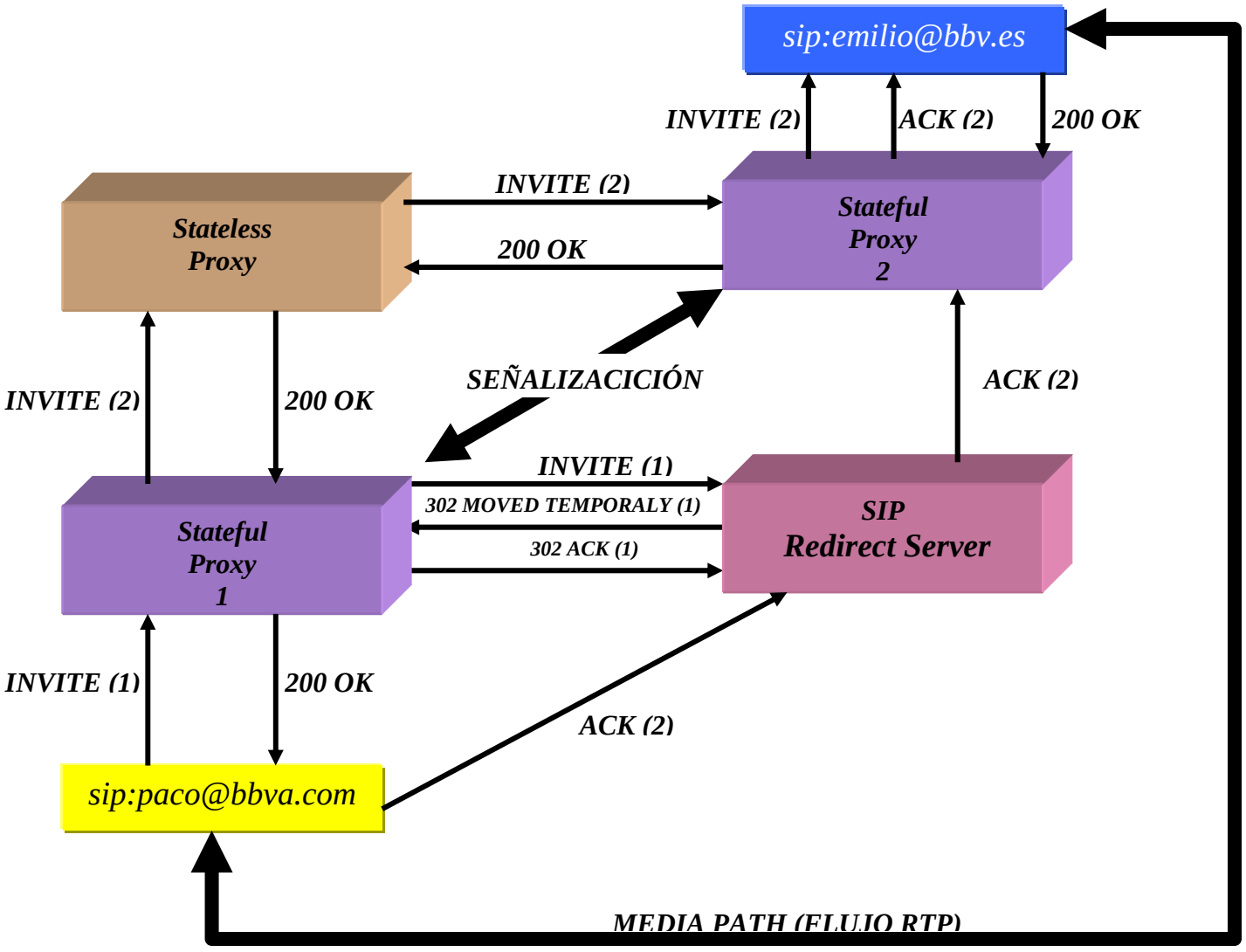


Diagrama 1. Establecimiento de una llamada utilizando SIP

En este ejemplo, el usuario paco@bbva.com quiere hablar con emilio@bbva.com es decir con un usuario que habitualmente está en su mismo dominio; pero por algún motivo, que desconocemos, hoy no está en bbva.com, sino en bbv.es aunque paco no lo sabe: tal es así que manda una invitación (invocará un método INVITE) para el usuario emilio@bbva.com al servidor responsable de su dominio (en este caso es un servidor proxy con estado, 'Stateful Proxy 1'). El servidor enviará la invitación a un servidor para de redirección para tratar de averigüar la localización actual de emilio. Es este servidor de redirección el que determina que el usuario emilio está en el dominio bbv.es y le contesta al proxy con un 302 MOVED TEMPORARILY que incluye la nueva dirección de emilio(sip:emilio@bbv.es). El proxy responde con un 302 ACK, puesto que aquí termina la secuencia de la invitación inicial (INVITE(1) de la figura).

A partir de esta situación, el Proxy 1 [con estado] (Stateful Proxy 1) podría mandarle la dirección de emilio a paco para que él tratara de comunicarse con ´directamente con sip:emilio@bbv.es. En el ejemplo, lo que hace el proxy 1 es modificar la invitación y tratar de encontrar a sip:emilio@bbv.es. Como no conoce a ningún otro servidor con estado que se responsabilice del dominio bbv.es, pasará la invitación a un servidor sin estado ('Stateless proxy') que conocerá el siguiente salto que debe seguir para llegar hasta sip:emilio@bbv.es. Para simplificar el ejemplo hemos querido que ese primer proxy sin estado conozca a un servidor proxy que controla el dominio bbv.es ('Stateful Proxy 2'). Ese segundo proxy completa la entrega de la invitación para sip:emilio@bbv.es; momento en el cual emilio acepta la llamada enviando un mensaje de respuesta (200 OK), que recorre el mismo camino de vuelta de la invitación hasta llegar a sip:paco@bbva.com. Ahora paco debería mandarle un ACK de esta respuesta a emilio; y aunque en principio podría hacerlo directamente, en nuestro ejemplo hemos decidido que toda la señalización pase por los proxies de cada dominio (se supone que así lo habrán indicado en los mensajes de invitación que se han cruzado).

SIP sigue el modelo Cliente/Servidor: los proveedores de servicio [de acceso troncal] podrían ofrecer esa infraestructura SIP como un servicio IP más a otros proveedores de servicio, que a su vez podrían montar sobre ella sus propios servicios SIP que comercializarían en modo ISP/ASP.

SIP proporciona los mecanismos necesarios para ofrecer una serie de servicios:

Usuarios:

1. Localización.
2. Disponibilidad y capacidades (servicio de presencia y terminal asociado).
3. Perfil.

Llamadas

1. Establecimiento.
2. Mantenimiento.
3. Desvíos.
4. Traducción de direcciones.
5. Entrega de los números llamado y llamante.
6. Movilidad: direccionamiento único independiente de la ubicación del usuario.
7. Negociación del tipo de termina.l
8. Negociación de las capacidades del terminal.
9. Autenticación de usuarios llamado y llamante.
10. Tranferencias ciegas y supervisadas.
11. Incorporación a conferencias multicast.

SIP mecanismos necesarios para ofrecer una serie de servicios según se puede ver en la figura 5:

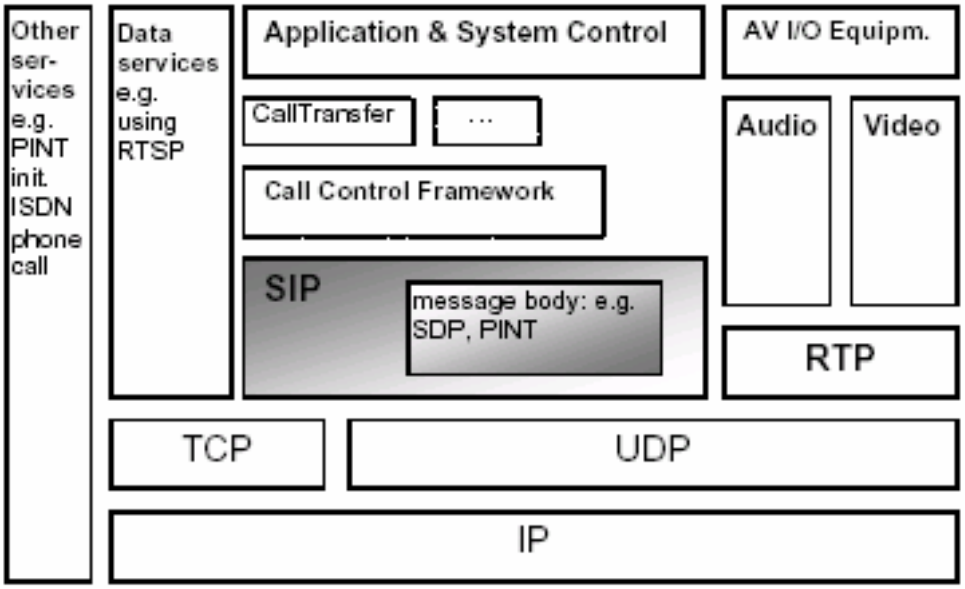


Figura 5

2.8. MENSAJERÍA INSTANTÁNEA (IM) DEL SIP.

La mensajería instantánea puede que merezca un apartado aparte, puesto que se ha convertido, por su sencillez e inmediatez, en un medio de comunicación que resulta adecuado para el intercambio rápido de ideas entre pequeños equipos de trabajo distribuidos. El concepto de la "lista de amiguetes" ('buddy list') que ha surgido en entornos de IM como AOL o ICQ resulta interesante: es el hecho de poder disponer de una lista de usuarios de un servicio, con su disponibilidad online anunciada constantemente en la red. Es un servicio que se integra fácilmente, puesto que se trata de clientes muy ligeros.

AOL y Yahoo han conseguido congregar una gran comunidad de usuarios en entornos corporativos (¿Quién no se ha pasado la mitad de la jornada mandándose mensajitos con sus colegas en el Yahoo Messanger?). Lotus y Microsoft (M$) están integrando servidores de IM en sus plataformas corporativas; e incluso es una funcionalidad que se está integrando en muchas plataformas CRM, como un canal más de contacto con el cliente.

Una sesión que se establece con SIP puede incluir cualquier medio de soporte, de manera que podemos pasar una comunicación vía IM a una conferencia telefónica, una pizarra compartida tipo NetMeeting o una videoconferencia. Podemos pensar en una especie de "telefonía instantánea" como evolución.

En el mundillo de la telefonía móvil hay un claro precedente de la IM: el servicio de SMS. Tanto Yahoo como AOL han visto la potencialidad de este servicio y ya se están moviendo para alcanzar acuerdos con proveedores de servicios móviles.

Ese concepto de presencia asociado a las 'buddy lists' también está evolucionando; se habla de presencia no sólo a nivel del propio PC del puesto, sino asociado con cualquier tipo de dispositivo o aplicación independiente: es el caso de los 'bots' que IBM utiliza en su Lotus SameTime: son 'buddy lists' que representan realmente consultas a bases de datos o directorios corporativos. En principio se trata de la extensión del concepto de mensajería instantánea a un contexto mucho más amplio del que propició su origen: estamos hablando del intercambio de mensajes entre usuarios, que pueden ser personas (usuarios finales del servicio que tendrán uno u otro perfil asociado), máquinas (cualquier tipo de terminal asociado a un usuario), o aplicaciones (que pueden incluir agentes inteligentes o servicios Web).

Todas las posibilidades que se han mencionado nos llevan a la integración de todo tipo de comunicación en el “escritorio” del puesto de cada empleado, posibilitando la gestión conjunta de todos los medios de comunicación a disposición de aquellos, con un ‘repositorio’ único de contactos a mantener. Este aspecto resulta de un interés indudable en el entorno empresarial, puesto que redunda de forma directa en el incremento de la productividad de los empleados, permitiendo el despliegue de servicios de valor añadido como cualquier otro servicio sobre una arquitectura SIP apoyada en una red IP multiservicio.

A pesar del ámbito de este documento, no debemos olvidar que, la que en boca de muchos es la ‘killer application’ que servirá de catalizador para los servicios de banda ancha en el acceso, los juegos en red, se beneficia enormemente de las posibilidades que ofrece SIP. Una sesión de juego en red (‘online gaming’) es una comunicación sobre UDP que se establece entre sockets seguros, durante la cual se intercambian flujos multimedia RTP. Además hoy en día ya se incorporan servicios de IM para la comunicación y coordinación táctica de los jugadores. SIP va a permitir evolucionar hacia un escenario de mayor interactividad con comunicación vía VoIP entre los jugadores; de la misma forma el servicio de presencia permitirá evitar la necesidad de conectarse con un servidor maestro para iniciar las partidas, pudiendo utilizar una lista para ver quién está conectado en cada momento e invitarle a una partida sobre la marcha.

2.9. PROTOCOLO H.248 (MEGACO).

Este protocolo se define en la Recomendación H.248 de la ITU-T. El protocolo H.248 o Megaco permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de siguiente generación. El protocolo Megaco, que tiene su origen en el protocolo MGCP (Media Gateway Control Protocol, Protocolo de control de puerta de enlace al medio), proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP. Megaco está adquiriendo solidez en el mercado porque permite una mayor escalabilidad que H.323, y da respuesta a las necesidades técnicas y a las funciones de conferencia multimedia que se pasaron por alto en el protocolo MGCP.

Funcionalmente, Megaco es un protocolo de señalización utilizado entre los elementos de una arquitectura distribuida que incluye media gateway y controladores de media gateway (conocidos a menudo como softswitches, gatekeeper o call server)

H.248 es el resultado de la cooperación entre la ITU y el IETF. Antes de lograr esta cooperación existían varios protocolos similares compitiendo entre si, principalmente MGCP (la combinación de SGCP e IPDC) y MDCP. H.248 se considera un protocolo complementario a H.323 y SIP, ya que un Media Gateway Controller (MGC), controlará varios Media Gateways utilizando H.248, pero será capaz de comunicarse con otro MGC utilizando H.323 o SIP.

2.9.1. MGCP.

El MGCP es, en esencia, un protocolo maestro/esclavo, donde se espera que los gateways ejecuten comandos enviados por el MGC. El Protocolo de Control de Media Gateway (MGCP) es usado para controlar los gateways de telefonía desde los elementos de control de llamadas externos llamados Media Gateways Controllers (MGC) o Gatekeepers. Un gateway de telefonía es un elemento de red que provee conversión entre las señales de audio transportadas sobre los circuitos telefónicos y los paquetes de datos transportados sobre la internet o sobre otra red de paquetes.

MGCP asume una arquitectura de control de llamada, donde la inteligencia del control de la llamada está fuera de los gateways y manejada por un elemento de control de llamada externo. El MGCP asume que estos elementos de control de llamadas o MGC, se sincronizarán entre sí para enviar comandos coherentemente a los gateways que están bajo su control.

Lo que se propuso con MGCP fue sacar el control de la señalización del propio gateway (GW), llevándolo a otro elemento, el 'media gateway controller' MGC (que se conoce como 'softswitch') que se encargará del control de los media gateways'(MGW). A nivel de sistemas lo que se ha hecho es desagregar el gatekeeper (GK) en sus equivalentes en el mundo SS7. Esta iniciativa surgió de varios fabricantes con el nombre de IPDC (Cisco, Alcatel, 3Com et al.) por un lado y SGCP (Telcordia) por otro; un esfuerzo que el IETF aglutinó bajo la denominación de MGCP y asignada a la responsabilidad del grupo de trabajo Megaco. MGCP es en la fecha de redacción de este documento un documento de trabajo. Tanto IETF como la ITU-T trabajan para llegar a un estándar, el primero bajo la responsabilidad de Megaco y como H.248 para el segundo.

En MGCP se puede decir que se ha separado la "inteligencia" (las funciones de control) de los datos (los contenidos: 'the media'). Que se trata de un protoclo Maestro/Esclavo. El maestro es el MGC ('softswitch' o 'call agent') y el esclavo es el

MGW (que puede ser un GW de VoIP, un DSLAM, un router MPLS, un teléfono IP,...). Esta es precisamente la característica que más choca con la filosofía (P2P) de SIP. Otra característica interesante es que intenta reproducir el modelo de la PSTN/IN sobre IP (en la Figura 6 se ilustra el escenario típico para un despliegue tipo 'Internet Telephony' que es la aplicación para la que se pensó, al menos en principio esta solución), en contra del modelo distribuido que propone SIP.

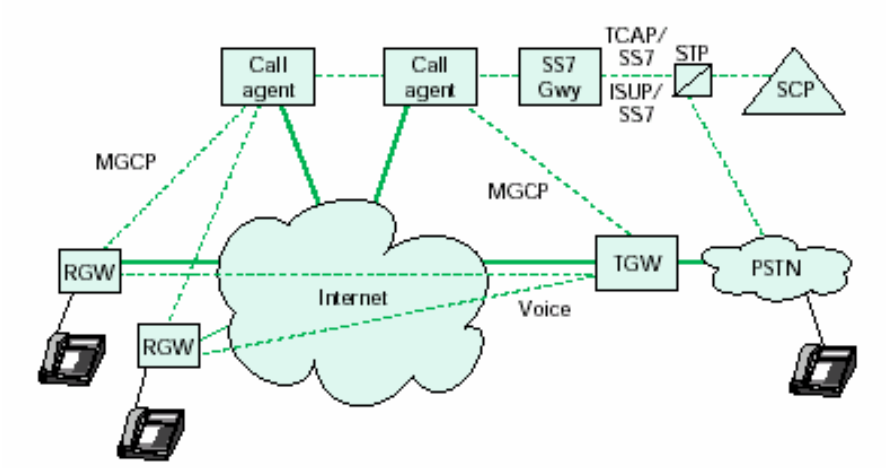


Figura 6

El Megaco pretende dar una solución basada en una visión propia de las Telcos tradicionales, una oficina central (Central Office, CO, en este caso IPCO) y una red de sucursales (Branch Offices, BO). Tal y como se observa en la Figura 7, SIP puede complementar a MGCP en un escenario donde tengamos varios MGC.

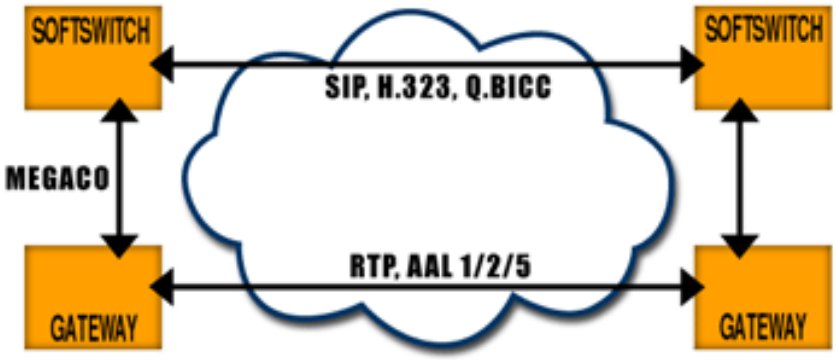


Figura 7

En la Figura 8 se detalla un poco más lo que sería un escenario integrado con la PSTN, pensando en prestar el servicio de telefonía sobre Internet.

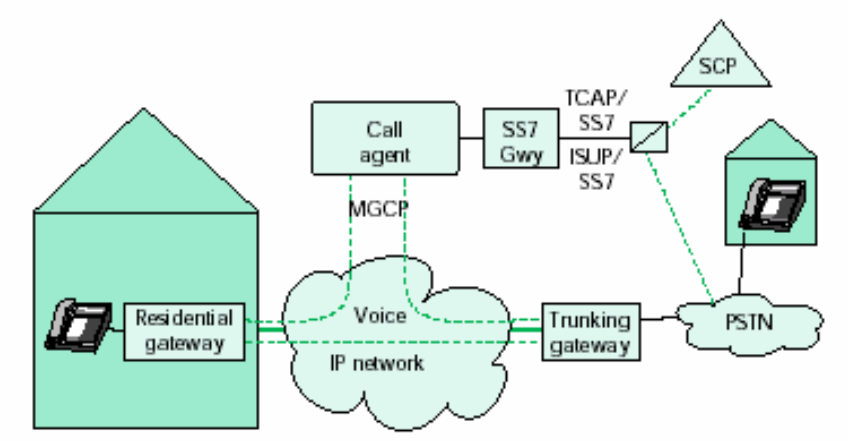


Figura 8

Un tema de debate importante es la utilización de MGCP para controlar los terminales (los teléfonos IP por ejemplo); el problema que surge es que sólo soporta servicios básicos de red inteligente. El tema es que si se quieren desplegar servicios avanzados necesitamos montar SIP tanto en los terminales como sobre la red de señalización, realizando las funciones de control asociadas al servicio.

Ya se ha comentado más arriba que la visión de los partidarios de MGCP es que la inteligencia del servicio esté pegada a los MGC (softswitch), y de hecho en el corto plazo es un planteamiento adecuado puesto que el esfuerzo de convergencia se centrará en los puntos de interconexión entre la PSTN y la red IP, y pro tanto interesará que los servidores SIP estén junto a los MGC en la CO. Pero, según avancemos hacia un escenario más integrado, la atención se centrará en la infraestructura IP, con lo cual la función de los MGC se alejará de los puntos de interconexión. Finalmente, en un entorno IP puro, la función de creación de servicios se distribuirá por toda la red: se puede extender el modelo ASP para dar servicios de voz. Tanto los ASPs como los ISPs, o incluso los propios usuarios finales pueden crear sus propios servicios. Se puede pensar en un escenario basado en SIP, donde se utilice MGCP para controlar internamente un GW de Telefonía IP (TIP) y los servidores de aplicaciones SIP distribuirían servicios por la red a través de los servidores proxy SIP.

Como conclusión debemos extraer el hecho de que MGCP no se puede considerar como un competidor de SIP, puesto que ambos resultan complementarios en ciertos aspectos, mientras que son mutuamente excluyentes en otros.

Esta idea de dividir el Gateway de voz en varias entidades funcionales se ha propuesto también desde iniciativas como TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) de la ETSI, con la intención de proporcionar una arquitectura “escalable” que soporte el servicio de Telefonía IP con la necesaria capacidad para convivir con las redes tradicionales de conmutación de circuitos (SCN, Switched Circuit Networks) como la PSTN. Esta división es la que se ilustra en el Diagrama 2 (de la misma forma en la Figura 9 podemos ver los componentes e interfaces en cuya definición trabaja la ETSI en el ámbito de TIPHON).

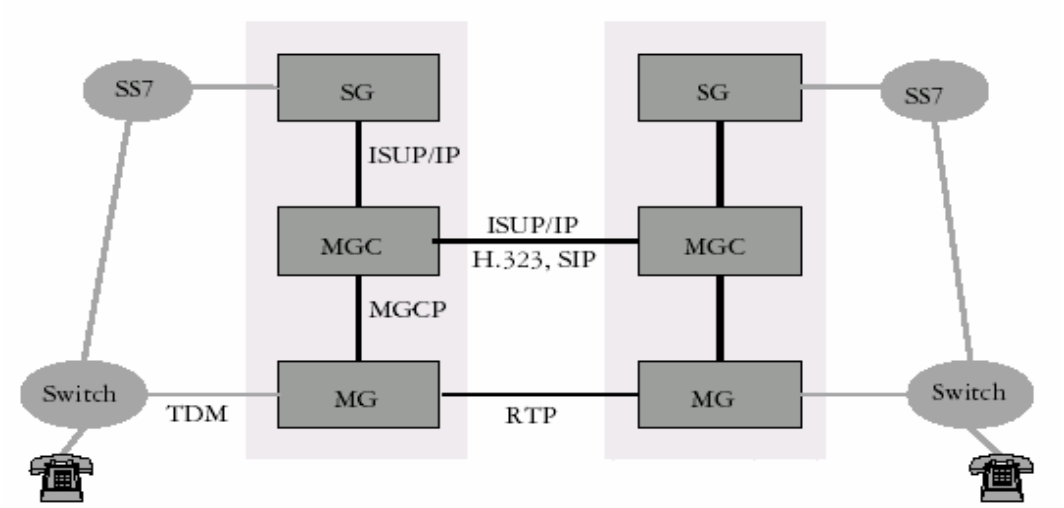


Diagrama 2. Descomposición del Gateway e interacción con la PSTN

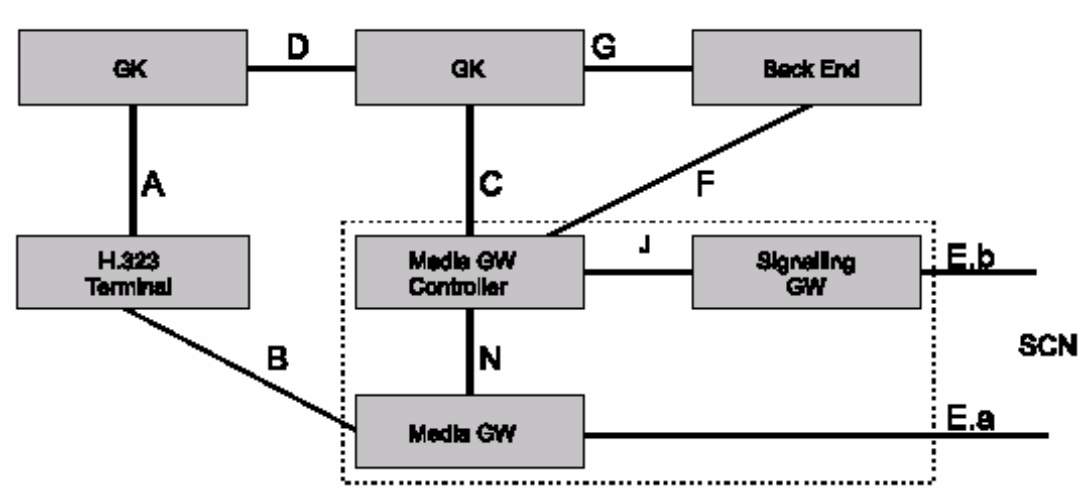


Figura 9

2.10. SIGTRAN.

2.10.1 ¿QUÉ ES EL SIGTRAN ?

SIGTRAN (de signalling transport) es el nombre del grupo de trabajo del IETF encargado de definir una arquitectura para el transporte de señalización en tiempo real sobre redes IP. A raíz de ello, no sólo se creó una arquitectura, sino que se definió un conjunto de protocolos de comunicaciones para transportar mensajes SS7 sobre IP.

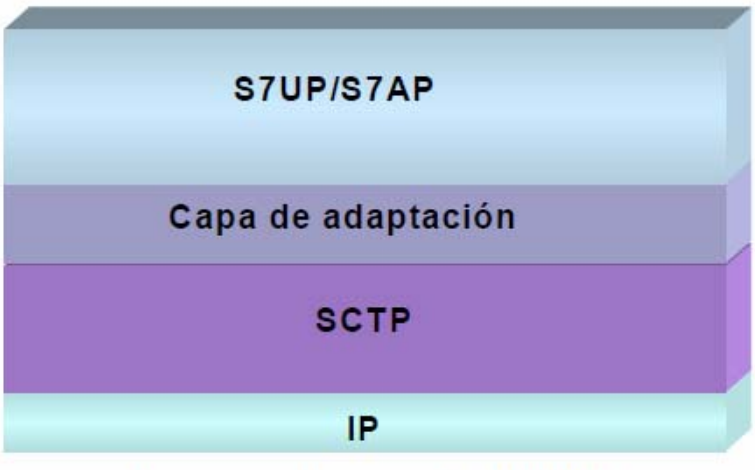
2.10.2 ARQUITECTURA DE LOS PROTOCOLOS SIGTRAN .

La arquitectura definida por el Sigtran [RFC2719] consta de tres componentes:

• IP estándar como protocolo de red.

• Un protocolo común de transporte de señalización. Los protocolos definidos por el Sigtran se basan en un nuevo protocolo de transporte sobre IP, llamado SCTP (Stream Control Transmission Protocol).

• Capas de adaptación específicas para cada capa de la torre SS7 que se necesite transportar. El IETF ha definido las siguientes: M2PA, M2UA, M3UA, SUA, TUA e IUA. IP SCTP Capa de adaptación S7UP/S7AP



Arquitectura de protocolos SIGTRAN

2.11. M2UA [RFC 3331].

M2UA son las siglas de MTP2 User Adaptation. El protocolo M2UA, al igual que M2PA, adapta MTP3 a SCTP, e igualmente gestiona asociaciones SCTP en lugar de enlaces MTP3. M2UA permite el intercambio de mensajes MTP3 entre dos puntos de señalización IP o entre un punto de señalización IP y una pasarela IP-SS7.

M2UA es un protocolo entre pares en caso de que la comunicación comience y termine en dos puntos de señalización IP, sin SGWs intermedios, tal como muestra la Figura 12.

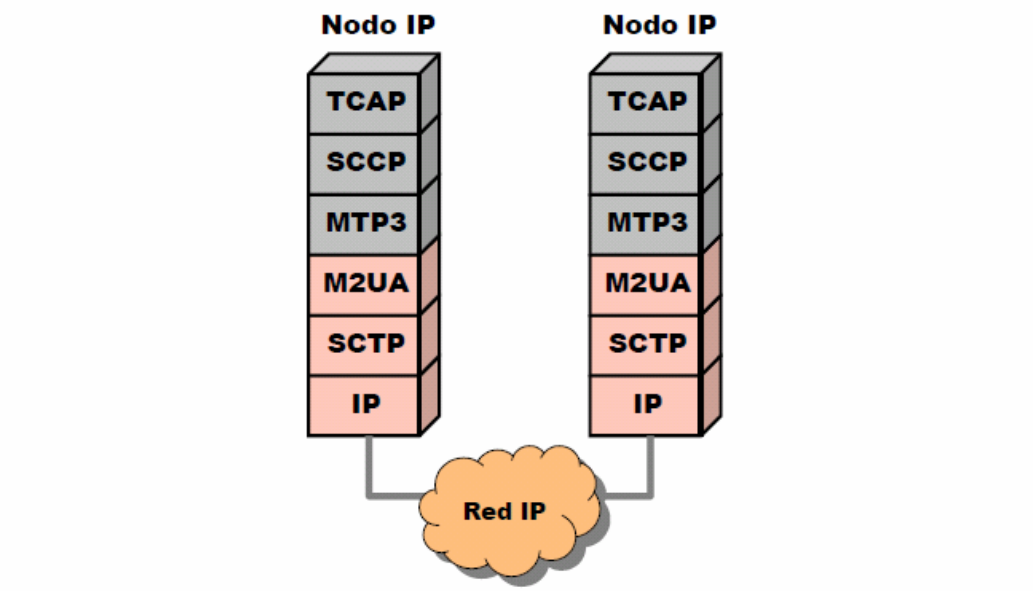


Figura 12. Transporte de MTP3 entre dos puntos de señalización IP, mediante M2UA

Sin embargo, M2UA no es un protocolo entre pares si se implementa en una pasarela de señalización. En ese caso, M2UA no procesa las órdenes (primitivas del protocolo) que le llegan desde la capa superior (MTP3), sino que las envía tal cual hacia un nodo remoto, mediante SCTP.

Como M2UA no procesa las primitivas de MTP3, sino que las reenvía, en caso de que se utilice un SGW se debe entender este protocolo como un medio que comunica la capa MTP3 de un nodo IP con la capa MTP2 de un SGW, tal como muestra la Figura 13.

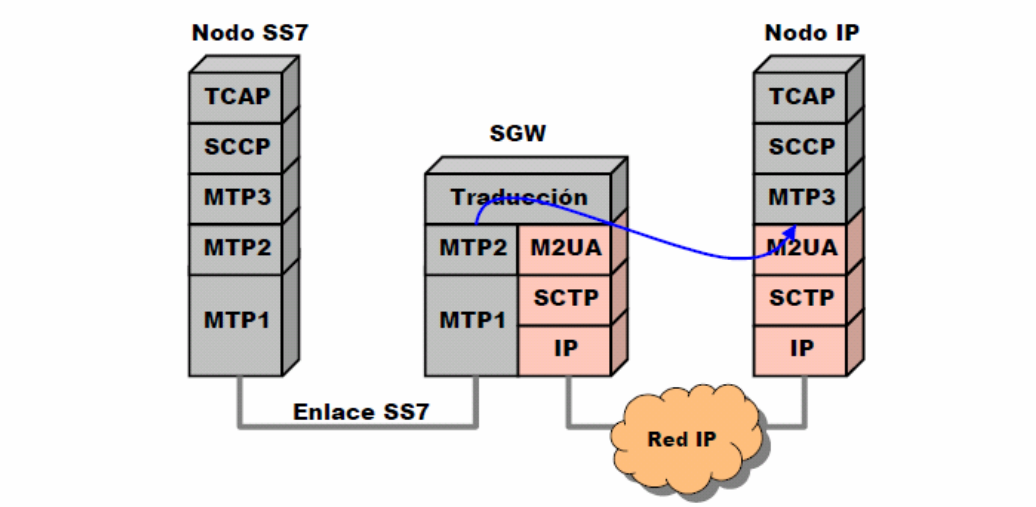


Figura 13. Transporte de primitivas MTP3 hacia una capa MTP2 remota, mediante M2UA.

De esta forma, varios puntos de señalización IP con MTP3 sobre M2UA pueden acceder a la red SS7 tradicional a través de los mismos enlaces MTP2 físicos.

Es importante tener en cuenta que, debido a la propia naturaleza del protocolo, sólo puede existir un SGW M2UA en una misma comunicación MTP3, por lo que no se puede utilizar para transportar mensajes MTP3 entre dos nodos SS7 puros a través de una red IP. Si se utiliza M2UA, alguno de los extremos es un punto de señalización IP.

2.12. M3UA [RFC 3332].

M3UA son las siglas de MTP3-User Adaptation. M3UA es un protocolo que transporta mensajes procedentes de un usuario de MTP3 (ISUP, TUP o SCCP) a través de una red SCTP/IP hasta un nodo remoto.

De forma similar a M2UA, M3UA simplemente transporta los mensajes hasta el destino, pero no realiza por sí mismo las funciones de la capa MTP3. Esto significa que M3UA no dispone de tablas de encaminamiento basadas en puntos de señalización, ni realiza ninguna otra función propia de MTP3.

En general, M3UA se utilizará como medio de transporte de primitivas entre la capa usuaria de MTP-3 (SCCP o ISUP) de un punto de señalización IP y la capa MTP3 de un SGW remoto, tal como muestra la Figura 14.

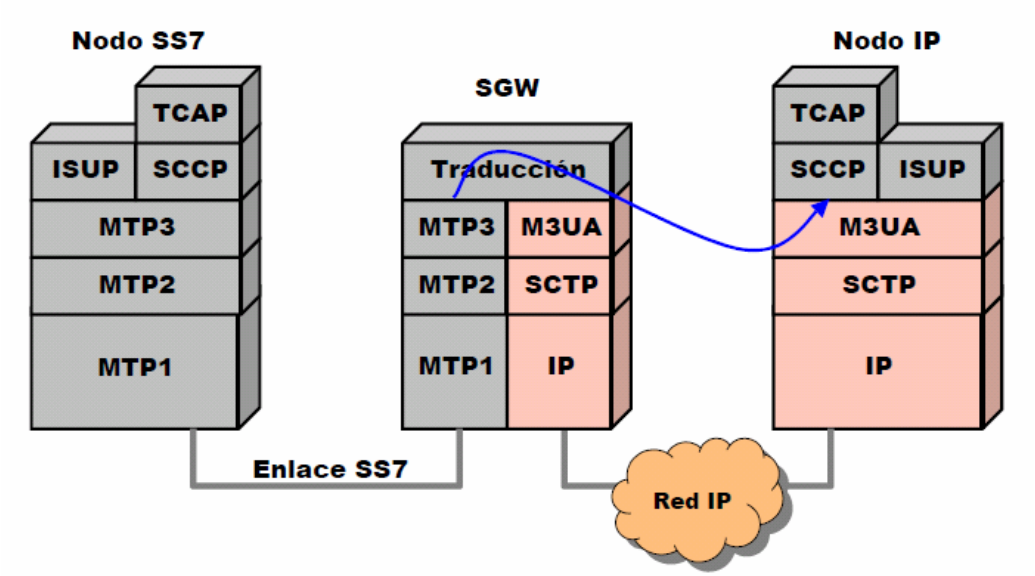


Figura 14. Transporte con M3UA de primitivas ISUP o SCCP hacia una capa MTP3 remota.

2.12.1. UTILIZACIÓN DE M3UA.

Como se ha visto, dado que M3UA transporta primitivas desde la capa ISUP o SCCP de un nodo hasta la capa MTP3 de otro (típicamente un SGW), este protocolo sólo puede utilizarse para conectar nodos con señalización IP a una red SS7. Por tanto, no se puede utilizar M3UA para descargar tráfico SS7 entre dos nodos TDM a través de red IP, a no ser que se utilicen SGWs con SCCP. Pero para esta aplicación es mucho más adecuado utilizar SGWs con M2PA, por los motivos indicados en el apartado 3.3.

2.13. CARACTERÍSTICAS PRINCIPALES DEL SIGTRAN.

Debido a los inconvenientes mencionados de TCP y UDP, el SIGTRAN definió del protocolo SCTP, cuyas principales características son las siguientes:

• Es un protocolo punto a punto. Se establece intercambio de datos entre dos extremos conocidos.

• Define tiempos de reintento (time-outs) mucho menores que los de TCP.

• Proporciona transporte fiable de datos de usuario, detectando y reparando los datos erróneos o fuera de secuencia. • Se adapta a la tasa de transferencia, disminuyendo la velocidad de envío de datos en caso de congestión en la red.

• Permite definir en un mismo extremo SCTP en varios servidores físicos (multihoming). Un único extremo SCTP se puede definir en varias direcciones IP.Hacia cada una de ellas se encaminan los mensajes de forma independiente, de manera que si uno de los nodos físicos queda fuera de servicio, el resto de comunicaciones no se ven afectadas.

2.13.1. FUNCIONES DE SCTP.

2.13.2 ESTABLECIMIENTO Y LIBERACIÓN DE ASOCIACIONES

Una asociación SCTP es una relación de comunicación de mensajes entre dos entidades SCTP (comunicación orientada a conexión). Las asociaciones SCTP se establecen a petición del usuario de nivel superior de este protocolo. Para proporcionar protección frente a ataques de denegación de servicio, se emplea un protocolo de establecimiento de asociaciones en cuatro pasos, basado en cookies [RFC2522].

2.13.3. ENTREGA ORDENADA DENTRO DEL STREAM DENTRO DEL SCTP.

Dentro del protocolo SCTP, se utiliza el término stream para referirse a una secuencia de mensajes de usuario que debe entregarse al nivel superior de forma ordenada. El número de streams que se enviarán a través de una asociación se define en el establecimiento de la misma, de forma negociada entre ambos extremos de la comunicación. Los streams son unidireccionales, de forma que para una comunicación bidireccional se deberán definir al menos dos streams en una asociación SCTP.

Los mensajes de usuario se asocian a streams determinados, de forma que el extremo receptor SCTP entrega al nivel superior todos los mensajes de un mismostream en el mismo orden en que se enviaron. Sin embargo, no existen restricciones de entrega ordenada entre mensajes de distintos streams de la misma asociación. De esta forma, los mensajes de un stream se pueden seguir entregando aunque otro esté bloqueado esperando el siguiente mensaje. Adicionalmente, SCTP proporciona un mecanismo para no utilizar el servicio de entrega ordenada de mensajes, de forma que los mensajes enviados mediante dicho mecanismo se entregan al nivel superior del destino SCTP tan pronto como se reciben.

2.13.4. FORMATO DE PAQUETES SCTP.

Un paquete SCTP se compone de una cabecera de 24 octetos y una serie de unidades de información, denominadas chunks. Estas unidades de información pueden contener datos de usuario, o instrucciones de control del propio protocolo SCTP (establecimiento y liberación de asociaciones, control de flujo, retransmisiones, etc). Los chunks tienen estructura propia, y presentan una serie de campos, dependiendo del tipo de chunk que sean.

En el ámbito de la planificación de una red SS7 sobre IP, el dato más relevante es el tamaño de las cabeceras de los datos de usuario. La cabecera de un chunk de datos de usuario mide 16 octetos, y pueden contener hasta 65520 octetos de información del nivel superior. Esto significa que, en principio, cualquier mensaje de cualquier operación MAP, ISUP o CAMEL cabe en un chunk de datos SCTP, incluyendo las cabeceras de los protocolos de adaptación intermedios.

Además, SCTP permite transportar varios mensajes de usuario en un único mensaje SCTP, mediante el uso de distintos chunks de datos dentro del mismo mensaje.

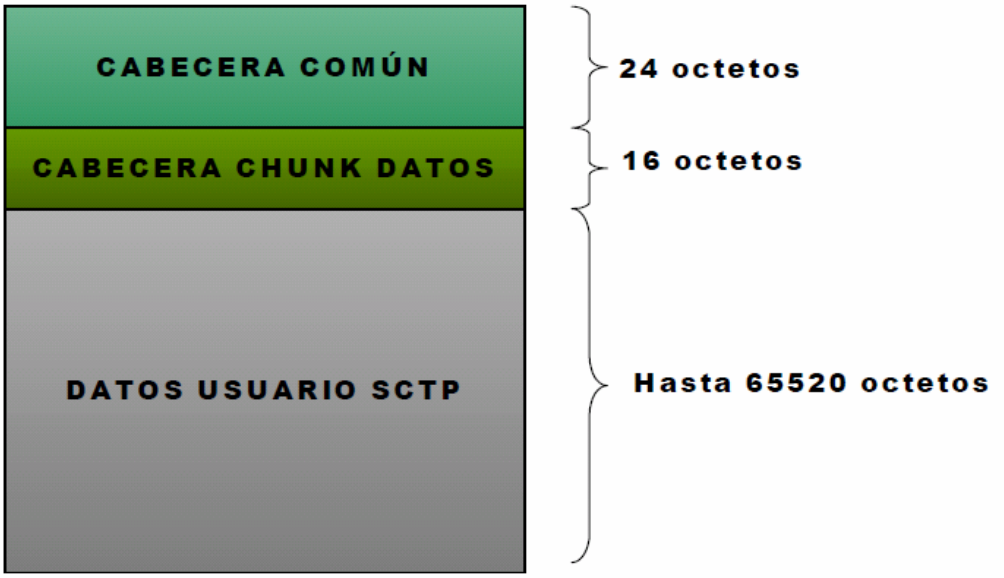


Figura 9 . Formato paquete SCTP con datos de usuario

2.13.5. VALIDACIÓN DE PAQUETES.

Dentro de la cabecera común de SCTP se incluye un campo de verificación obligatorio, aparte de otro campo de 32 bits con una suma de comprobación (checksum) frente a errores. El valor del campo de verificación obligatorio lo decide el extremo de la comunicación SCTP en el establecimiento de la asociación. De esta forma se consigue más protección frente a comunicaciones con suplantación de identidad. La suma de comprobación se calcula a partir de los datos de la propia cabecera SCTP y la protege frente a errores en la comunicación.

2.13.6. GESTIÓN DE CONEXIONES

El usuario del nivel SCTP puede manipular el conjunto de direcciones de transporte destino de los mensajes. La función de gestión de conexiones de SCTP escoge la dirección de transporte destino para cada paquete SCTP que se envía, basándose en las instrucciones del usuario de SCTP y en las direcciones disponibles alcanzables para ese destino SCTP.

En periodos de inactividad, la función de gestión de conexiones monitoriza la disponibilidad de los extremos de la comunicación mediante mensajes de comprobación (heartbeats). Si SCTP percibe algún extremo como inalcanzable informa a su usuario de nivel superior.En el establecimiento de la asociación, se define un camino primario para cada extremo SCTP, que es el que se usa en el envío normal de paquetes.

En el extremo receptor, la gestión de conexiones se encarga de comprobar la existencia de una asociación SCTP válida a la que pertenece cada paquete SCTP recibido.

2.13.7. FRAGMENTACIÓN DE LOS DATOS DE USUARIO

SCTP posee mecanismos de fragmentación y re-ensamblado de mensajes de usuario para adecuarlos al tamaño requerido por el nivel inferior (IP en el caso de SS7 sobre IP).

2.13.8 CONTROL DE ENTREGA DE MENSAJES.

SCTP asigna un número de secuencia de transmisión (TSN) a cada mensaje de datos de usuario, fragmentado o no. El TSN es independiente del stream por el que se envía el mensaje. El extremo receptor envía acuses de recibo (ACK) de todos los TSNs recibidos, aunque no lleguen de forma ordenada. De esta forma, la fiabilidad en la entrega de los mensajes se mantiene funcionalmente separada de la entrega ordenada dentro del stream.

CAPITULO 3

VOZ EN CONMUTACIÒN DE PAQUETES CxP

3. ¿QUÉ ES VOIP ?.

VoIP o Voz sobre IP, es una red de paquetes de datos para transportar tráfico de voz en tiempo real. Esta consiste de hardware y software y permite a las compañías y a las personas realizar conversaciones telefónicas sobre la red de datos. También puede ser definida como la habilidad para hacer llamadas telefónicas y enviar fax sobre la red de datos basada en IP con una adecuada calidad de servicio (QoS) y a una relación costo/beneficio superior. Esto también es conocido como telefonía por internet. Sin embargo, este último término es usado en referencia a las llamadas hechas sobre la internet pública y la VoIP es frecuentemente usada para referirse a las llamadas hechas en una red privada.

La red de voz tradicional o PSTN, usa técnicas de conmutación de circuitos. Esto significa que una comunicación particular usa un enlace dedicado durante la duración de la llamada. Aunque esta provee una conexión muy confiable para la transmisión de voz, hace un uso muy ineficiente del ancho de banda. Por otro lado, la red de datos generalmente usa conmutación de paquetes. Aquí se usa Conmutación de celdas estadísticas (STDM) con la finalidad de proveer un ancho de banda dinámico a una particular cadena de datos, basada en sus requerimientos y en los requerimientos y demandas de otros datos de la red. Esta provee un uso más eficiente de ancho de banda pero puede crear problemas para el tráfico de voz, el cual es sensible al retardo, debido a que cada paquete es enrutado individualmente a través de la red; esta conmutación de paquetes hace a la red menos eficiente en el tráfico de voz y presenta mayores retos a la calidad de la transmisión de voz. Esto incluye: pérdida de paquetes, retardo (eco), Jitter (variación en la velocidad de transmisión de paquetes de datos) y la entrega de paquetes poco confiable y fuera de orden debido a la naturaleza no orientada a conexión de la red de paquetes.

3.1. ARQUITECTURA.

Las llamadas de VoIP requieren al menos dos gateways de VoIP. Típicamente, un proveedor de servicios debería instalar gateways (o interactuar con otros proveedores de servicios y acceder a sus gateways) en todos los países o regiones hacia los cuales se realizan o se reciben llamadas. El resultado de la red de VoIP se compone de gateways, el acceso de la PSTN a cada gateway y la red IP que enlaza los gateways.

En la red telefónica IP, la información de señalización es intercambiada entre los siguientes elementos funcionales. Estos mismos se tomarán en cuenta para las configuraciones de red que se plantearán más adelante.

Media Gateway: la tecnología de VoIP permite que las llamadas originadas y terminadas en la PSTN, sean transportadas sobre la red IP, es decir, éste traduce TDM a paquetes. El gateway de VoIP sirve de puente entre la red PSTN y la red IP para ambos lados de origen y terminal de la llamada. Para realizar una llamada, el abonado llamante accederá el gateway mas cercano o por conexión directa o realizando una llamada sobre la red PSTN e ingresando el número telefónico de destino.

La tecnología de VoIP traduce el número telefónico de destino en la dirección de la red de datos ("dirección IP") asociada con el correspondiente gateway terminal mas cercano al número de destino. Usando el protocolo apropiado y la transmisión de paquetes sobre la red IP, el gateway terminal iniciará una llamada al número telefónico de destino sobre la red PSTN para completar el establecimiento de la comunicación en ambos sentidos con los extremos finales (punto a punto). A pesar de la conexión adicional requerida, el tiempo total del establecimiento de la llamada no es significativamente mas largo que con una llamada soportada por la PSTN.

Los gateways pueden emplear un protocolo común, por ejemplo, el H.323 o MGCP o un protocolo propietario, para soportar el estándar de señalización telefónico. Los gateways emulan las funciones de la PSTN en respuesta a los estados de cuelgue y descuelgue, recibiendo o generando dígitos DTMF y recibiendo o generando tonos de llamadas en progreso. Las señales identificadas son interpretadas y mapeadas para la transmisión del mensaje apropiado hacia el gateway con la finalidad de soportar el establecimiento de la llamada, mantenimiento, facturación y finalización de la llamada.

Media Gateway Controlador o Gatekeeper: un gatekeeper (GK) maneja los registros y la gestión de los recursos de los media gateways de manera que no se produzcan situaciones de saturación en la red. Un gatekeeper intercambia mensajes ISUP con las centrales telefónicas via un gateway de señalización. De esta forma el GK traduce direcciones telefónicas a direcciones IP.

La interpretación del número telefónico de destino en la dirección IP del media gateway terminal indicado es una función primordial del gatekeeper. La tabla de

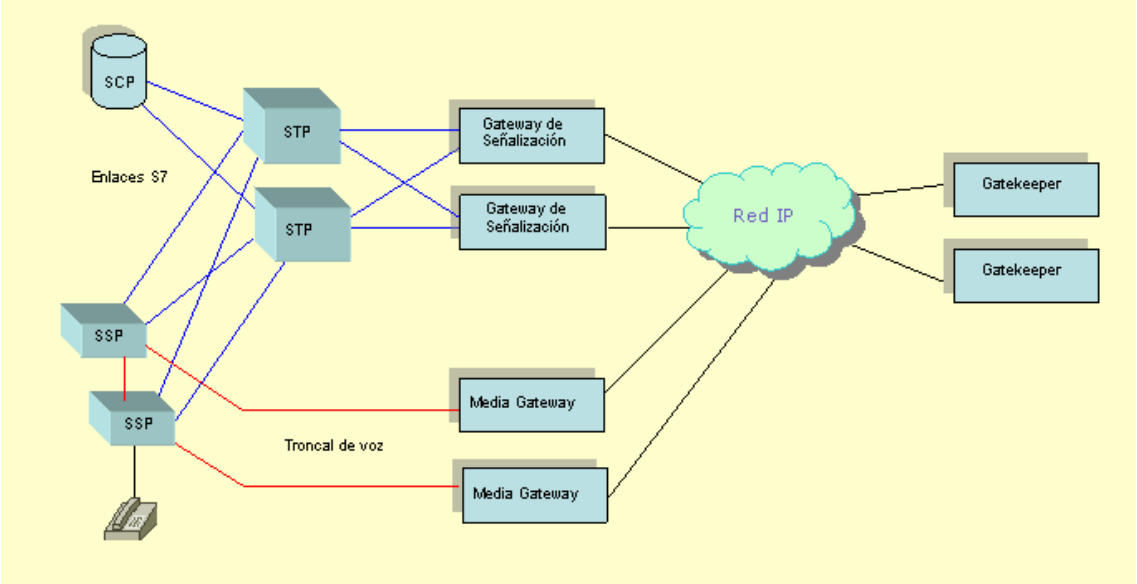
enrutamiento mantenida por el gatekeeper decide cual media gateway corresponde al número telefónico de destino con la finalidad de completar la llamada.

La funcionalidad del gatekeeper puede ser distribuída entre todos los media gateways de la red de VoIP o puede ser centralizada en una o varias localidades. Cuando las funciones del gatekeeper están implantadas en cada media gateway, todos los gateways de toda la red de VoIP actúan independientemente para coordinar sus acciones. Cuando un gatekeeper es centralizado, todos los media gateways de la red coordinan sus acciones con respecto al gatekeeper centralizado en lugar de que actúen independientemente.

Gateway de Señalización o Signaling Gateway: el gateway de señalización provee una traducción transparente de la señalización entre la conmutación de circuitos y la red IP. Un gateway de señalización puede señalizar en S7 (señalización Nº 7) o traducir y transmitir mensajes sobre una red IP a un media gateway controlador o a otro gateway de señalización. Debido a su rol crítico en la integración de la red de voz, los gateway de señalización son normalmente desarrollados en grupos de dos o más para asegurar alta disponibilidad.

La funcionalidad del media gateway, o gateway de señalización y/o media gatekeeper pueden estar separadas en dispositivos diferentes o integrados en una sola unidad.

Ejemplo de una configuración de red VoIP



3.2. CALIDAD DE SERVICIO (QOS).

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final. En esto influyen dos factores fundamentales:

- La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red.
- La demora extremo a extremo, debido a las sucesivos procesos de codificación, decodificación, paquetización y "encolados". Afecta la interactividad en la conversación y por tanto a la QoS.
- Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, jitter y pérdida de paquetes.

La preparación de los medios en los terminales para ser enviados y transferidos por la red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica demora de procesamiento y demora de empaquetado:

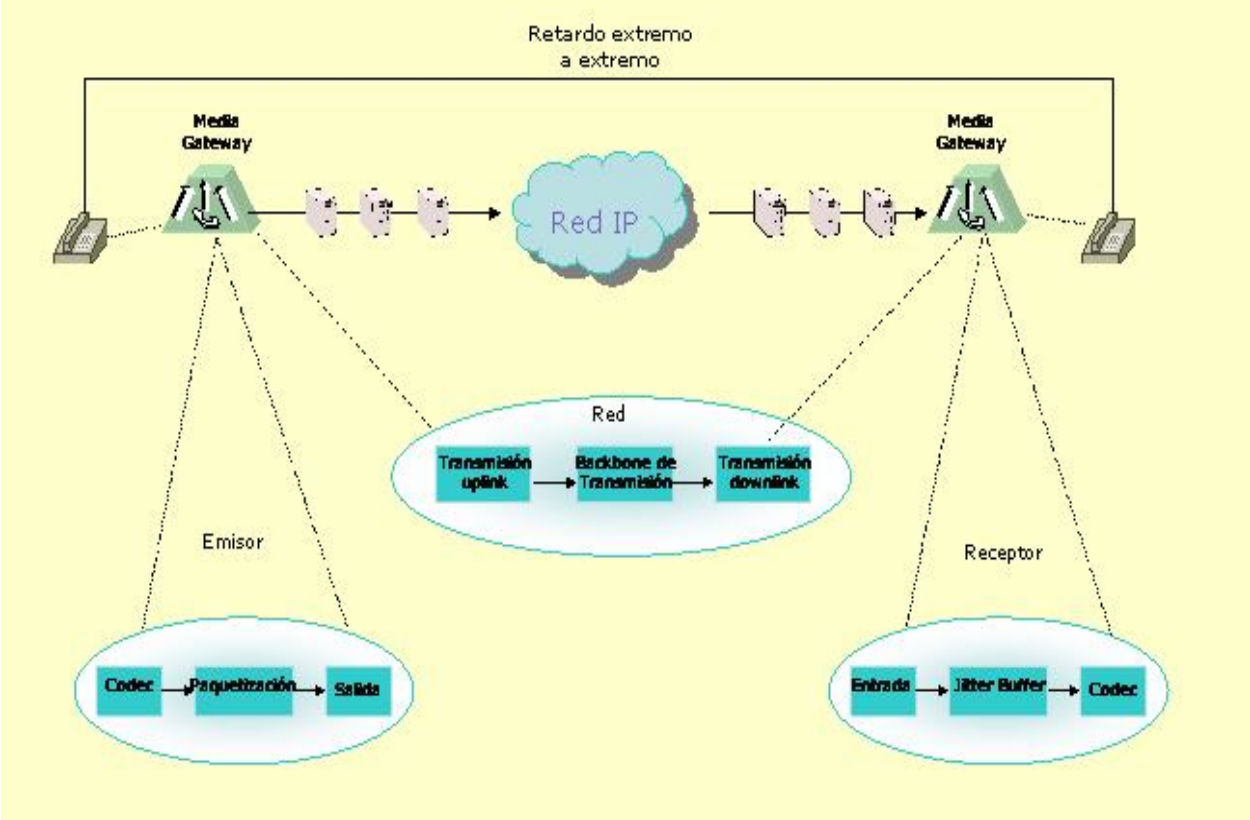
• Demora de procesamiento: demora producida por la ejecución del algoritmo de codificación, que entrega un stream de bytes listos para ser empaquetados.

• Demora de paquetización: es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados. Debe señalarse que el resultado de esta codificación – paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa el retardo y la distorsión de la señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación. Otro aspecto a considerar es el compromiso entre el retardo de paquetización y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de paquetización para cierto estándar de codificación. Claro está, según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50 %, con un crecimiento de la demora en forma exponencial en el

caso de los codecs de baja velocidad como el G.723.1. La demora de paquetización también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP. A las demoras de procesamiento y empaquetado se suma también la demora que introduce el proceso de buffering en los terminales, y la demora de "encolado" en la red. Todo esto da una demora extremo a extremo que percibe el usuario final en mayor o menor medida. A continuación se resumen los aspectos que afectan la QoS en las redes de VoIP.

3.3. RETARDO.

Se refiere sobre todo al tiempo de tránsito total, incluido el tiempo necesario para reconstituir el orden de los paquetes cuando se reciben y para compensar las fluctuaciones de los tiempos de tránsito (este tiempo de tránsito total debe ser inferior a 400 ms si se han de respetar las limitaciones de la conversación interactiva). Los excesivos retardos punto a punto hacen conversaciones difíciles y poco naturales. Cada componente en el camino de transmisión – emisor, red y receptor añaden retardo. ITU-TG.114 (tiempo de transmisión en un solo sentido) recomienda 150 mseg. como el máximo retardo deseado en un sentido para lograr alta calidad de la voz.



Retardo extremo a extremo

El retardo causa dos problemas: eco y traslape del habla. El eco es causado por las señales reflejadas por el equipo telefónico del extremo distante que regresan al oído del hablante. El eco llega a ser un problema significativo cuando el retardo del viaje redondo llega a ser mas de 50 milisegundos. A medida que el eco se incremente, los sistemas de paquetes se ven en la necesidad de utilizar controles como la cancelación de eco.

El traslape del habla (cuando dos personas hablan casi al mismo tiempo) es significativo si el retardo en una sola vía es mayor de 250 milisegundos. Por lo tanto el retardo completo llega a ser mayor. Algunas de las fuentes de retardo en una sola vía para una llamada hecha con paquetes de voz se describen a continuación

3.3.1. RETARDO ACUMULADO (Retardo algorítmico).

Es causado por la necesidad de recolectar un marco de muestras de voz para que sean procesados por el codificador de voz. Esto está relacionado con el tipo de codificador usado y varia de una sola muestra en el tiempo (.125 μsg) a muchos milisegundos.
Codificadores de voz y sus tiempos:

1. G.726 modulación adaptativa diferencial de pulsos codificados (ADPCM), 16, 24, 32, 40 Kbps = 0.125 μsg.
2. G.728 predicción lineal de excitación de código LD (CELP), 16 Kbps = 2.5 msg
3. G.729 CS-ACELP 8Kbps = 10 msg
4. G.723.1 codificador multitasa, 5.3, 6.3 Kbps = 30 msg.

3.3.2. RETARDO DE PROCESAMIENTO.

Es causado por el procesamiento de codificación y recolección de las muestras codificadas en paquetes para la transmisión sobre una red de paquetes. El retardo de codificación es una función del tiempo de ejecución del procesador y el tipo de algoritmo usado. A menudo se recolectan múltiples marcos de codificación de voz en un solo paquete para reducir la cabecera del paquete. Por ejemplo, 3 marcos de palabras codificadas en G.729 (equivalente a 30 milisegundos de habla) se recolectan y empacan en un solo paquete.

3.3.3. RETARDO DE RED.

Es causado por el medio físico y los protocolos usados para transmitir los datos de voz y por los buffers usados para remover el jitter en el lado receptor. El retardo de red es una función de la capacidad de los enlaces en la red y del procesamiento que ocurre a medida que los paquetes transitan por esta. Los buffer para jitter agregan retardo, que es utilizado para remover la variación de retardo a la que están sujetos los paquetes a medida que transitan en una red de paquetes.

3.4. COLAS.

S e definen como las que manejan el trafico mediante la asignación de distintas cantidades de espacio en la cola a las diversas clases de paquetes y a continuación dan servicio a las colas en la modalidad de ordenamiento cíclico. Aunque se puede asignar un mayor espacio en la cola a un protocolo, usuario o aplicación particular, ninguno de ellos podrá monopolizar nunca toda la anchura de la banda.

3.5. ECO.

El eco es el tiempo que transcurre entre la transmisión de una señal y su regreso al transmisor. Por lo general, este problema aparece en el contexto de las comunicaciones de PC a teléfono, de teléfono a PC o de teléfono a teléfono, y es causado por los componentes electrónicos de las partes analógicas del sistema que reflejan una parte de la señal procesada Un eco menor que 50 milisegundos es imperceptible. Por encima de este valor, el hablante oirá su propia voz después de haber hablado. Si se desea ofrecer un servicio de telefonía IP, las pasarelas tendrán que procesar el eco generado por la transferencia de dos a cuatro hilos, de lo contrario, no será posible utilizar el servicio con equipos analógicos clásicos. Como solución, se están instalando compensadores de eco de alta calidad en la pasarela de la red. A medida que el eco se incremente, los sistemas de paquetes se ven en la necesidad de utilizar controles como la cancelación de eco.

3.5.1. COMPENSACIÓN DE ECO.

El eco en una red telefónica, es causado por las reflexiones de señales generadas por un circuito híbrido que convierte de 4 hilos (un par para transmisión y uno para recepción) a 2 hilos (un solo hilo para transmisión y uno para recepción). Estas reflexiones de la voz del hablante son escuchadas por el oyente. El eco se presenta aún en las redes de conmutación de circuitos, sin embarco acá es aceptable ya que los retardos completos a través de la red son menores que 50 msg. Y el eco es enmascarado por el tono lateral que todo teléfono genera.

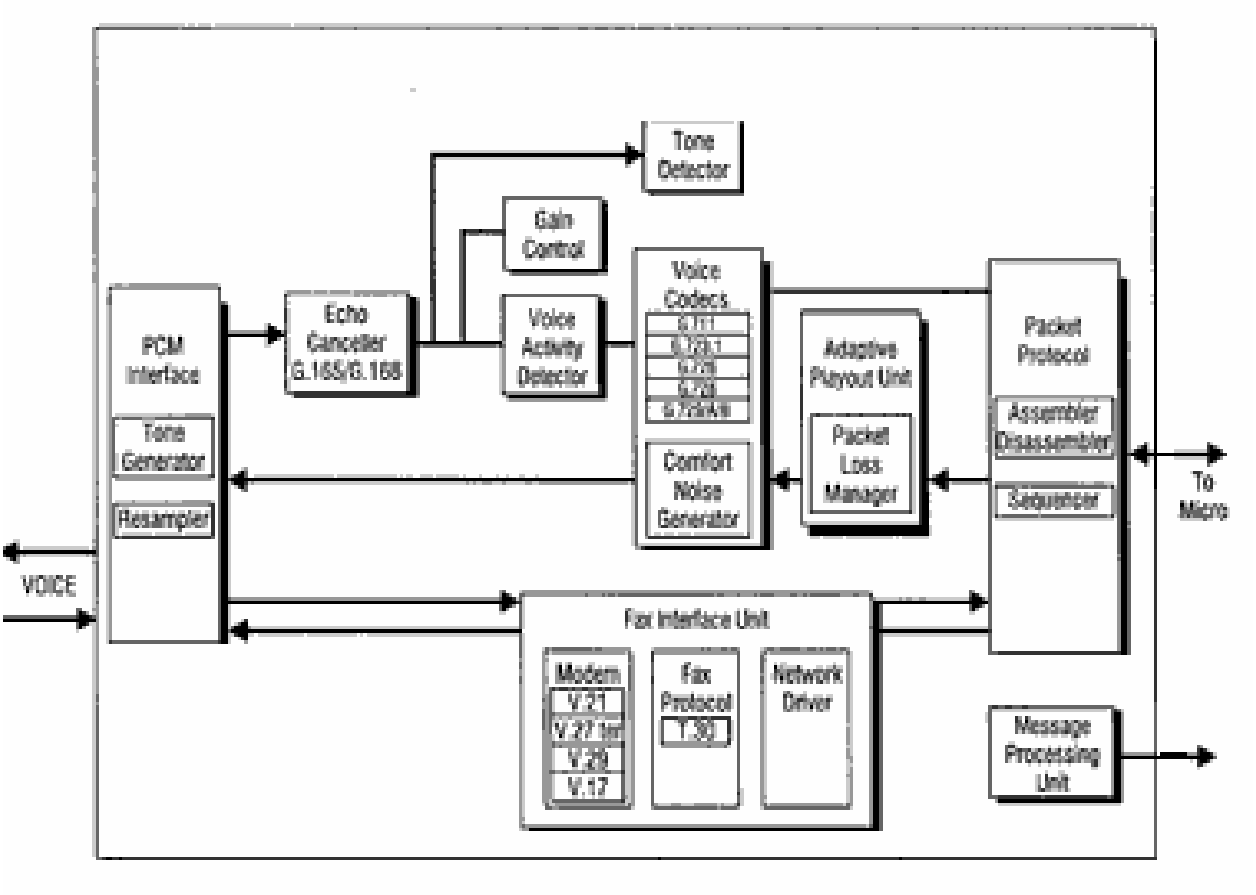
Existen dos (2) tipos de eco. Uno tiene alto nivel y poco retardo y se produce en el circuito híbrido de 2 a 4 hilos local; mientras que otro es de bajo nivel y gran retardo y se produce en el circuito separador híbrido remoto.

El eco es problema en una red de paquetes de voz cuando el retardo completo en la red es mayor que 50 msg, entonces se deben aplicar técnicas de cancelación de eco.El estándar G.165 de la UIT define el desempeño de los canceladores de eco, en la recomendación G.IEC se encuentran mas características.

El cancelador de eco compara los datos de voz recibidos de la red de paquetes con los datos de voz que están siendo transmitidos por la red de paquetes. Se construye mediante la técnica de ecualización transversal autoadaptativa. Consiste en usar una parte de la señal de transmisión para cancelar el eco producido por la desadaptación de impedancias en el circuito híbrido que convierte de 4 a 2 hilos.El eco del híbrido de la red de paquetes se remueve con un filtro digital en el camino de transmisión hacia la red de paquetes.

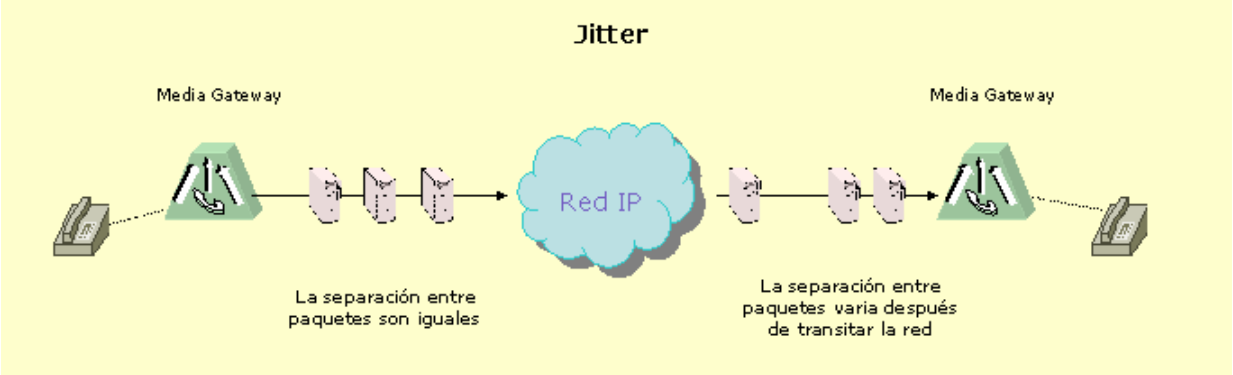
3.5.2. AMBIENTE DE PORTABILIDAD EN TIEMPO REAL.

Provee un ambiente de operación para el software que reside en el DSP. Esto hace funciones de sincronización, tareas de gestión, gestión de memoria, y gestión de tiempos.



3.6. JITTER.

Cuantifica el efecto del retardo total en la red ocasionado por los paquetes que llegan al receptor. Los paquetes transmitidos a intervalos iguales desde el gateway de la izquierda llegan al gateway de la derecha a intervalos irregulares. El excesivo jitter hace que la voz sea entrecortada y con dificultades para entenderse. El jitter es calculado basado, en las horas de llegada entre paquete y paquete de los paquetes exitosos. Para una alta calidad de voz, el promedio de las horas de llegada entre los paquetes en el receptor debería ser casi igual a la diferencia entre los paquetes en el transmisor y el estándar de desviación debería ser bajo. El jitter buffer (el buffer mantiene paquetes entrantes por una determinada cantidad de tiempo) es usado para neutralizar los efectos de las fluctuaciones de la red y crear un fácil flujo de paquetes en la recepción.



Es tambien, la variación de tiempo entre los paquetes causada por la red. Remover el jitter requiere la recolección de paquetes y retención de estos el tiempo suficiente para que el paquete mas lento llegue a tiempo para ser interpretado en la secuencia correcta.

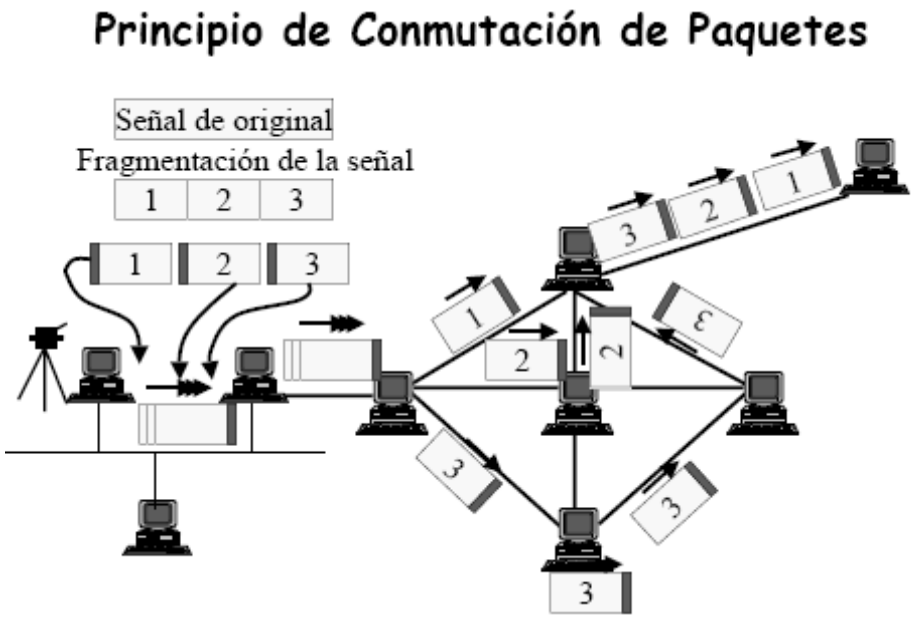
El conflicto que se produce al querer mezclar el retardo con la supresión del jitter, ha generado varios esquemas para adaptar el tamaño del buffer de jitter a los requerimientos de variaciones de tiempo de la red. Esta adaptación tiene la meta explícita de minimizar el tamaño y retardo del buffer de jitter mientras que al mismo tiempo previene el sobre flujo del buffer causado por el jitter.Se han hecho dos aproximaciones para adaptar el tamaño del buffer, la selección de la aproximación depende del tipo de red de paquetes usada.

La primera aproximación es medir la variación del nivel de paquetes en el buffer de jitter en un periodo de tiempo e incrementalmente adaptar el tamaño del buffer para que coincida con el jitter calculado. Esto funciona mejor con redes que tienen jitter constante en un periodo de tiempo, como las redes ATM

La segunda aproximación es contar el número de paquetes que llegan tarde y crear una relación de estos paquetes al numero de paquetes que son procesados exitosamente. Esta relación es usada para ajustar el buffer de jitter a una relación permisible de paquetes tardíos predeterminada. Esto funciona mejor con redes que tengan intervalos de arribo de paquetes altamente variable, como las redes IP.Además de estas técnicas, la red debe estar configurada y gestionada para que tenga retardos y jitter mínimos, permitiendo así un alto QoS.

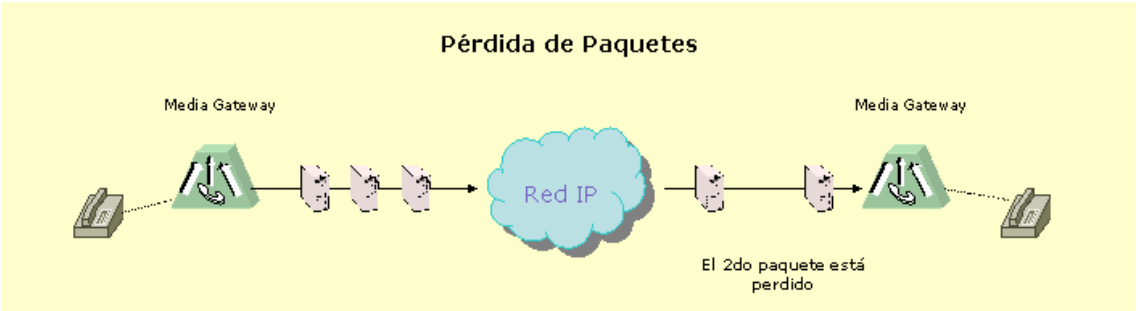
3.7. CONMUTACIÓN DE PAQUETES.

Es un método de comunicación exclusivamente digital, en el que los mensajes que se transmiten se dividen en segmentos y que, junto a la información adicional necesaria para su encaminamiento en la red, se convierten en paquetes. Éstos son transferidos a través de la red mediante procesos de almacenamiento y reenvío sobre circuitos virtuales (circuitos no físicos), que permiten compartir los canales físicos de comunicaciones de la red, pues solamente los ocupan durante el tiempo de transmisión.



3.7.1. PÉRDIDA DE PAQUETES.

Típicamente ocurre en ráfagas o periódicamente debido a una red regularmente congestionada. La pérdida periódica en exceso de 5-10% de todos los paquetes de voz transmitidos pueden degradar la calidad de voz significativamente. La pérdida ocasional de grupos de paquetes puede también hacer difícil la conversación.



3.7.2. COMPENSACIÓN DE PERDIDA DE PAQUETES.

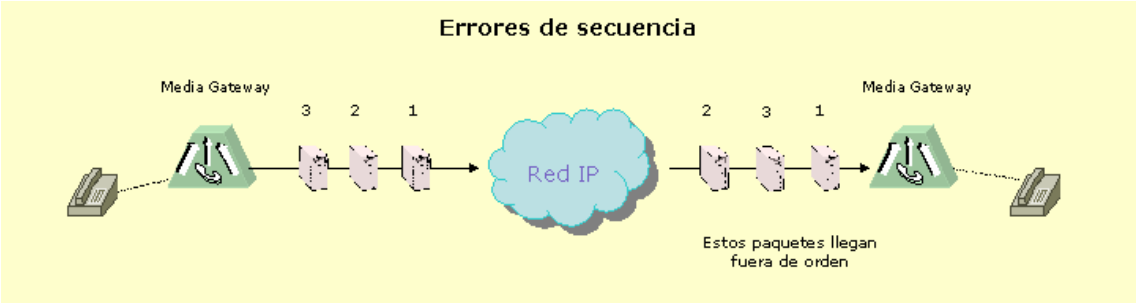
La pérdida de paquetes puede ser un problema aún mayor dependiendo del tipo de red de paquetes que esté siendo usada. Ya que la red IP no garantiza el servicio, usualmente tiene mayor pérdida de paquetes que las redes ATM. En redes IP actuales, todos los marcos de voz son tratados como datos. Bajo congestión, los marcos de voz serán descartados al igual que los de datos, estos últimos sin embargo no son sensibles al tiempo, y los paquetes descartados pueden ser recuperados con la retransmisión, mientras que los paquetes de voz no pueden ser tratados de esta manera.

3.7.3. SOLUCIÒNES PARA CORREGIR LA PÉRDIDA DE PAQUETES DE VOZ

- Interpolar los paquetes de voz perdidos al repetir el último paquete recibido durante el intervalo cuando el paquete perdido supuestamente debía ser analizado, este esquema es un método simple que llena el tiempo entre marcos de voz no continuos, trabaja bien cuando la incidencia de marcos perdido es poco frecuente; si el numero de paquetes pedidos en una fila o ráfaga es alta no trabaja muy bien.
- Enviar información redundante a expensas de la utilización del ancho de banda; esta aproximación hace una réplica y envía el n-ésimo paquete de voz con el (n+1)ésimo paquete; este método tiene la ventaja que poder corregir la pérdida del paquete exacto, sin embargo usa más ancho de banda e incrementa el retardo.
- Usar una aproximación híbirida con ancho de banda menor del codificador de voz para proporcionar información redundante que será llevada en el (n+1)ésimo paquete; esto reduce el problema de necesidad de ancho de banda extra pero falla en la resolución del problema de retardo.

3.7.4. ERRORES DE SECUENCIA.

La congestión en la conmutación de paquetes de la red puede causar paquetes que toman diferentes rutas para alcanzar el mismo destino. Los paquetes pueden llegar fuera de orden resultando una conversación distorsionada.



3.7.5. COMPRESIÓN.

Es usada en cualquier proporción de 1:1 hasta 12:1 en las aplicaciones de VoIP para consumir menos ancho de banda y dejar mas para los datos u otras comunicaciones de voz y fax. La calidad de la voz puede decrecer con el incremento en la proporción de la compresión.

3.7.6. REDES DE CONMUTACIÓN DE CIRCUITOS.

Por conmutación de circuitos se entiende por el control o enrutamiento de señales en un circuito electrónico para transmitir datos o señales entre puntos específicos en una red; el circuito permanece establecido el tiempo que dure la llamada, quedando en este caso a disposición de otros usuarios para su utilización de igual forma. Esta red es considerada la red telefónica tradicional, la cual sirve de apoyo para extender otros servicios a innumerables usuarios, alcanzando hasta los lugares más recónditos.

Conmutación de Circuitos-versus-Paquetes

Características	Conmutación de Circuito	Conmutación de Paquetes
Tiempo de establecimiento	•Aceptable para voz •Muy largo para datos	•No existe fase de establecimiento.
Retardo de transmisión	•Despreciable	•Existe en toda comunicación •Orden de mseg.
Asignación de circuitos	•Único y exclusivo para cada comunicación	•Compartido por otras comunicaciones simultaneas.
Identificación del destino	•Sólo en la fase de establecimiento	•Se incluye un identificador en cada paquete.
Necesidad de almacenar en la red	•No	•Si, en los nodos de la red.
Flexibilidad de la red	•Encaminamiento alternativo	•Gran flexibilidad.

3.7.7. ESTANDARES MAS USADOS EN COMPRESIÓN EN EL DOMINIO IP.

- **Recomendación G.711**

La ITU ha estandarizado la Modulación de Código de Pulso Modulation como G.711, permite una señal de audio de calidad tarificada con un ancho de banda de 3.4 KHz que ha de ser codificado para la transmisión de índices de 56 Kbps o 64 Kbps. El G.711 utiliza A-law o Mu-law para una compresión simple de amplitud y es el requisito básico de la mayoría de los estándares de comunicación multimedia de la ITU.

PCM es un método de codificación de señal de audio analógica más popular y es ampliamente utilizado por la red telefónica pública. Sin embargo, el PCM no soporta compresión de ancho de banda, por lo que otras técnicas de codificación como el ADPCM utilizan estimaciones basándose en dos muestras cuantificadas consecutivas para reducir el ancho de banda.

- **Recomendación G.728.**

G.728 codifica una señal de audio de calidad tarificada con un ancho de banda de 3.4 KHz para transmitir a 16 Kbps. Es utilizada en sistemas de videoconferencia que funcionan a 56 Kbps o 64 Kbps. Con un requisito de ordenador más alto, el G.728 proporciona la cualidad del G.711 a un cuarto del índice de datos necesario.

- **Recomendación G.723.1.**

G.723.1 define cómo puede codificarse una señal de audio con un ancho de banda de 3.4 KHz para transmitirse a 5.3 Kbps y 6.4 Kbps. G.723.1 requiere un índice de transmisión muy bajo ofreciendo una calidad de audio cercana a la tarificada. G.723.1 ha sido seleccionada por el VoIP Forum como el codec básico para aplicaciones de telefonía IP de bajo índice de bits.

El codificador de habla G.723.1 opera con tramas de 30 m de señales de habla en ancho de banda de teléfono digitalizadas y de muestreo a 8 kHz. Las tramas se dividen en cuatro subtramas de 7,5 m de 60 muestras cada una. Cada trama con 240 muestras de entrada se transforma en una palabra de 12 16 bits de datos comprimidos a alta velocidad o palabras de 10 16 bits de datos comprimidos a baja velocidad. Las Detección de Actividad de Voz/Generación de Ruido Confortable (Voice Activity Detection/Comfort Noise Generation o VAD/CNG) especificado en el Anexo A se incorporan por completo al ITU-T G.723.1.

- **Recomendaciones G.729 y G.729A.**

Estas recomendaciones codifican señales de audio cerca de la calidad tarificada con un ancho de banda de 3.4 KHz para su transmisión a una velocidad de 8 Kbps. G.729A requiere una potencia de ordenador más baja que G.729 y G.723.1. Tanto G.729 como G.729A tienen una latencia (el tiempo que necesita para convertir de analógico a digital) más baja que G.723.1. Se espera que G.729A tenga un impacto mayor en la compresión de voz para su transmisión sobre redes inalámbricas.

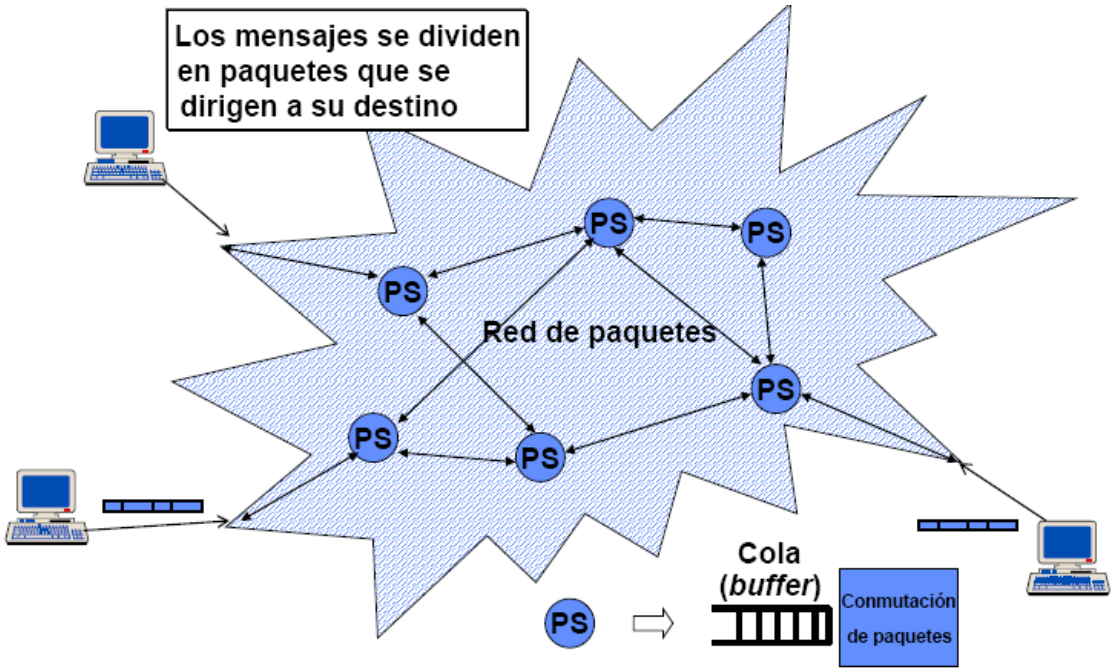
El codificador procesa tramas de muestreo de habla de 10 m a una velocidad de 8 kHz, que junto a una anticipación de 5 m se traduce en un retraso algorítmico total de 15 m. Para cada trama de 80 muestras de datos PCM lineales de 16bits, el codificador obtiene cinco palabras de 16bits. Las aplicaciones que utilizan el vocoder G.729 incluyen telefonía digital, comunicaciones vía satélite y wireless, y Voz sobre Frame Relay (VoFR).

3.7.8. TABLA COMPARATIVA DE CALIDAD.

Clase N°	Retardo por cada sentido	Observaciones
1	De 0 a 150 ms	Aceptable para la mayoría de las conversaciones; sólo algunas funciones altamente interactivas pueden experimentar degradación.
2	De 150 a 300 ms	Aceptable para las llamadas de baja interactividad (satélite con 250 ms por salto).
3	De 300 a 700 ms	Prácticamente una llamada semidúplex.
4	Más de 700 ms	Inútil, a menos que los llamantes estén habituados a conversar en semidúplex (como en el ejército).

Clases de calidad del UIT-T según el retardo de transmisión

3.7.9. PROCESO DE LLENADO DE PAQUETES.



- **Conmutación de paquetes por datagramas.**

– La ruta se elige según una base paquete por paquete.
– Los distintos paquetes pueden seguir rutas diferentes.
– Los paquetes pueden no llegar en orden a su destino.

CAPITULO 4

PROTOCOLOS DE TRANSPORTE EN VoIP

4- PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP).

Es un protocolo que como su nombre lo indica, está orientado a la transmisión de información en tiempo real, como la voz o el video. Este es un protocolo de las capas superiores de usuario que funciona sobre UDP (user datagram protocol) , como mecanismo de transporte porque posee un menor retardo que TCP, y además porque el trafico de voz en la actualidad, sin importar que sean datos o señalización, toleran menos niveles de perdida y no tienen la facilidad de retransmisión, en el UDP se cambia confiabilidad por velocidad, lo cual es básico para manejo de transmisiones en tiempo real como la VoIP. El protocolo RTP tiene como objetivo asegurar una calidad de servicio QoS para servicios del tipo tiempo-real. Incluye: la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (función del protocolo RTCP).El RTP trabaja en capa 4 y sobre UDP, de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertas (port UDP).Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x forma una familia del ITU-T de normas para videoconferencia).

El RTP funciona en conjunto con RSVP (capa 3) para la reservación de ancho de banda y asegurar de esta forma la QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversos alternativas de prioridad para formar una cola de espera en routers. Un algoritmo particular de gestión de prioridad de tráfico es el WFQ (Weighted Fair Queuing) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes. Cada cliente ocupa un intervalo de tiempo en un Round-Robin.

El RTP además provee transporte para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo IGMP para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el encabeza del RTP y ocupa el campo de carga útil.No es lo suficientemente confiable por si solo, este proporciona "ganchos" con protocolos y aplicaciones de capas inferiores y recursos proporcionados por los switches y enrutador para garantizar confiabilidad.

Los paquetes RTP no contienen campo de longitud, ya que al funcionar sobre UDP, este protocolo es quien encapsula la voz comprimida en datagramas. Para la compresión RTP usa una aplicación llamada "vocoder" pudiendo reducir de 64 kbps hasta a 8 kbps la rata para digitalización y compresión de voz produciendo un desmejoramiento en la calidad de la voz poco perceptible, además de esto usa h.323 g.729 y otros protocolos más para transmisiones en tiempo real. RTP es capaz de correr sobre protocolos WAN de alta velocidad como ATM sin ningún problema, también en redes asimétricas como ADSL, cable-modem o por enlace satelital pero cumpliendo con ciertas características de ancho de banda para ambas direcciones y uso exclusivo para la aplicación RTP. Las herramientas de las que se vale RTP para lograr transmisiones en tiempo real son el RTCP, que proporciona un feedback a cerca de la calidad de distribución y la congestión, con esto, la empresa que ofrece el servicio puede monitorear la calidad y puede diagnosticar los problemas que pueda presentar la red.

4.1-CARACTERISTICAS GENERALES DEL PROTOCOLO (RTP).

Fiabilidad	• No es fiable si se utiliza junto con UDP o IP, que a su vez no son fiables. • Puede apoyarse en el servicio prestado por las capas inferiores de las redes que funcionan en modo conectado (por ejemplo capas ATM, AAL3/4 o AAL5).
Control de congestión	• No tiene un mecanismo de control de congestión incorporado, como TCP.
Estabilidad de trenes	• No garantiza el control de los tiempos de transmisión o la continuidad de flujo en tiempo real.
Recursos	• No reserva ningún recurso y no repercute directamente en el compor-tamiento de red.
Información y herramientas para el destinatario	• El encabezamiento RTP contiene varios ítems de información para la sincronización y restitución de la señal en el receptor, a saber: indicación de tiempo, índices de tren y secuencias, fuentes que contribuyen, etc.
Información para el remitente	• No proporciona, por sí mismo, ninguna información útil al remitente. Se utiliza por lo general con el protocolo RTCP, que ofrece al remitente una información muy completa acerca de la calidad de transmisión: pérdidas de paquetes, retardos etc. Permite al remitente modular su velocidad de salida según los recursos disponibles.

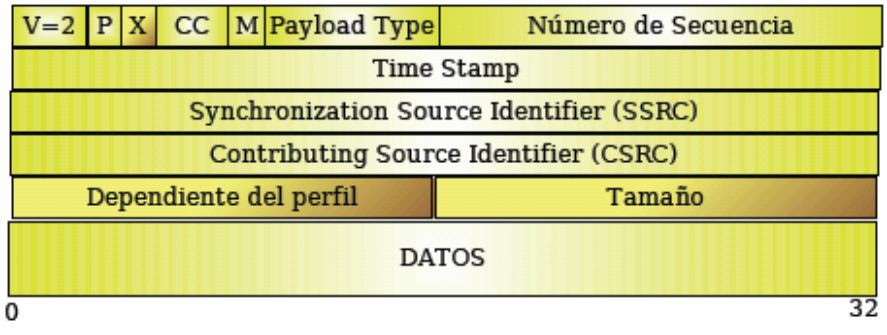
Protocolo de transporte en tiempo real

4.2.- FUNCIONES DEL PROTOCOLO (RTP).

- Entre sus funciones se encuentran: la memorización de datos, la simulación de distribución interactiva, el control y mediciones de aplicaciones.
- La funcionalidad ToS (Tipo de Servicio) en IP puede determinar un ancho de banda específico para el cliente. Un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección

de origen y destino IP, tipo de protocolo y número de socket para asignar una ponderación. En redes que disponen de switch de capa 2 se requiere extender la gestión de la calidad de servicio a dicha capa. Para ello la IEEE ha determinado el ToS sobre IEEE-802.

4.3. DIAGRAMA DEL PAQUETE DE TRANSPORTE RTP.



P = Padding , X = Extenciones tras CSRC(0), CC = CSRC Count(0)

M = Marcador (SID Support), Nª Sec = Comienza en nª aleatorios

Timestamp = Tick count tras la emisiòn del 1er paquete. 1tick =1/8000

SSRC = Origen del medio. Mismo origen, mismo tiempo y nuecero de secuencias.

4.4. PROTOCOLO RTCP (REAL-TIME CONTROL PROTOCOL).

Se basa en la periódica transmisión de los paquetes de control a todos los participantes en sesión, utilizando el mismo mecanismo de distribución como dato paquete. El protocolo subyacente debe proveer de la multiplexación de los datos y de los paquetes del control.

4.5. CARACTERISTICAS GENERALES DEL PROTOCOLO (RTCP).

- Es una herramientas de las que se vale RTP para lograr transmisiones en tiempo real, que proporciona un feedback a cerca de la calidad de distribución y la congestión.
- RTCP sincroniza el audio y el video, conoce el número de usuarios presentes en una conferencia y con esto calcula la rata a la cual deben ser enviados los paquetes.

- Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo de RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (UDP Port) como mecanismo de identificación de protocolos.
- La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio. Se relaciona con el control de congestión y flujo de datos. El RTCP involucra varios tipos de mensajes, por ejemplo:

  -Send report para emisión y recepción de estadísticas (en tiempo random) desde emisores activos. es uno de los más interesantes, disponen de 3 secciones bien diferenciadas:

  1. Los primeros 8 Bytes se refieren a un encabezado común.

  2. La segunda parte de 20 Bytes permite la evaluación de diferentes parámetros (retardo, jitter, eficiencia de datos, etc).

  3. La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado. Incluye los siguientes reportes: cantidad total de paquetes RTP perdidos y a la proporción de los mismos; la cantidad de paquetes recibidos y el jitter entre paquetes; el horario del último paquete recibido y el retardo de transmisión del mismo.

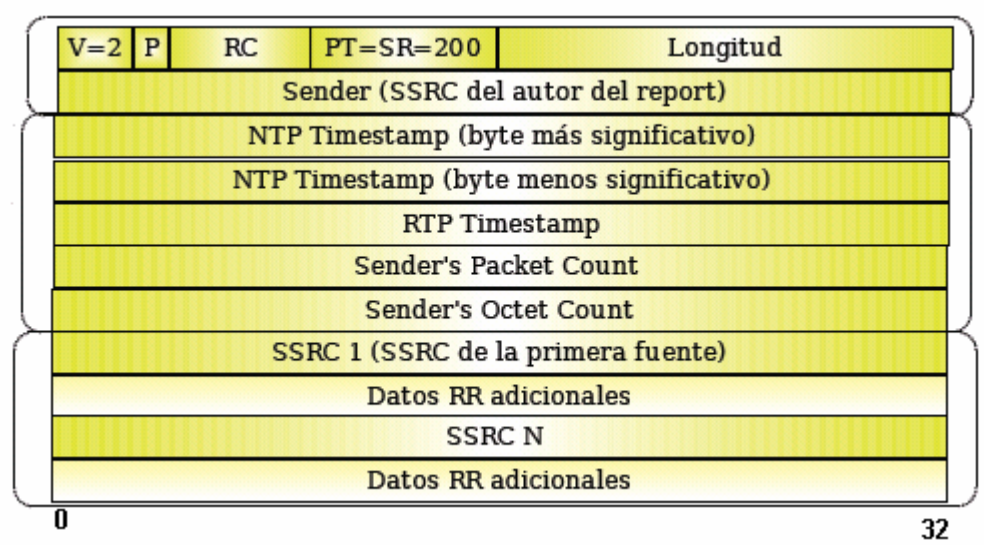
  -Receiver Report para recepción estadísticas desde emisores no activos.

  -Source Description para un identificador de nivel de transporte denominado CNAME (Canonical Name).

  -Bye para indicar el final de la participación en la conexión.

  -Application para aplicaciones específicas.

4.6. DIAGRAMA DEL PAQUETE DE TRANSPORTE RTCP.



SR (Informe de emisor)	Conjunto de estadísticas de transmisión y recepción que proviene de participantes que son emisores activos.
RR (Informe del receptor)	Conjunto de estadísticas que proviene de participantes que sólo son receptores.
SDES (Descripción de fuente)	Los paquetes de descripción de fuente están compuestos de varios elementos, incluido el CNAME. Constituyen la «tarjeta de visita» de la fuente.
BYE (Mensaje de fin)	Indica que se termina una sesión.
APP	Funciones específicas de una determinada aplicación.

Tipos de paquetes RTCP

- PIMER CUERPO:

- RC = Report Count PT: Carga util = 200 para SR.
- Longitud del reporte SSRC: que lo origina.

-SEGUNDO CUERPO:

- NTP timestamp: segundos desde el 1/1/1900. entero y decimal.
- Instante de tiempo en que se envia el reporte (32 +32).
- RTP timestamp: el mismo enstante en ticks de RTP (equivalencia.
- Paquetes y octetos enviados desde el inicio de la sesiòn por (SSRC).

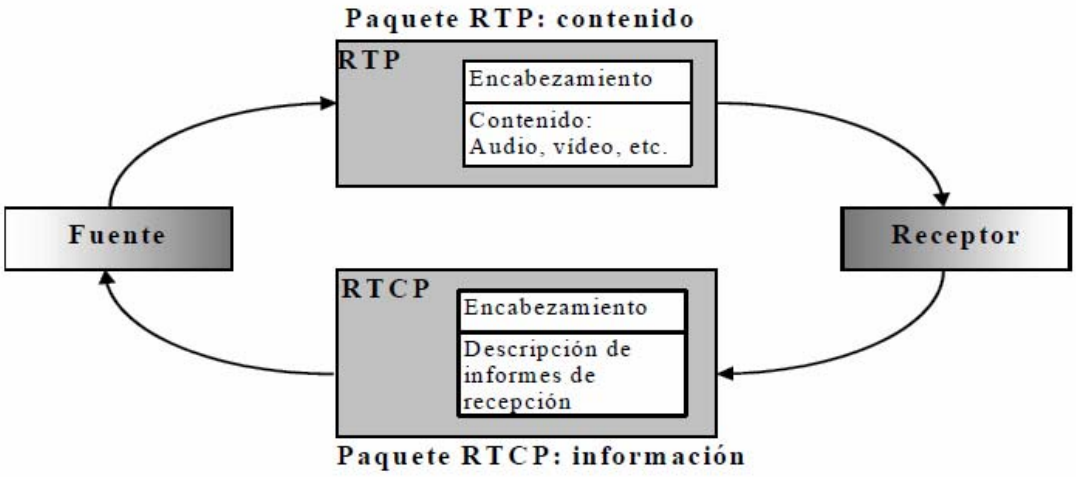
-TERCER CUERPO:

- Conjunto de RR, uno por cada fuente escuchada.

SSCR de la fuente sobre la que se reporta	
Tasa de pérdidas	Nº acumulado de paquetes perdidos
Nº de secuencia mayor recibido	
Variación del retardo entre llegadas: J(i)=J(i-1)+(|Di|-J(i-1))/16	
Último SR y tiempo transcurrido desde entonces	

4.7. DIAGRAMA DE PAQUETE COMPLETO DE TRANSPORTE.

Los destinatarios de los paquetes RTP devuelven información sobre de la calidad de recepción, utilizando diferentes formas de paquetes RTCP, según si ellos mismos son emisores de contenido o no. Los dos tipos, SR y RR, contienen ninguno, uno o varios bloques de informe de receptor, previstos para la sincronización de las fuentes de las cuales el receptor ha recibido un paquete de contenido RTP desde el último informe. La evaluación de la calidad de recepción no es sólo útil para el emisor, sino también para el receptor y cualquier supervisor de red que pudiera existir. El emisor puede modificar su transmisión de acuerdo con la información recibida; el receptor puede inferir si las dificultades de recepción que observa son de origen local, regional o más amplio. El supervisor recibirá solamente los paquetes RTCP, con lo cual podrá evaluar la calidad de funcionamiento de la red.



Paquetes RTP y RTCP para el control de la calidad en recepción

CONCLUSIONES

La investigación sobre VoIP, nos permite ajustarnos de una forma más segura y sencilla al incremento del tráfico que vaya surgiendo como producto de las nuevas migraciones que se hagan hacia la plataforma de VoIP.

La rentabilidad en la utilización de soluciones IP se basa en el desarrollo de nuevos servicios, VoIP significa rapidez en la instalación si se compara con una red similar usando tecnología de circuitos conmutados.

Está claro que el escenario actual seguirá evolucionando hacia la convergencia tecnológica efectiva: la tendencia es ir a un escenario final donde dispondremos de una red de multiservicios que integre todo tipo de contenidos (voz, vídeo y datos) y que nos permita entregarlos de forma personalizada a cualquier tipo de usuario, en cualquier tipo de terminal, con la calidad requerida e independientemente de la ubicación de aquél.

En el estado actual de esta evolución, la tecnología adecuada parece ser la VoIP como soporte del servicio de Telefonía IP (TIP); y como primera propuesta para disponer de un mecanismo de señalización y control para las necesidades que plantea el servicio de TIP, se ha desarrollado la recomendación H.323 de la ITU-T, y todos los protocolos asociados que han surgido del mundo tradicional.

Sin embargo, parece que ante un escenario basado en redes y servicios IP, ha ganado muchos puntos la sencillez, flexibilidad y robustez de SIP; y se perfila como la apuesta clara de futuro (que por otra parte se veía venir como contrapartida desde el mundo de Internet ante las iniciativas del mundo institucional).

Evidentemente, a nadie se escapa que, inmersos como estamos en un esfuerzo de integración y convivencia entre tecnologías, que parten de planteamientos, en principio divergentes, no debemos buscar soluciones excluyentes; de manera que no hay que olvidarse de iniciativas como la de MGCP, o esfuerzos dirigidos a buscar mecanismos de interoperabilidad como el proyecto TIPHON de la ETSI.

Si tenemos que quedarnos con una idea, debe ser la siguiente. Ante la creciente demanda de servicios de multiconferencia multimedia en tiempo real, con funcionalidades de colaboración, parece que son los desarrollos ligados a SIP los que dan una respuesta más satisfactoria a los retos que presenta la implementación de tales servicios. Además en un mundo IP, con la Web como canal de comunicación por defecto, y una oferta cada vez mayor de tecnologías de acceso y soluciones de movilidad, tiene sentido apostar decididamente por SIP.

Se puede concluir diciendo que VoIP es una tecnología que tiene todos los elementos para su rápido desarrollo. Como muestra se puede ver que compañías como Cisco, la han incorporado a su catálogo de productos, los teléfonos IP están ya disponibles y los principales operadores mundiales, así como Telefónica, están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado se tiene ya un estándar que nos garantiza interoperabilidad entre los distintos fabricantes.

Después de haber realizado el estudio de la integración de IP sobre redes ópticas vemos que nos ha proporcionado una descripción de diversos protocolos y soluciones hardware para los paquetes IP de transporte sobre una red WDM/DWDM.

La mejor opción para IP sobre WDM/DWDM en las futuras redes. Se ha visto que se precisan algunos cambios en las configuraciones del hardware para hacer los routers capaces de manejar los paquetes a velocidades de Gigabit, así como el uso de switch fabricados en vez de buses. También se ve que el uso de MPLS es el relevo a la carga de las largas tablas de búsqueda en los routers, y además realiza las funcionalidades de la red.

El trabajo ha mostrado algunas de las posibilidades de las cuales WDM puede dar en términos de funcionalidad. La posibilidad de conexión cruzada y enrutar los flujos IP con la ayuda de las longitudes de onda y de tal modo de conseguir una menor laténcia en la red. Por otra parte se ve las diversas formas de realizar la protección de la conmutación de la longitud de onda y cómo esto se compara en términos de velocidad con la redundancia en los interfaces de los routers.

Las tendencias que prevalecen en IP sobre WDM son interfaces de routers más rápidos, incremento del número de las longitudes de onda, el movimiento del enrutamiento a las capas más bajas, los nuevos protocolos adaptados a IP sobre WDM y protocolos menores de conversión entre las particiones de la red. En el resumen, estas tendencias representan la conducción de las fuerzas detrás del movimiento de hacer las redes más simples y más rentables usando IP sobre WDM.

Considerando los costes de gestión de hoy en día, las soluciones de gestión integrada para entregar servicios extremos a extremo eficientemente en un ambiente de múltiples capas heterogéneos de la red constituyen un factor dominante para la introducción de las nuevas arquitecturas de red, tecnologías, y servicios.

BIBLIOGRAFÍA

CANTV, VoIP. Informe 2001

CANTV, Plan inicial de Evaluación de VoIP. 2001

http://www.cesga.es/ga/default.html?Recetga/Proxrecet.html&2

http://www.monografias.com/trabajos3/voip/voip.shtml

http://www.hi-teck.com/ip_telephony/benef_home.jsp

http://www.comtest.com/tutorials/VoIP.html

http://intranet.upb.edu/laboISTEC/Articulos/Articulo%20VoIP%20_eng.pdf

http://www.pt.com/tutorials/iptelephony/tutorial_voip_signaling.html

http://www.networkcomputing.com/netdesign/1109voip.html

http://www.protocols.com/voip/architecture.htm

http://www.comunicaciones.unitronics.es/tecnologia/H.323.html#Gatekeeper

http://www.comunicaciones.unitronics.es/tecnologia/voip.htm

http://www.aui.es/biblio/libros/mi99/19voz_ip.htm

http://www.avaya.es/Informacion_de_la_empresa/Sala_de_Prensa/Notas_de_Prensa/prensa30.asp

http://www.recursosvoip.com/protocolos/megaco.php

http://www.commworks.com/Spanish/Softswitch/Softswitch_Components/Session_Agents/H.323_SIP/

http://neutron.ing.ucv.ve/revista/e/No7/Russomanno%5Cvoz%20sobre%20IP.html

http://www.protocols.com/pbook/VoIP.htm#MGCP

http://www.monografias.com/trabajos11/descripip/descripip.shtml

http://www.protocols.com/voip/testing.htm

http://www.aui.es/biblio/libros/mi99/19voz_ip.htm

http://www.gbm.net/bluetech/Edicion14.4/telefoniaip

http://eia.udg.es/~atm/tcp-ip/tema_4_6_1.htm