ANALISIS DE LA IMPLEMENTACION DE IUB FULL IP EN LA RED 3G SOBRE TECNOLOGIA MPLS

María Victoria Farías – Diego Lucas Fernández

A mis padres, en el cielo y en la tierra, por inculcarme y motivarme a la búsqueda del camino propio. Gracias por su apoyo continuo e incondicional.

Diego.-

Dedico este proyecto a las personas que me apoyaron desde un principio para poder continuar mis estudios, ya que sin ellos no podría haberlo logrado, mi padre y madre, quienes me han motivado constantemente. A mi hija que ha sido mi pilar y el impulso para llegar hasta aquí.

María Victoria.-

INDICE

INDICE DE GRAFICOS

INTRODUCCION

La popularización del uso de Internet móvil en los últimos años ha impuesto un ritmo acelerado en el crecimiento y constante actualización de las redes móviles. No sólo ha continuado aumentando el volumen de tráfico en la red sino que ya se requiere mayor calidad de servicio para las aplicaciones multimedia. Por lo que se ha hecho necesario disponer de enrutadores (routers) de gran capacidad para poder procesar y encaminar grandes cantidades de paquetes por segundo. Durante esta evolución para acelerar las funciones de encaminamiento de los routers surgió el concepto de conmutación de nivel 3 (modelo OSI). En la carrera para disponer de routers de alta velocidad aparecieron varias propuestas para acelerar el transporte de paquetes IP a través de la red. Esto tuvo como consecuencia una sobrecarga de procesamiento, mal uso de recursos, problemas de incompatibilidad con tecnologías de capa de enlace, necesidad de ingeniería de tráfico, redefinición de algoritmos de enrutamiento, entre otros, lo cual es percibido por el cliente como un rendimiento pobre de la red.

Otros problemas que se presentaron fueron:

- Falta de compatibilidad y adaptación con los diferentes protocolos de capa de enlace ya que estos últimos no fueron concebidos bajo el esquema de IP.
- El crecimiento desmesurado de usuarios. Las direcciones IP que nos facilita la comunicación a través de Internet se agotan rápidamente.
- Ingeniería de Tráfico, concepto el cual los protocolos de enrutamiento de la Internet no implementan; por lo que contribuyen a agravar el problema de congestión.
- Necesidad de Calidad de Servicio (QoS) por parte de las distintas aplicaciones que fueron surgiendo en los últimos años.

Muchas soluciones alternativas a estos inconvenientes fueron relacionadas con el uso de conmutadores ATM; por ello la integración de IP con las redes ATM fue de capital importancia.

Como una solución a estos problemas se creó el protocolo IPv6, evolución del protocolo IPv4, un protocolo perfectamente capaz de proporcionar mayores facilidades y/o

funcionalidades requeridas por las aplicaciones. Además, proveyó de nuevas herramientas, lo que proporcionó simplicidad al modelo de red, mayor número de direcciones IP, compatibilidad con nuevos protocolos que podían mejorarlo, arquitecturas que permitían Calidad de Servicio (QoS), cabecera fija, entre otros; a todas estas nuevas funcionalidades se sumó el hecho de que proporcionaba simplicidad, dado que las herramientas anteriormente mencionadas no implicaron que el modelo se volviera más complejo.

A pesar de lo antes citado, muchas entidades no han adoptado todavía el nuevo protocolo de Internet IPv6 y algunas otras están en un proceso lento de adopción de este protocolo a pesar que entró en vigencia hace más de una década (IPv6 fue propuesto en 1998 como solución al problema de la escasez de direcciones del protocolo IPv4). El principal motivo por el cual las empresas proveedoras de Internet aún no han adoptado IPv6 es que poseen equipos e infraestructura diseñada para soportar IPv4, por lo cual son pocos los equipos capaces de soportar el cambio a IPv6, ya que la gran mayoría no fueron concebidos para este nuevo protocolo. Sólo los equipos más recientes están disponibles para este cambio de protocolo.

La propuesta de “Multiprotocol Label Switching” (MPLS) fue el resultado de este proceso de convergencia y de integración entre ATM e IP. MPLS pretende resolver problemas presentados en las redes actuales, tales como: velocidad y retardo, escalabilidad, manejo de la calidad de servicio QoS, e ingeniería de tráfico.

Gracias a MPLS se pudo afrontar los siguientes problemas:

- La migración de IPv4 a IPv6 de manera progresiva sin los problemas citados.
- Los proveedores pueden adoptar este protocolo de manera más sencilla.
- Alta compatibilidad con tecnologías de capa 2 como ATM y Frame Relay.
- Ingeniería de tráfico y QoS.
- Capacidad de proporcionar un envío rápido de la información.
- Capacidad de definir VPN (Virtual Private Network).
- Compatibilidad con los protocolos de capa de enlace

Para justificar estos argumentos de la problemática que generó el crecimiento abrupto en las redes de telecomunicaciones, comenzaremos con un repaso de los protocolos de internet y su evolución desde mediados de los años 90, como así también del Modo de Transferencia Asincrónica (ATM – Asyncronic Transference Mode).

Con esta base estamos en condiciones de introducir y desarrollar MPLS: origen y objetivos, descripción, terminología, estructura, arquitectura y conmutación.

Luego, en la próxima etapa del desarrollo de esta tesis indagaremos sobre el aspecto funcional de la tecnología MPLS y discutiremos la actuación conjunta de sus componentes y con los elementos de red móvil UMTS, en función de la Ingeniería de tráfico, clases de servicio y calidad de servicio (QoS) y VPN (red privada virtual).

OBJETIVO

Nuestro proyecto tiene como objetivo analizar la implementación de una red de transporte IP RAN, para servicios 3G de una operadora existente en nuestro país, tomando como muestra un tramo de su red y analizar las mejoras en la capacidad de la WBTS y sus costos asociados.

CAPITULO 1: LA RED UMTS

Una red UMTS pude ser visualizada desde varios ángulos, ya sea desde el punto de vista del usuario, desde el plano de gestión de red, o desde la función de cada uno de sus subsistemas. Justamente de este último punto se puede describir la red UMTS haciendo foco en cada uno de los diferentes elementos que la componen.

La red UMTS puede ser dividida en 4 subsistemas:

- Equipamiento del usuario
- Red de Acceso de Radio (RAN)
- Red Core, incluidos los elementos de red para los distintos grupos de servicios (CN)
- Subsistema de gestión de red

A su vez, en cada subsistema se puede encontrar diferentes tecnologías. Así como la RAN puede clasificarse según la técnica de acceso que predomine en la interface de aire, el CN actualmente puede describirse según su dominio en conmutación de circuitos (CS) y su dominio de conmutación de paquetes (PS)

Figura 1.1.- Red de Acceso de Radio y Red Core

1.1 Subsistema Equipamiento de Usuario (UE)

El equipamiento del usuario tiene a su vez una sub-estructura. La tarjeta universal que contiene el circuito integrado (UICC) similar a la SIM en GSM. Esta se ubica en el equipo móvil (ME) el cual es independiente del cliente.

Tradicionalmente el UE o equipamiento de usuario era una única pieza, la red UMTS nos brinda la posibilidad de que un UE contenga interconectadas varios ME compartiendo la misma UICC, como por ejemplo, una red de laptops.

La transmisión de radio, el control del recurso de radio, el soporte de QoS de datos son funciones que corresponden al Terminal Móvil (MT) el cual puede o no estar integrado del teléfono móvil o formar parte de la misma UICC, permitiendo a una laptop, Tablet, PC con USB 3G o Smartphone adoptar las funciones de UMTS.

La UICC contiene información del cliente para varias tecnologías: para aplicaciones de GSM (igual que la tarjeta SIM), para aplicaciones UMTS e información de identidad necesaria para el servicio multimedia IP. Una característica importante de la UICC es la inaccesibilidad por parte del cliente a los datos contenidos en la tarjeta, pudiendo ser manipuladas únicamente por el operador que vende la UICC.

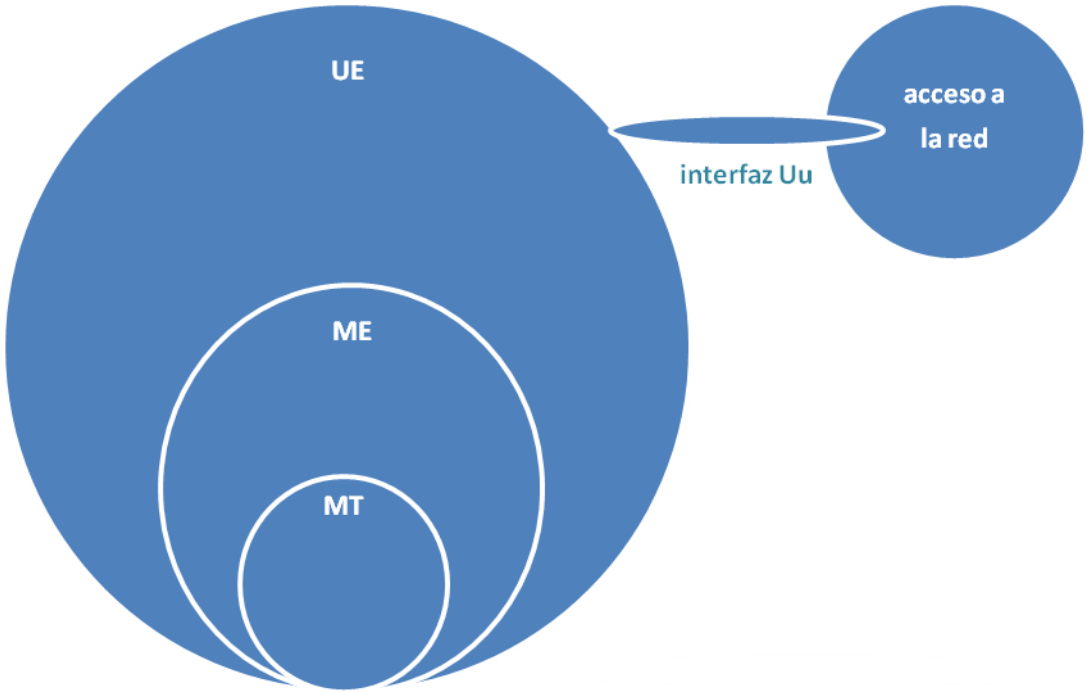


Figura 1.2 - equipamiento de usuario

1.2 RAN – Red de Radio Acceso

La RAN se compone de dos grandes sub-redes, la GERAN y la UTRAN (GSM Edge Radio Access Network y UTMS Terretrial Radio Access Network respectivamente). Empezaremos desarrollando la UTRAN ya que pertenece a la red 3G y luego describiremos como interviene la tecnología 2G a través de su red de acceso, o GERAN

1.2.1 UTRAN

La UTRAN se encuentra compuesta por los RNC (Radio Network Controller) y los Nodos B o Estación Base, los cuales se interconectan entre sí a través de la interfaz Iub. La interfaz de aire Uu permite a los UE poder ingresar a los servicios de red. Este conjunto recibe el nombre de RNS (Radio Network Sub-system). Tal como se muestra gráficamente en la figura 1.3.

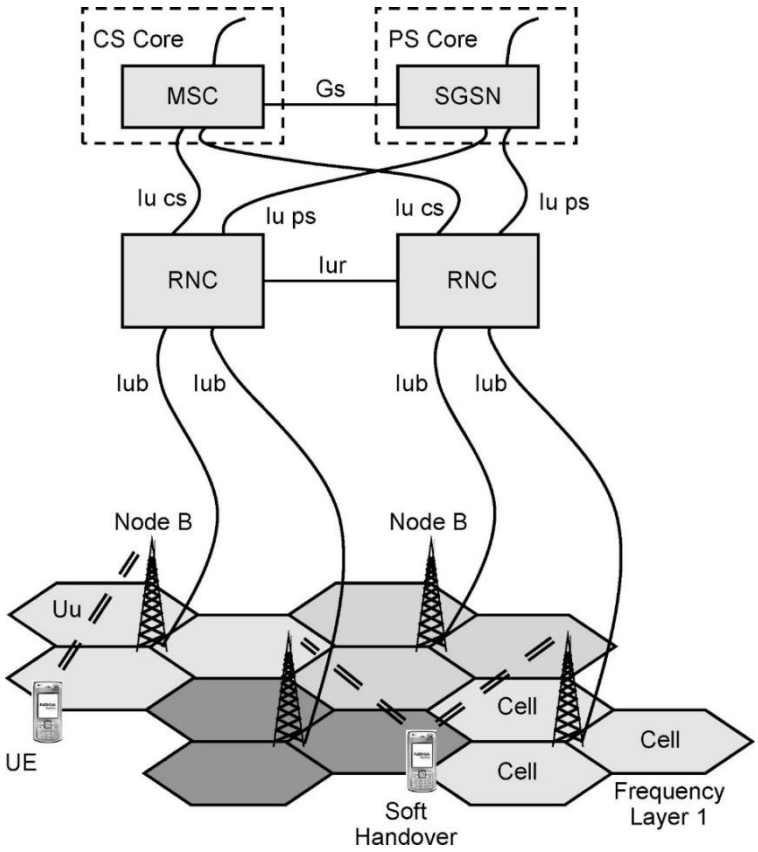


Figura 1.3.- Interfaces de la red de acceso

1.2.1.1 Interfaz de aire Uu.

Esta interfaz es la localizada entre el equipo terminal y un nodo B. Por lo tanto el medio de transmisión se encuentra basado en señales electromagnéticas a través del aire, utilizando técnica de acceso múltiple a fin de poder compartir el espacio radioeléctrico.

CDMA es una técnica de Acceso Múltiple por División de Códigos. Su origen proviene del entorno militar y se desarrolló a modo de optimizar otras dos técnicas de acceso que se basaban en la división de frecuencias (FDMA) y en la división de tiempos (TDMA). CDMA básicamente permite que se use todo el ancho de banda disponible, todo el tiempo requerido para cada canal, diferenciando estos últimos por diferencia de códigos.

Se dio a conocer a WCDMA como solución de “espectro ensanchado” (la W de la sigla significa width – ancho). Este espectro fue generado a partir de la señal de banda base y una señal moduladora de un ancho de banda superior al de la banda base, utilizando un código de expansión que permite separar entre diferentes comunicaciones que comparten una misma portadora.

En este caso el ensanchamiento se consiguió multiplicando la señal digital en banda base por una secuencia conocida por los extremos en comunicación. Esta secuencia posee una velocidad mucho mayor a la de banda base.

En WCDMA la información comparte todo el espectro de frecuencia con el resto de los canales (se pueden digitalizan entre 8 y 10 llamadas como máximo), diferenciándose a través de un código único. Esta tecnología se creó para el tratamiento de datos.

Algunas de las ventajas que ofreció este tipo de codificación son:

- Mayor calidad en las comunicaciones de voz al utilizar vocoders, a la vez que se logró maximizar la capacidad del sistema.
- Debido a la dispersión del espectro en WCDMA, fue necesario un menor número de celdas para ofrecer cobertura, lo que llevó a un menor costo de equipamiento.
- El uso de códigos, no solo proporcionó seguridad, sino que además permitió diferenciar los canales, eliminando interferencias de co-canal
- En el caso de superar la demanda de servicio, WCDMA puede modificar su capacidad temporariamente, recuperando luego sus características.

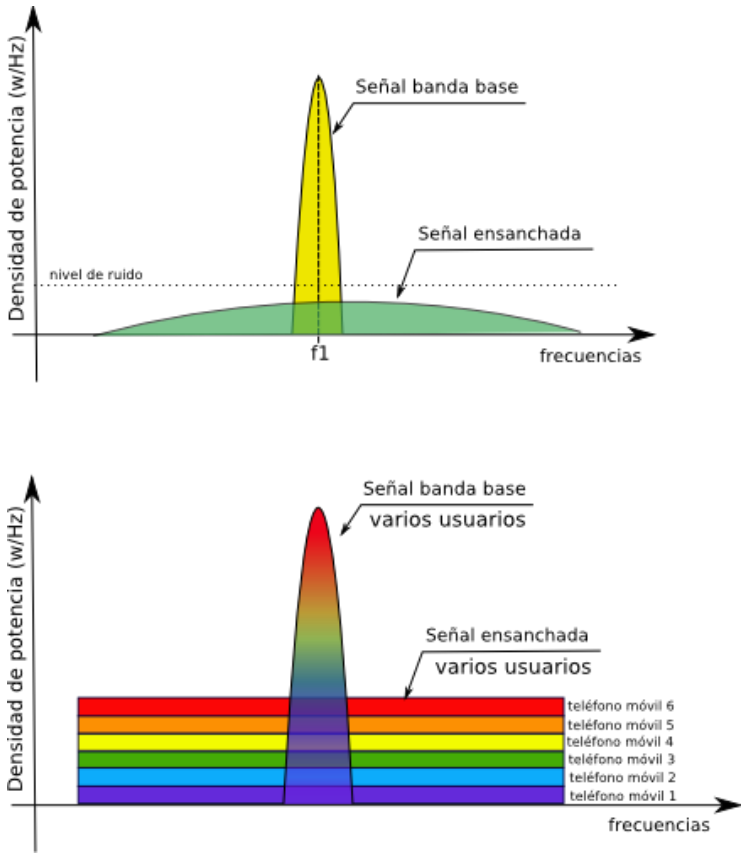


Figura 1.4.- Espectro ensanchado

1.2.1.1.1 Estructura Lógica de UMTS

La frecuencia que se destinó en Argentina para el servicio UMTS va de los 824 -890 MHz (conocida como la banda de 850) y 1910-1990 MHz (conocida como la banda de 1900) ambas bandas utilizan la Duplexación por División de Frecuencia (FDD, W-CDMA) tanto para subida como bajada con canales de 5 MHz separados 200 kHz. La banda de 1900 también utiliza la técnica de Duplexación por División de Tiempo (TDD, TD/CDMA), con separación de canales de 5 MHz, solo que la Tx y Rx no se encuentran separadas en frecuencia sino que los canales están separados por un intervalo de tiempo.

UMTS abarcó 2 sistemas, llamados modo FDD y TDD, conformadas según el modelo OSI.

- Modo **FDD** (Frecuency Division Duplex): Cada trasmisión fue identificada por la portadora y código Pseudoaliatorio WCDMA, es decir, por la portadora en la que tiene lugar y su secuencia multiplicadora. Al utilizar una portadora diferente por enlace ascendente y descendente dentro de una banda apareada, les permitió poder

procesar varios usuarios simultáneamente. Este método fue comúnmente utilizado para cobertura tipo macroceldas de usuarios con gran movilidad.

- Modo **TDD** (Time Division Duplex): Cada trasmisión se identificó con la frecuencia de la portadora y uno de los 15 intervalos de tiempo de la trama TDMA (timeslot). Se empleó una única portadora, tanto para el canal ascendente como descendente, permitiendo a los intervalos de tiempo ser repartidos en forma dinámica. Este modo fue una solución ideal para el tráfico asimétrico, como lo es el de internet.

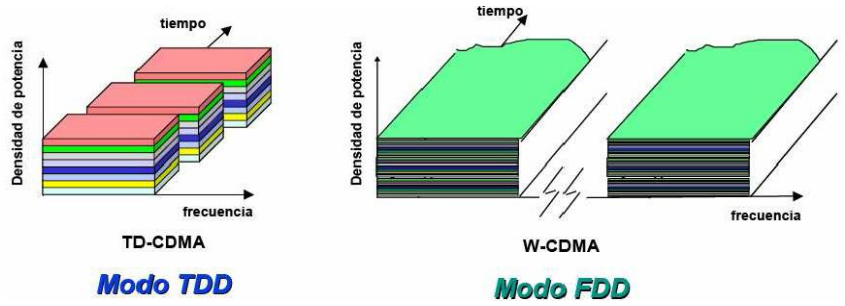


Figura 1.5.- Métodos de acceso

Volviendo a la comparación con OSI, son 3 las etapas intervinientes, la capa 1 o Física, la capa 2 o Enlace y por último la capa 3 o de Red. Además podemos identificar 2 grandes planos, el de control referido a todo lo que tiene que ver con la señalización del sistema y el plano de usuario, referido al tráfico de información.

La capa 1 es la encargada de trasmitir la información a través de algún medio, en este caso es el aire a través de ondas radioeléctricas.

La capa 2 se encarga de ofrecer una trasmisión libre de errores hacia la capa superior. Esta capa a su vez está subdividida en capas diferentes. La primera subcapa es la de control de acceso al medio (MAC), en ella se puede encontrar los protocolos de gestión de acceso a los recursos. Por encima de esta se situó la subcapa control de enlace de radio (RLC) que ofrece un servicio de trasmisión de datos a la capa de red. Estas 2 subcapas pertenecen al plano de control. Mientras que en el plano usuario se observaron 2 subcapas, la subcapa de protocolo de control de Broadcast/Multicast (BMC) encargada de trasmitir información de difusión o multidifusión sobre la interfaz de radio y la subcapa protocolo de convergencia de paquetes de datos (PDCP), quien cumple la misma función que BMC solo

que exclusivamente para los paquetes de datos. Además se encarga de comprimir los paquetes de las capas superiores para mejorar la eficiencia espectral.

Finalmente la capa 3 se encarga de que los paquetes lleguen a destino. También se dividió en 3 subcapas, las cuales son, Gestión de los recursos de radio (RRM); Control de llamadas (CC) y Gestión de la movilidad (MM). Por encima de la subcapa RRM se encuentra una subcapa de Prevención de Duplicaciones que linda con el Core Network y la RAN.

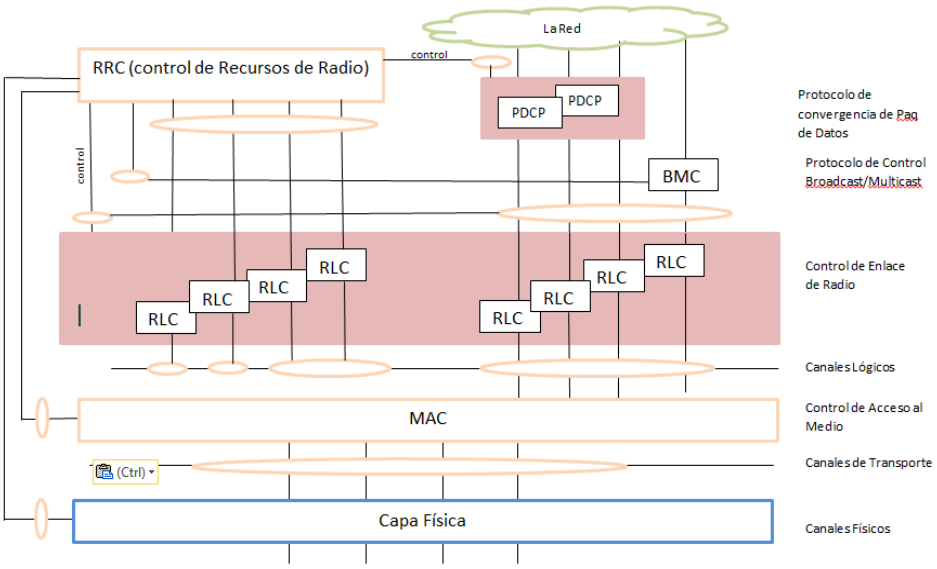


Figura 1.6.- Sistema UMTS según el modelo OSI

1.2.1.2 Nodo B

Un Nodo B puede dar servicio a una o más células a fin de conectar a los dispositivos de los usuarios, a través de la interfaz de aire Uu, con la red. Posee otras funciones como la realización de mapeos de la información, tanto de aquella que provienen de los terminales de usuarios en términos del ancho de banda y Qos (calidad de servicio), como aquella que definen los recursos de la interfaz Iub.

1.2.1.3 Interfaz Iub

A diferencia de la interfaz Uu que trata de una conexión directa a través de ondas radioeléctricas, la interfaz Iub es mucho más compleja ya nunca un nodo B se conecta directamente a una RNC.

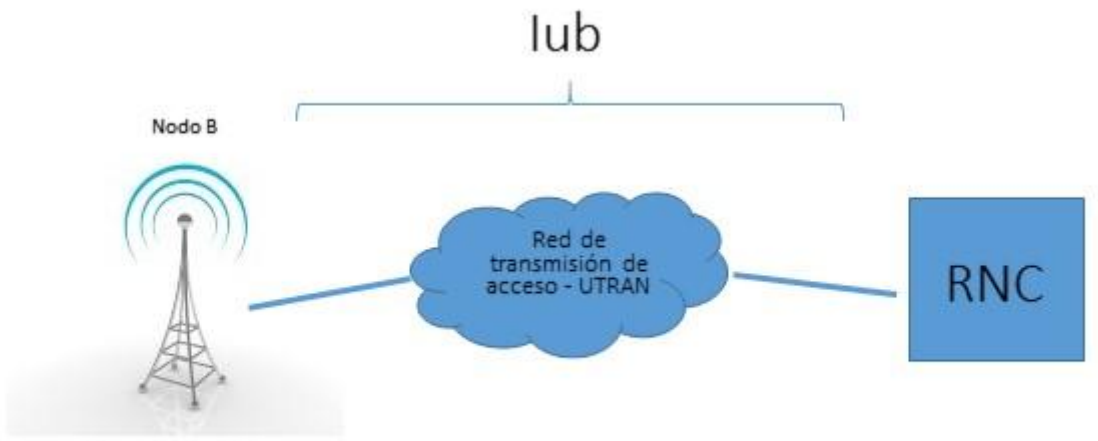


Figura 1.7.- Red de acceso UTRAN

Es muy común que una sola RNC controle cientos de nodos B. Las RNCs suelen estar ubicadas en los centros de conmutación de las operadoras, mientras los Nodos B se encuentran repartidos en todo el territorio al que se le quiere dar servicio UMTS. Esta aclaración es validad para demostrar que en muchos casos existen grandes distancias entre un componente y otro, lo que requirió el despliegue de una red de transporte/transmisión de área extensa (WAN) que uniera a cada nodo B con su respectiva RNC. A esta red se la llamó Red de Trasmisión de Acceso o UTRAN.

Una de las características de la Iub, es que utiliza como tecnología de trasporte ATM o IP. Respecto a esto el grupo 3GPP publicó en la Release 99 (año 2000) la primera red UMTS juntos con todas sus características, y en una posterior especificación (UMTS Core Network based on ATM Transport – Spen 23925) se definió como núcleo de red a la tecnología ATM como así también la tecnología de transporte.

Sin embargo, a partir de la Release 5, se permitió utilizar tanto ATM como IP para transportar los datos de usuarios y la señalización del Nodo B proveniente de la RNC a través de la interfaz Iub. Dicha interfaz permite transportar 2 tipos de información, la información Móvil-Red correspondiente a la señalización o tráfico de usuario, la cual intercambian los móviles y nodos de ingreso al CORE (pueden ser MSC para el caso CS o SGSN para el caso PS); la señalización UTRAN que abarca la información entre NBs - RNCs, y entre RNCs - CORE Network y entre las mismas RNCs

Además, a partir de la Release 4 se separaron las funciones de transporte y control en dos planos diferenciados e independientes: plano de control y plano de usuario.

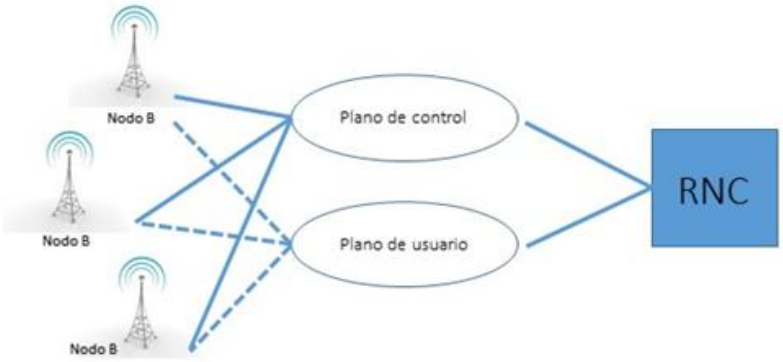


Figura 1.8.- Plano de Control y Plano de Usuario

En la figura 1.9 y 1.10 podemos observar ambos planos con su respectiva pila de protocolos usando ATM e IP.

El protocolo AAL2 permitió multiplexar varios flujos de datos sobre un circuito ATM. Estos flujos de datos se convierten en flujo de paquetes CPS a los cuales se los denominó miniceldas AAL2 que se encuentran comprendidos por una cabecera de 3 octetos y una carga que va desde 1 a 45 octetos. Estos flujos de miniceldas son multiplexados formando bloques de 47 octetos. A esto se le añade un octeto de puntero destinado a facilitar el recupero ante pérdidas en la recepción, formando asi un bloque de 48 octetos con lo que se rellena la carga útil de una celula ATM.

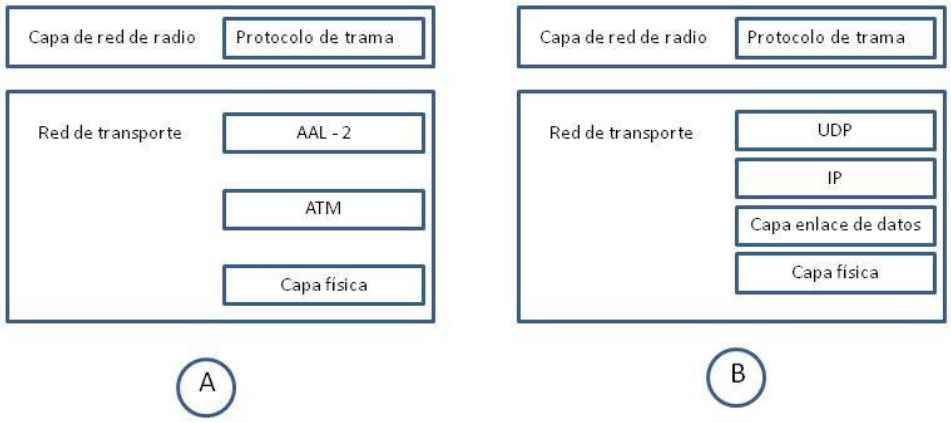


Figura 1.9.- Pila de protocolos del plano de usuario a) ATM b) IP

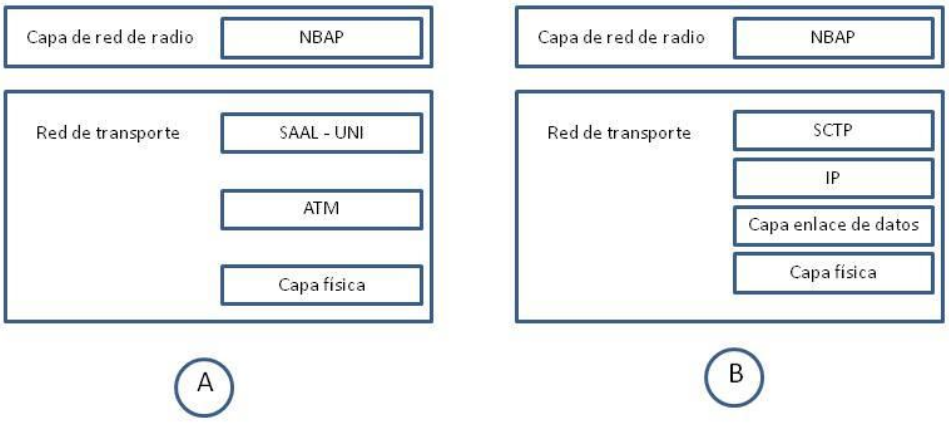


Figura 1.10.- Pila de protocolos del plano de control a) ATM b) IP

En el caso de Iu-PS, se adoptó como solución un tunel IP por sesión de datos, conocido como el protocolo AAL5.

NBAP son las siglas de Node B Application Part. Este es el protocolo de señalización utilizado por la RNC para controlar al Nodo B.

1.2.1.4 Diferentes tipos de Iub

En los orígenes de las redes UMTS la información transportada entre los nodos B y la RNC debió ser realizada a través de la red de acceso TDM existente para GSM mediante el empaquetado de cierta cantidad de E1 sobre la tecnología ATM. Sin embargo, a partir de la Release 5 del 3GPP permitió el transporte IP además de ATM, debido a que se ha ido extendiendo la tecnología Ethernet por la red de acceso. Esto permitió tres configuraciones posibles de interfaces Iub:

A) Iub ATM/TDM: IMA

Esta era la configuración habitual hasta la llegada de IP y Ethernet a la red de acceso.

Los Nodos B disponían de puertos E1 que eran agrupados o empaquetados a través de un protocolo llamado IMA (Inverse Multiplexing for ATM o multiplexación inversa de ATM) de manera que se creaba de extremo a extremo un enlace lógico o virtual de mayor

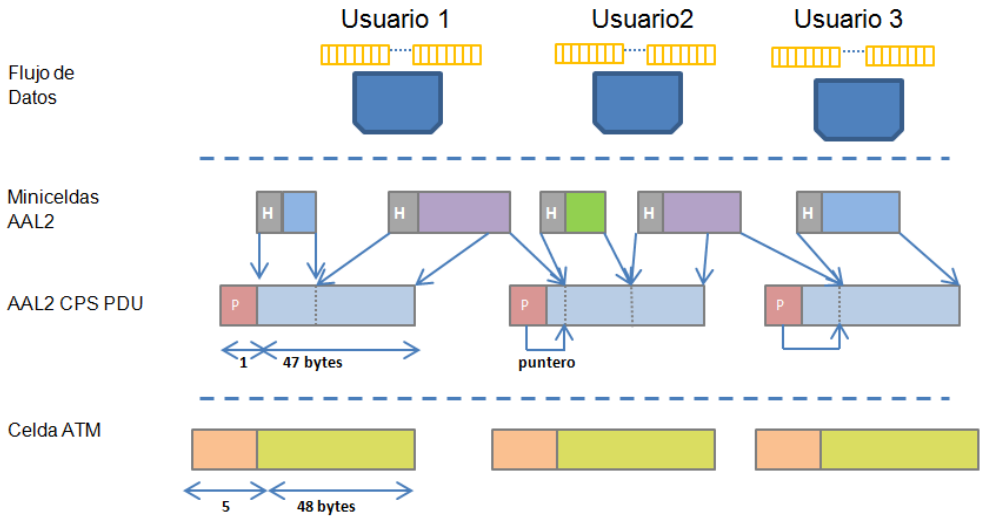


Figura 1.11.- Flujo de datos para celdas ATM

ancho de banda, llevándola a una capacidad equivalente aproximada a la suma de E1s utilizadas. El flujo de tramas E1 era distribuido entre los múltiples E1s y se re ensamblaba en el destino para crear el flujo original, tal como lo muestra gráficamente la figura 1.12.

Periódicamente se transmitían celdas especiales llamadas ICP (IMA Control Protocol) que se descartaban en el extremo destino. IMA es un protocolo mediante el cual se podría crear circuitos emulados ATM para transmitir datos a mayor ancho de banda del que ofrecían los enlaces por separados.

Según la especificación, un grupo IMA no podía estar constituido por más de 32 E1s, otorgando una capacidad máxima al vínculo de 64 Mbps. Comúnmente los nodos B tiene una máxima configuración de hasta 8 E1s.

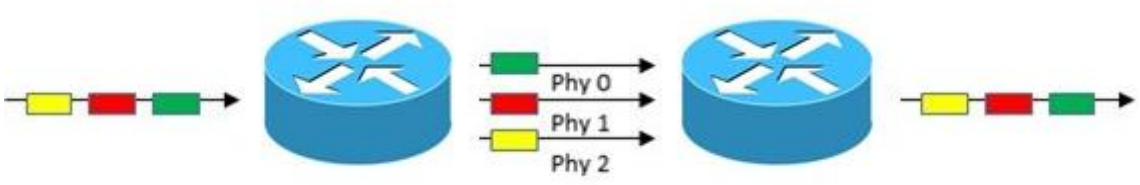


Figura 1.12.- Esquema IMA

Estos enlaces ofrecían la posibilidad de dar calidad de servicio (QoS) aunque a expensas de un alto porcentaje de ancho de banda utilizado para datos de cabecera. Recordemos que la celdas ATM tienen una longitud de 53 bytes, de los cuales 5 bytes son de cabecera, es decir, casi un 10% de desaprovechamiento.

B) Iub FULL IP

Esta configuración ha determinado que existe una ruta completa Ethernet entre un nodo B y la RNC. Por lo tanto, dejó de estar limitada a 16Mbps (8 E1s) bajo la tecnología ATM, pudiendo ahora llegar a los 100Mbps. Esta es la evolución que se está llevando a cabo en la actualidad, y se pretende alcanzar a todos los nodos B, continuando la evolución a Full-IP.

Una ruta lógica FULL IP puede llegar a consistir en atravesar varios enlaces de tecnologías diferentes Ethernet hasta llegar al equipo MPLS más próximo. En este punto entraría a la red MPLS donde los paquetes son encaminados mediantes protocolos MPLS-IP (ver capitulo MPLS) hasta alcanzar el equipo MPLS que se encuentra conectado directamente a la RNC. Dicho equipo se encarga de desencapsular los paquetes y entregarlos a la RNC a través de una interfaz Gigabit Ethernet.

C) Iub Dual-Stack

Esta configuración le permitió a un nodo B establecer dos caminos Iub diferentes: una ATM y el otro IP, actuando simultáneamente. Figura 1.13

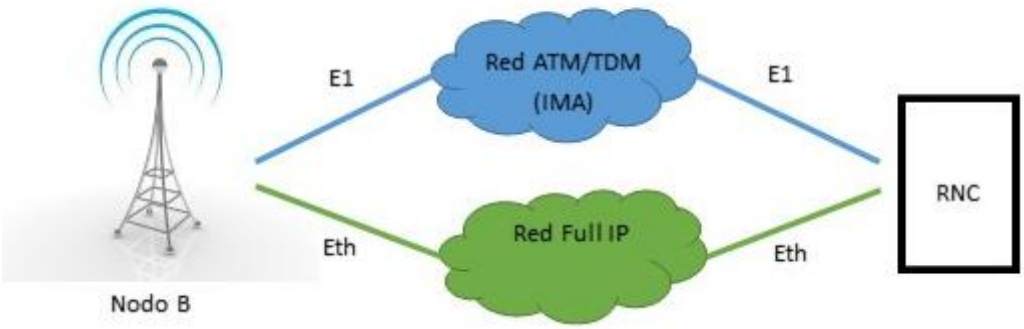


Figura 1.13.-Nodo B con Interfaz Dual-Stack

De esta manera se obtuvo ventajas al poder disponer distintas caminos:

- Permitió usar un camino como principal y el otro como secundario; como protección frente a cortes del primero.

- Utilizar un camino (IP o ATM) de mayor ancho de banda para el enlace downlink y de menor ancho de banda para enlaces uplink.
- Enviar por ATM la voz y datos según la norma Release 99, como así también la señalización, es decir, información con una mayor sensibilidad al retardo y pérdida; trasmitiendo los datos de menor sensibilidad por el camino IP sobre la red de conmutación de paquetes.

Desde el punto de vista de las operadoras, esto fue beneficioso pues permitió un mayor ahorrar en la red de transporte, a la vez que garantizó QoS al tráfico sensible y proporcionar ráfagas de velocidad pico.

1.2.1.5 RNC – Radio Network Controller

La RNC es la Unidad Central de Control de una RNS. Se encuentra conectada a través de distintas interfaces basadas en tecnología ATM. Como se desarrolló en el punto anterior, la **interfaz Iub** conecta con los Nodo B mientras que la **Interfaz Iur** conecta hacia otras RNC. Por último utilizó la **interfaz Iu** para conectar con el Core Network (CN), que puede ser dividida en Iu-PS y Iu-CN.

Algunas de las funciones que cumple la RNC son:

1) Mantenimiento de conexión móvil-red troncal: La red de acceso se encarga de transportar los datos de usuario y señalización entre el móvil y la red troncal. Un aspecto importante es la gestión de los recursos de la red de radio para brindar garantía de calidad de servicio extremo a extremo requerida por los usuarios.

   Para esto, la red se encarga de traducir los parámetros de calidad de servicios del usuario (por ejemplo tasa de bit, retardo), a parámetros de calidad de servicio del enlace radio (por ejemplo intervalos de transmisión, tamaño del bloque de radio, esquema de codificación), que la red de acceso debe cumplir para garantizar la calidad.

2) Control de acceso al medio: La red de acceso de radio, en conjunto con el móvil son los encomendados a realizar el control de acceso de acuerdo a las reglas de la red troncal.

3) Gestión de recursos radio: A través de las funciones de control de potencia, handover, gestión de la asignación de canales/códigos, la red radio se logra asignar y mantener de forma óptima los recursos de radio utilizados por el móvil. Estos

recursos dependen principalmente de la aplicación a utilizar, ya sea voz, datos o video. Tradicionalmente, han existido canales de radio dedicados y compartidos, los cuales se utilizaban dependiendo del tipo de comunicación (voz/datos/video) y de los parámetros de calidad de servicio que ésta requería. Las mejoras e introducciones de nuevos canales radio son constantes en la evolución de estas redes, con el objeto de mejorar la eficiencia espectral y la calidad de servicio. En las redes 3G los últimos canales que fueron incluidos en las especificaciones técnicas son aquellos que proporcionan soporte a los servicios de difusión/multidifusión (broadcast/multicast). En muchos casos, el soporte a estos nuevos servicios no solo involucra nuevos canales, sino cambios en la arquitectura al incluir nuevos elementos y funciones de red.

4) Movilidad de radio: La red de radio es la encargada de gestionar la movilidad, como parte de la gestión de recursos radio, cuando el móvil está conectado a la red, a través de procedimientos de registro, gestión de los estados de movilidad, paging, traspasos, de forma tal de mantener al usuario conectado y utilizar sólo los recursos necesarios de acuerdo a su perfil de movilidad y actividad.

1.2.2 GERAN

Se puede basar uno en la evolución de las redes móviles de acuerdo al siguiente grafico para terminar definiendo a la red GERAN.

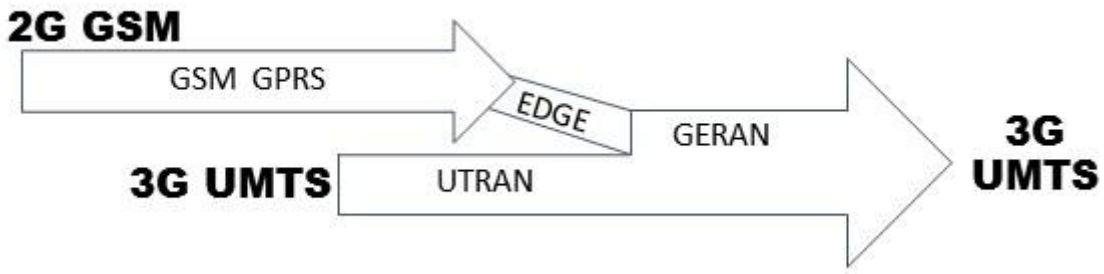


Figura 1.14.-Evolución de la red móvil

Si bien no es tema de nuestra investigación desarrollar la red 2G, la red de acceso de 2G aún forma parte de la actual red de acceso 3G. En ella se define a BSS (Base Station Subsystems – Subsistema de Estaciones Base) como la red de acceso 2G la cual está

compuesta por las BTSs (Base Transceiver Station – Estación Base) siendo el primer componente de la red que permite la conexión de los dispositivos móviles con la red 2G, y las BSC (Base Station Controller –Controlador de Estaciones Base) que controlan las estaciones bases, análogo a los nodos B y RNC en la red 3G.

1.3 Core Network (CN) o Red Troncal

La red troncal debe gestionar la información tanto de voz como de datos que genera la red de acceso. Gracias al protocolo SS7 denominado MAP (Mobile Application Part) UMTS pudo utilizar los mismo estándares que GSM dentro de la red troncal, es decir, las redes troncales GSM, UMTS y GPRS pudieron comunicarse entre sí para ofrecer servicios a los usuarios.

El CN se encuentra compuesto de 2 grandes dominios, la MSC (Mobil Swiching Center) y SGSN (Serving GPRS Support Node). Tanto RNS y BSS conectan a la misma MSC. Ambas son piezas centrales para la conmutación de circuitos y conmutación de paquetes respectivamente. El MSC cuenta con diferentes interfaces para conectar a la red PSTN y a través de esta se transporta el tráfico como señalización.

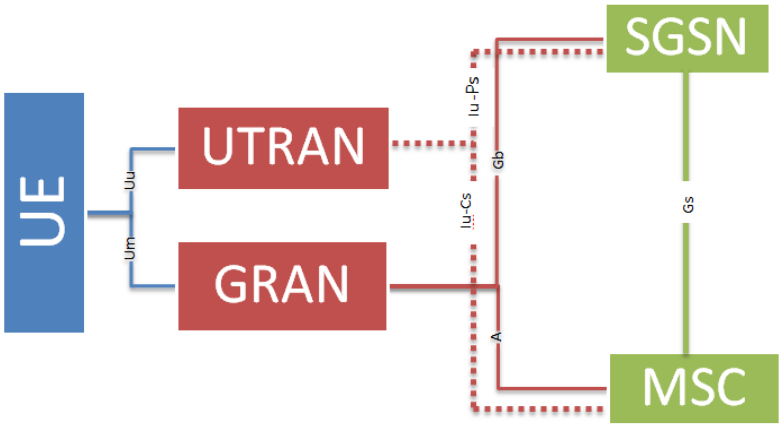


Figura 1.15.-Interfaces de conexión hacia la MSC y SGSN

La MSC es la pieza central de la red basada en conmutación de circuitos. A ella se puede conectar tanto la red GSM como UMTS hacia la red Fija. El MSC es el responsable de realizar la trasmisión de voz, datos y servicios de fax así como Servicios de Mensajes Cortos (SMS) y desvío de llamadas.

Para el caso de GSM, la información de datos y fax debe ser enviada una vez codificada digitalmente al MSC. En este último la señal se debe convertir a señal "analógica" (señal PCM de 64 kbit/s).

La GMSC (Gateway MSC) se puede ubicar entre la PSTN y el resto de los MSCs de la red y su función consiste en rutear las llamadas entrantes al MSC correcto.

SGSN como dijimos anteriormente es una pieza central que se encuentra basada en la conmutación de paquetes, y conectado a la UTRAN mediante la interfaz Iu-PS y a la GSM-BSS mediante la interfaz Gb. Es esta responsabilizado en la entrega de paquetes de datos desde y hacia las estaciones móviles dentro de su área de servicio geográfica. Es además el encargado de enrutar y transferir paquetes, la gestión de movilidad (conexión / desconexión), y la gestión de enlace lógico, autenticación y funciones de carga.

GGSN (Gateway GPRS Support Node), es el encargado de traducir los paquetes que recibió de la red de internet u otras redes privadas. Los paquetes originados por móviles son encaminados a la red correcta por el GGSN.

1.3.1 Interfaces Iu

Esta interfaz se encuentra conectada a la red troncal con la red de acceso de radio UMTS (UTRAN). Es la interfaz central y la más importante para la 3GPP. Puede tener dos diferentes instancias físicas para conectar dos diferentes elementos de la red, dependiendo si se trata de una red basada en conmutación de circuitos (Iu-CS) o basada en conmutación de paquetes (Iu-PS).

En el primer caso, a la interfaz Iu-CS, le corresponde servir de enlace entre la UTRAN y el MSC, mientras que la interfaz Iu-PS es debe encargar de conectar la red de acceso de radio con el SGSN de la red central, tal como muestra la figura 1.3.

1.3.2 Interfaz Iur

Es la interfaz destinada a unir las diferentes RNC entre sí y cuyo propósito es trasmitir datos de soft handover.

1.4 Servicio de portadora

Existen servicios muy importantes, entre ellos la arquitectura del servicio de portadora, que fue definida para negociar las características de la portadora y lograr la trasmición de la información.

GSM y UMTS son diferenciados en base al soporte de alta velocidad de bit, denominada servicio de portadora.

El parámetro de la portadora que se tomó en cuenta, es el servicio/aplicación de este mismo dado por una solicitud de calidad de servicio (QoS). Este servicio es el encargado de proveer la capacidad de transmición de señales entre puntos de acceso involucrando solo funciones de la capa física.

Los servicios de portadora de radio son:

- Dato de conmutación de circuitos: son servicios de dato en tiempo real serán proporcionados para trabajar con la red PSTN/ISDN, operando con la mínima pérdida de datos en Handover.
- Datos de conmutación de paquetes: son provistos para trabajar con redes IP y LANs garantizando la contnuidad de paquetes en Handover

La negociación de atributos de servicio de portadora, para modos de comunicación en tiempo real /no-real y el apropiado servicio de portadora, son flexibles, una de sus principales características.

Cada uno de los servicios de portadora deben ser mapeados a uno o más canales lógicos de interfaz de radio. Estos servicios son identificadod por características puestas entre terminales, con requerimientos en QoS.

La QoS, hace referencia al control de congestión de potencia en donde se pretende mejorar el porcentaje de uso de la misma.

Los requerimientos de servicio de portadora:

- Requerimiento de transferencia de información, caracterizado por la capacidad transferencia de datos entre usuarios en la red
- Las características de calidad de Información de usuarios.

1.5 Arquitectura de Servicio de portadora

Para los servicios y aplicaciones de UMTS, es posible negociar las características de portadora, para la transferencia de información y durante esta.

La calidad de servicio extremo a extremo se sustenta de la calidad de servicio que proporcionan los servicios de portadora subyacente; como el servicio de portadora local, el servicio de portadora UMTS y el servicio de portadora extremo. Estos servicios son construidos sobre servicios que se proveen por la red de acceso.

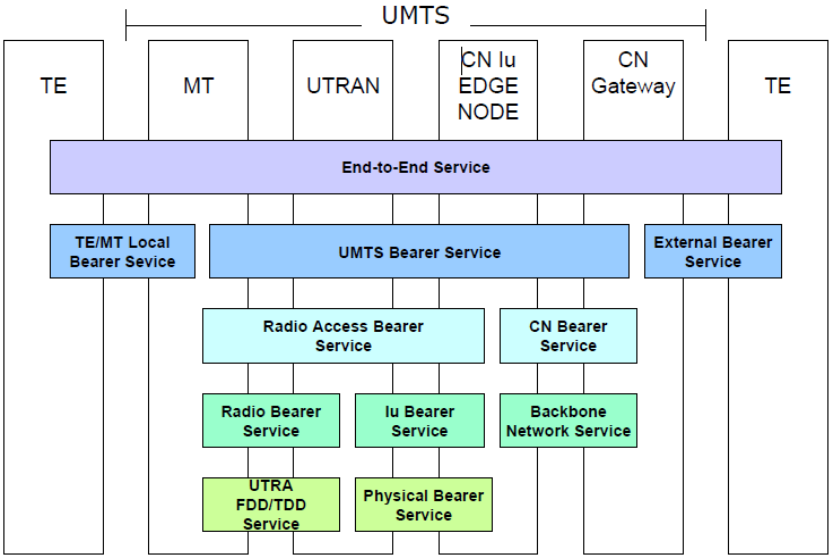


Figura 1.16.-Servicios de portadora UMTS

En una segunda descomposición, el servicio de portadora es sustentado por la QoS que le proporciona el servicio de portadora de la Red de Acceso (RAB), que abarca el trayecto entre el terminal móvil y el nodo de acceso al núcleo de red (MSC/SGSN). Este concepto fue determinante en la provisión de servicios UMTS con diferentes perfiles de QoS, debido a que utiliza la interfaz de servicios de radio y la red de acceso, siendo que ambas poseen limitaciones en su ancho de banda y el servicio de portadora del núcleo de red, que abarca el trayecto entre el nodo de acceso (MSC/SGSN) hasta la red destino. La Qos durante este trayecto es apoyada en la calidad que proporciona el backbon de circuitos o de paquetes.

Para UMTS se han definido cuatro clases de tráfico:

- Convencional. Pudiendo encontrar las comunicaciones de audio y video en tiempo real que exigen un retardo reducido para no perder la sensación de interactividad.

- Streaming. Comprendido por la descarga de contenidos multimedia para su reproducción on-line. El hecho de que la transferencia de información sea unidireccional permitió poder retrasar el instante de inicio utilizando buffers relativamente grandes en el extremo receptor, absorbiendo las fluctuaciones de retardo.
- Interactivo. Abarcado por las aplicaciones de acceso remoto a información en la modalidad on-line, donde el usuario envía peticiones, esperando una respuesta en un tiempo relativamente reducido.
- Background. Esta última clase es usado para aplicaciones de datos que no requieren una respuesta inmediata por parte de la red.

Como hemos apreciado en el gráfico 1,16 cada servicio de portadora está destinado a ofrecer servicios individuales para cada capa.

Las propiedades de una portadora pueden mediante procedimientos ser renegociadas dentro de las conexiones activas. La negociación es realizada por una aplicación, mientras que la renegociación puede ser realizada por la aplicación o la red, como por ejemplo en un handover. La negociación de aplicación debe solicitar una portadora dependiendo de su necesidad. La red luego se encarga de revisar los recursos disponibles y la suscripción de usuarios y posteriormente responder a la solicitud.

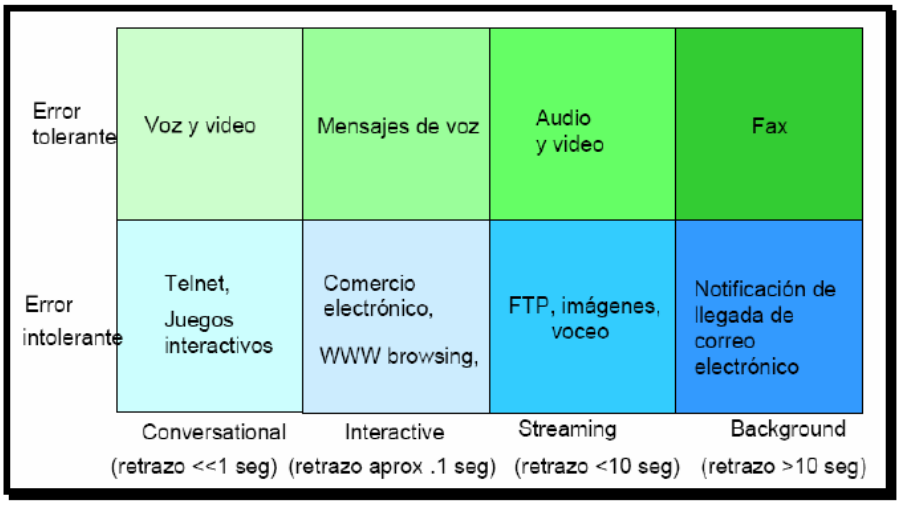


Figura 1.17.-Trafico UMTS

1.6 Sincronización en redes 3G

Una de las funciones más críticas es mantener la sincronización de la red y el usuario. Esta ha sido lograda manteniendo las estaciones bases conectadas entre sí en conjunto con la MSC, utilizando el sistema de posicionamiento global GPS, relacionado en forma síncrona con el tiempo coordinado universal (UTC). Este tiempo debe estar a su vez alineado en forma fija con el código de Seudo Ruido (PN- Pseudo Noise), utilizado por todas las estaciones bases (2 PN cortos de 26.66 ms y un PN largo de 41 días).

La exigencia en la sincronización se debieron a que todas las estaciones bases transmitían a la misma frecuencia y utilizaban los mismos códigos cortos para el ensanchamiento de la señal para el enlace descendente. Las señales diferían en los móviles porque cada estación base utilizaba un desplazamiento del código PN. El móvil al adquirir la señal de la estación base tomaba la referencia del tiempo del sistema al leer la información en el canal de sincronización. Este mensaje permitía al móvil sincronizar su PN largo y su referencia de tiempo con la Estación Base, pero retrasada debido al tiempo de propagación. El móvil trasmitía en el canal ascendente y la señal era recibida en la estación base con un retardo adicional.

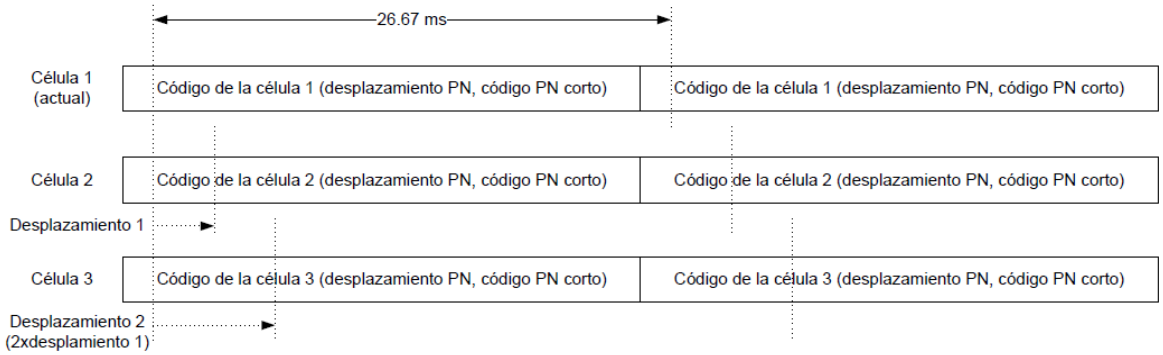


Figura 1.18.-Sincronización de canales

1.6.1 Sincronización para soft-handover

En este caso la MSC se comunica mediante el enlace de bajada con dos estaciones base, por lo que se debe calcular el tiempo de transmisión de la trama, para que al incluir el tiempo de retardo de los enlaces, los mensajes de datos lleguen con el suficiente tiempo para ser transmitidos por la interfaz de aire, además se debe reducir el tiempo de almacenamiento de radio de la estación base, con el fin de minimizar los requisitos de memoria local de las estaciones.

Para lograr este proceso, conocido como alimento de tiempos entre las estaciones bases, los mensajes de bajada (A3-CEData Fordware) contienen el tiempo del sistema, indicando el tiempo en que la trama debe ser enviada por la interfaz de aire, al recibirlo, la estación base deberá calcular el promedio entre el tiempo del sistema al recibir el mensaje y el tiempo ideal, a este tiempo se lo conoce como PATE (Packet Arrival Time Error) y es incluido en el próximo mensaje ascendente. Con esta información el MSC va ajustando la transmisión para su próximo mensaje de datos y se va corrigiendo hasta lograr un PATE 0 o cerca a este valor.

1.7 High Speed Downlink Packet Access (HSDPA)

HSDPA, fue la optimización de la red UMTS/WCDMA que se consideró el paso anterior a la tecnología 4G, ofreciendo una conexión más rápida que las características de 3G pueden aprovechar.

Consistió en un canal compartido en el enlace descendente que mejoró la capacidad de transferencia alcanzando como máximo los 14 Mbps.

La mejora en la red WCDMA obtuvo su máximo potencial en las prestaciones de banda ancha, mediante un aumento de la capacidad de datos, con throughput más elevados. No solo se mejoraron las aplicaciones sino que además permitió que la red sea utilizada por un mayor número de usuarios; proveyendo tres veces más capacidad que WCDMA.

HSDPA proporcionó una mejora en la latencia comparada con otras tecnologías. Siendo la latencia el tiempo transcurrido entre la solicitud enviada y la respuesta de vuelta.

Esto fue de suma importancia para las aplicaciones en tiempo real como VoIP ya que determinaron la calidad del servicio.

Los principios operativos básicos de HSDPA son:

- El RNC se encarga de encaminar los paquetes de datos destinados para un UE particular al Nodo-B apropiado.
- El Nodo-B deben tomar los paquetes de datos y programar su transmisión al terminal móvil emparejando la prioridad del usuario y el ambiente de funcionamiento, estimado del canal con un esquema apropiadamente elegido de codificación y de modulación (es decir, el 16QAM)

- El UE se responsabiliza de reconocer la llegada de los paquetes de datos y de proporcionar al Nodo-B información sobre el canal, control de energía, etc.
- Una vez enviado el paquete de datos al UE, el Nodo-B deberá esperar un asentimiento. De no recibir uno dentro de un tiempo prescrito, asumirá que el paquete de datos fue perdido y lo deberá retransmitir.

CAPITULO 2: PROTOCOLOS DE LA FAMILIA TCP/IP

TCP/IP fue desarrollado a principios de los años 70 por el Departamento de Defensa de EE.UU (DoD) a fin de crear una red que pudiese sobrevivir a cualquier circunstancia. El DoD requería una transmisión de datos confiable hacia cualquier destino de la red en forma independiente en un mundo cruzado por numerosos tendidos de cables, alambres, microondas, fibras ópticas y enlaces satelitales.

En 1993 adoptó su estructura actual –INTERNET- para la interconexión de diversas redes de datos. Los protocolos de la familia TCP/IP definieron básicamente la forma de interconectar subredes y enrutar tráfico entre ellas.

TCP e IP no son protocolos OSI y por lo tanto no se ajustaban a su Modelo de Referencia, sin embargo el servicio que ofrecía el protocolo IP es muy similar al servicio de red no orientado a conexión y, de esta manera, a IP se lo designó como un protocolo de capa 3. De forma similar TCP puede ser comparado en funcionalidad con un protocolo de capa 4 del Modelo de Referencia.

La familia de protocolos TCP/IP definió 4 capas. Algunas de estas capas si bien fue denominada del mismo modo que las del Modelo de Referencia OSI, cada capa se desempeñó de manera diferente en cada modelo.

2.1 Protocolo de Capa de Aplicación

Los protocolos describen el conjunto de normas y convenciones que rige la forma en que los dispositivos de una red intercambian información, algunos protocolos de la capa de aplicación del modelo TCP/IP son:

- Telnet: protocolo de emulación de terminal estándar que es utilizado para la conexión de terminales remotas, permitiendo que los usuarios sean registrados en dichos sistemas y utilicen los recursos como si estuvieran conectados localmente.

OSI	TCP/IP	PROTOCOLOS
APLICACIÓN PRESENTACION SESION	APLICACION	TELNET, FTP, LDP, SNMP, TFTP, SMTP, NFS, X WINDOWS
TRANSPORTE	TRANSPORTE	TCP, UDP
RED	INTERNET	ICMP, BOOT, ARP, RARP, IP
ENLACE DE DATOS FISICA	RED	ETHERNET, FAST-ETHERNET, TOKEN RING, FDDI

Figura 2.1.- Comparativa entre el Modelo de Referencia OSI y el Modelo TCP/IP

- FTP: destinado a la transferencia de archivos entre dispositivos de una red utilizando un mecanismo orientado a conexión.
- TFTP: versión simplificada de FTP que permite la transferencia de archivos de una manera menos confiable.
- DNS: sistema de denominación de dominios utilizado para convertir nombres de los nodos en direcciones.
- SMTP: protocolo simple de transferencia de correo basado en texto utilizado para el intercambio de mensajes de correo electrónico entre distintos dispositivos.
- SNMP: protocolo de administración de redes, que brinda una forma de monitoreo y controlar dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.
- DHCP: protocolo que proporciona un mecanismo para asignar direcciones IP en forma dinámica, permitiendo la reutilización de dirección IP automáticamente a medida que un dispositivo ya no la necesite.

2.2 Protocolo de Capa de Transporte

Encargado de dar soporte a la capa superior brindando apoyo, al enviar datos sin importar el contenido de los mismos.

- TCP: protocolo de control de transmisión, encargado del control de flujo, reensamblado de paquetes y acuses de recibo. Este protocolo, se encuentra orientado a conexión y utiliza un *saludo* de tres vías antes de la transmisión de datos. El flujo de paquetes es negociado dinámicamente entre el emisor y el receptor definiendo los acuses de recibo (ACK) que confirman la recepción y el envío de los posteriores paquetes.
- UDP: es en general menos seguro que TCP porque no es orientado a conexión y tampoco posee control de errores. Los datos son enviados sin verificar previamente el destino, sin embargo es muy utilizado por el bajo consumo de recursos de la red.

2.3 Protocolo de Capa de Internet

Estos son algunos de los protocolos más usados que operan en la capa de internet del modelo TCP/IP:

- IP: proporciona enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. No se ve afectado por el contenido de los paquetes sino que se encarga de buscar una ruta hacia el destino.
- ARP: protocolo de resolución de direcciones. Determina la dirección de la capa de enlace de datos, la dirección MAC o la dirección física de los dispositivos, para las dirección IP conocidas (direcciones lógicas)
- RARP: protocolo de resolución inversa de direcciones, establece la dirección IP cuando se conoce la dirección MAC.
- ICMP: protocolo de mensajes de control en internet. Suministra capacidades de control y envió de mensajes. Herramientas tales como PING, utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específica y esperando una determinada respuesta.

2.3.1 Direccionamiento IP

Para que dos dispositivos de comuniquen entre si es necesario identificarlos claramente. Una dirección IP es una secuencia de unos y ceros de 32 bits. Para hacerlo más compresible, una dirección IP aparece escrita en forma de cuatro secuencias de números decimales separados por puntos. Cada número decimal se define como un octeto de 8 bits de acuerdo al posicionamiento exponencial del número binario. Así cada octeto

puede tomar un valor entre 0 (todos los bits en cero) y 255 (todos los bits en uno). Un ejemplo estaría determinado en la figura 2.2.

Decimal	172.	16.	1.	3
Binario	10101100	00010000	00000001	00000011

Figura 2.2.- dirección IP de 4 octetos

Las direcciones IP se dividieron en clases para definir las redes de tamaño grande, mediano y pequeño. Las direcciones de clase A se asignaron a las redes de mayor tamaño, las direcciones de clase B para redes medianas y las clases C para las más pequeñas. Las direcciones IP constan de dos partes, una para identificar a la red y la otra que identificar al dispositivo conectado a la red.

- Clase A: se utilizó el primer octeto para definir la red, y los otros tres para definir los dispositivos en cada red. Rango de direcciones IP 0.0.0.0 a 127.0.0.0 permitiendo 128 redes de 16 millones de dispositivos.
- Clase B: los dos primeros octetos se usaron para definir redes mientras que los dos segundos para definir dispositivos, de la siguiente manera: rango de direcciones IP de 128.0.0.0 a 191.255.0.0 lo que permite un total de 16384 redes y 65000 dispositivos.
- Clase C: los tres primero octetos se dispusieron para definir la red y el último octeto para definir los dispositivos de la red. El rango puede variar desde 192.0.0.0 a 223.255.255.0 que permiten 2.097.152 redes con 254 dispositivos.

También se definieron las denominadas Clase D y Clase E. Siendo las primeras para uso multicast mientras que las segundas para uso experimental. A todas estas clases de direcciones también fueron conocidas como IPv4.

2.3.2 Determinación de Rutas IP

Existen dispositivos como router con la posibilidad de determinar la ruta al destino, teniendo un previo conocimiento de las diferentes rutas hacia él y de cómo llegar al mismo.

El aprendizaje y la determinación de estas rutas es llevado a cabo mediante un proceso dinámico a través de cálculos y algoritmos que son ejecutados en la red, o mediante un proceso estático, el cual es ejecutado manualmente.

EL router en base a la información de enrutamiento que recibió desde otros routers vecinos se encarga de armar su propia tabla de enrutamiento. Luego, se vale de esta tabla para determinar los puertos de salida a la hora de retransmitir un paquete.

La tabla de enrutamiento puede ser construida mediante uno de estos dos métodos, o de ambos:

- Rutas estáticas: son establecidas rutas en forma manual mediante un administrador, quien también debe actualizar manualmente cuando tenga lugar un cambio en la topología.
- Rutas dinámicas: rutas aprendidas automáticamente a través de la información enviada por otros routers.

2.3.3 Protocolo de Enrutamiento

Se dispusieron dos grandes núcleos de protocolos de enrutamiento:

- Protocolos de Gateway Interior (IGP): usado para el intercambio de información de enrutamiento dentro de un sistema autónomo. Ejemplo RIP, IGRP.
- Protocolo de Gateway Exterior (EGP): utilizado para el intercambio de información de enrutamiento entre sistemas autónomos.

Todos los protocolos de enrutamiento son diseñados para cumplir las mismas funciones, aprendiendo y determinando cual es la mejor ruta para llegar al destino. Existen dos clases de protocolos de enrutamiento:

- Vector distancia: determinan la dirección y la distancia a cualquier red.
- Estado de enlace: poseen una idea exacta de la topología de la red, y no efectúan actualizaciones a menos que ocurra un cambio en la topología de la red.

2.3.3.1 Vector distancia

Se conoce la distancia como una medida de longitud mientras que al vector se lo conoce como una dirección. Por lo tanto, cada protocolo de enrutamiento basado en vector

distancia se vale de un algoritmo, o una métrica diferente, para determinar el camino óptimo hacia el destino.

Las métricas utilizadas habitualmente por los protocolos de enrutamiento pueden calcularse basándose en uno o en múltiples características de la ruta, entre ellas se encuentran:

- Número de saltos: número de routers por lo que pasa un paquete
- Coste: basado generalmente en el ancho de banda, coste económico u otra métrica que puede ser asignado a una ruta.
- Ancho de banda: capacidad de datos de un enlace.
- Fiabilidad: normalmente se refiere al valor de errores de bits de cada enlace.
- MTU: unidad máxima de transmisión. Longitud máxima de trama que puede ser aceptada por todos los enlaces de la ruta.

2.3.3.2 Estado de Enlace

Los protocolos de estado de enlace construyen sus tablas de enrutamiento basándose en una base de datos de una determinada topología. Esta, son elaboradas a partir de paquetes de estado de enlace que se pasan entre todos los routers, para describir el estado de una red.

Una vez que se ha formado la tabla de enrutamiento, los routers proceden a calcular en forma independiente su mejor ruta hacia un destino determinado, generando una visión independiente de la red por cada routers.

Estos protocolos no están limitados por una cantidad de saltos. Al encontrar una falla en la red, el router debe avisar al resto de sus enrutadores vecinos mediante un mensaje multicast, y estos la reenvían a sus vecinos.

Los protocolos de enrutamiento de estado de enlace son del tipo enrutamiento de Gateway interior (IGP) ya que utilizan un sistema autónomo, el que a su vez, puede ser separado en sectores más pequeños mediante divisiones lógicas.

Haciendo un comparativo, los protocolos de estado de enlace son más rápidos y escalables que los de vector distancia, siendo algunas razones:

- Los protocolos de estado de enlace solo envían actualizaciones si hay cambios en la topología
- Las actualizaciones periódicas son menos frecuentes que en los de vector distancia

- Las redes que ejecutan protocolos de enrutamiento por estado de enlace puede ser segmentadas en distintas áreas, limitando así el alcance de las rutas.

2.4 IPV6

Para que un dispositivo pueda conectarse a internet, necesitan de una dirección IP. Cuando se diseñó IPv4, casi como un experimento, no se pensó que pudiera tener tanto éxito comercial, y dado que sólo dispone de 2^{32} direcciones (direcciones con una longitud de 32 bits, es decir, 4.294.967.296 direcciones), junto con el imparable crecimiento de usuarios y dispositivos, repentinamente este número se hizo muy fácil de alcanzar, especialmente para las redes de clase B.

Paralelamente, se produjo un gran y rápido aumento de las tablas de enrutamiento a medida que las redes de clase C se conectaban en línea. La inundación resultante de la nueva información de la red amenazaba la capacidad de los Routers de internet para ejercer una efectiva administración.

Por este motivo, y previendo la situación, el organismo encargado de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), creó hace más de una década IPv6 o IPng (IP nueva generación). El mismo permitió direcciones con una longitud de 128 números hexadecimales, proporcionando un total aproximado de 640 sextillones de direcciones.

El despliegue de IPv6 se comenzó a realizar gradualmente, en una coexistencia ordenada con IPv4, al que irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

Las direcciones IPv6 son asignadas a las interfaces y no a los nodos como lo hacía en IPv4, y como cada interfaz pertenece a un solo nodo. Cualquiera de las direcciones unicast asignada a las interfaces del nodo se puede usar como identificador del nodo.

Ejemplo de una dirección IPv6:

24AE:0000:F2F3:0000:0000:0687:A2FF:6184

Para que las direcciones sean más fácil de leer, es posible omitir los ceros iniciales de cada campo.

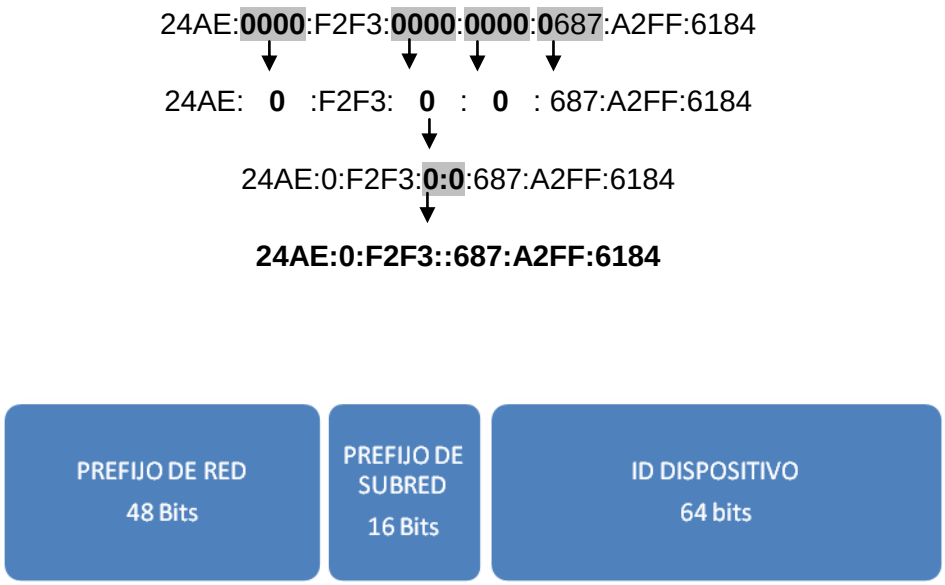


Figura 2.3.- composición de la dirección IPv6

2.4.1 Transición a IPv6

Dado que el protocolo predominante en la actualidad en Internet es IPv4, e Internet se ha convertido en algo vital, no ha sido posible sustituirlo, es decir, no es posible apagar la Red, ni siquiera por unos minutos y cambiar a IPv6.

No basta con la actualización de unos pocos equipos. Esta, es una operación que tendría que involucrar a cualquier organización, sea empresa, administración pública o proveedor de acceso o contenidos, de una forma sincronizada, lo cual es imposible.

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), diseñó junto con el propio IPv6, una serie de mecanismos llamados de transición y coexistencia.

Básicamente es importante entender lo que ello implica. No se trata de realizar una migración, como erróneamente se indica en muchas ocasiones, sino que ambos protocolos, IPv4 e IPv6, deberán existir durante algún tiempo, es decir se produce una coexistencia. Es como una balanza, en la que hoy en día, el lado con el mayor peso representa el tráfico IPv4, pero poco a poco, gracias a esta coexistencia, mientras se conformen más contenidos

y servicios con IPv6, el peso de la balanza se inclinará hacia el otro lado hasta que IPv6 sea predominante. A esto se lo denominó la transición.

El diseño del protocolo IPv6 da preferencia a IPv6 frente a IPv4, si ambos están disponibles (IPv4 e IPv6). De ahí que se produzca ese desplazamiento del peso de una forma natural, en función de múltiples factores, y sin que podamos determinar durante cuánto tiempo seguirá existiendo IPv4 en la Red y en qué proporciones.

2.4.2 IPv6 para Usuarios

Los usuarios de Internet, desde el punto de vista de usuarios conectados a una red doméstica o incluso un punto de acceso público, no deberían apreciar el uso de IPv4 o IPv6, al menos eso es lo que se ha intentado desde los organismos de estandarización (IETF).

Generalmente, hay varios elementos de la red doméstica en los que el uso de IPv4 o IPv6 es relevante: Las computadoras personales, tabletas, teléfonos inteligentes, dispositivos multimedia y cualquier otro aparato que se conecte a Internet.

Desde el año 2001, aproximadamente, la mayoría de los sistemas operativos, por ejemplo a partir de Windows XP, se implantó soporte de IPv6. Exactamente igual para Mac OS X, Linux, BSD, etc. Esto fue desarrollado tanto para sistemas operativos clientes como servidor.

La diferencia fundamental es que inicialmente IPv6 no estaba activado por defecto (caso de XP y 2003), mientras que en las siguientes versiones ya lo incorporaron (Windows Vista, 7, Mac OS X, mayoría de Linux y similares). Aquellos dispositivos que no tenían IPv6, podían ser actualizados.

Desde el punto de vista de las aplicaciones más comunes, por ejemplo en navegador (Internet Explorer, Firefox, Safari, Opera, etc.), pueden soportar de forma automática IPv6, incluso aplicaciones para compartir archivos como Bittorrent y similares. En cambio otras, como Skype, aún no, aunque la mayoría de los fabricantes de este tipo de aplicaciones han confirmado que están trabajando en ello. Esto no es presentó inconvenientes por el momento, además cabe destacar que es un proceso de forma automática y debería de ser transparente para el usuario.

El router de acceso a Internet, denominado CPE (Customer Premises Equipment) por los proveedores de acceso, no dispone de soporte para el protocolo IPv6, pero estos fueron suministrados por los proveedores de servicios de internet, aunque en muchas

ocasiones, incorporaron sistemas operativos de código abierto (Linux y otros), y que podían ser actualizados por usuarios avanzados.

En algunas redes domésticas, además del router, existen otros elementos de red, como por ejemplo, puntos de acceso WIFI, concentradores de red, puentes para usar la red eléctrica, etc. Muchos de estos elementos, funcionan en lo que se llama modo “puente” (bridge, o técnicamente “nivel 2”) y por tanto deberían de ser transparentes a IPv4 e IPv6. Si alguno de estos elementos son “nivel 3”, es decir, tienen funciones de encaminado, el usuario tendrá que comprobar que soporta IPv6, en caso contrario IPv6 no pasaría a través de dicho dispositivo.

Hasta el año 2011, pocos proveedores de Internet proporcionaban a sus clientes acceso con IPv6, aunque esto ha cambiado, se incrementó significativamente el ritmo de su introducción, de forma considerable.

Dado que las aplicaciones utilizan IPv6 de forma automática, los sistemas operativos se ocupan de detectar si la red, en la que el dispositivo está conectado, tiene soporte IPv6. Es decir, si tanto el router, como otros dispositivos de red y la propia conexión con el proveedor de servicios de internet, ofrecen IPv6. Si los tres elementos están preparados, el sistema operativo así se lo indicará a la aplicación, para que pueda usar IPv6. En caso de que alguno de estos tres elementos no esté preparado, el sistema operativo puede intentar los denominados mecanismos automáticos de transición

Los mecanismos automáticos de transición siempre funcionan para aplicaciones cliente-a-cliente (mensajería, compartición de ficheros, etc.), pero podrían fallar para aplicaciones cliente-servidor (navegación en páginas web, correo electrónico), porque muchos proveedores de servicios de internet no despliegan los denominados “relés” de esos mecanismos de transición.

Si estos no funcionan para aplicaciones cliente-servidor, entonces, el sistema operativo, tras un tiempo de espera, debe volver a intentarlo con IPv4.

Una alternativa es realizar transición en forma manual (por ejemplo los denominados tunnel brokers), que aunque son fáciles de configurar, incluso puedes ser proporcionado por el propio ISP. En general requieren ejecutar por parte del usuario alguna aplicación o configuración en su equipo, por lo cual su uso no está muy extendido.

2.4.3 IPv6 para empresas

Para empresa, sea del tamaño que sea, se plantearon en primer lugar, los mismos retos que en el caso de los usuarios finales.

Es posible que en una red corporativa utilice aplicaciones hechas a medida, bien por personal de la propia empresa o adquiridas a terceros. Será necesario comprobar que dichas aplicaciones siguen funcionando en una red doble-pila (con IPv4 e IPv6), y aunque no funcionen con IPv6 en una primera fase, es importante pensar que han de ser actualizadas en breve, para permitir que usuarios corporativos desde fuera de la red, conectados sólo con IPv6, puedan acceder a ellas.

Los routers suelen ser dispositivos no tan simple como un CPE doméstico, con la ventaja de que la mayoría de los que están en el mercado desde hace 4-5 años, ya tienen soporte IPv6 o podría ser actualizados con una nueva versión de software proporcionada por el fabricante. La complejidad en una gran empresa se da por la presencia de múltiples routers, incluso con múltiples enlaces a Internet o enlaces con otras redes de la corporación (ejemplo un banco con cientos de oficinas).

Los dispositivos presentes en la redes corporativas fueron aumentando proporcionalmente al tamaño de la empresa, número de oficinas, etc., como pueden ser cortafuegos, dispositivos de prevención de intrusión y otros dispositivos de seguridad, como, balanceadores de carga, dispositivos de cache y/o proxy, dispositivos de VPN, dispositivos de Voz sobre IP, teléfonos IP, dispositivos de videoconferencia, y un sinfín de elementos adicionales de red.

Es importante hacer una correcta evaluación de estos dispositivos, de sus capacidades de soporte IPv6, y el impacto sobre la red en caso de que no ser soportados. Es posible que no haya más remedio que reemplazar estos equipos, aunque en ocasiones, hay soluciones alternativas a la de reemplazarlos.

2.4.3.1 El Proyecto IPv6

Especialmente en empresas medianas y grandes, IPv6 puede constituir por sí mismo un nuevo proyecto del equipo de Tecnologías de la Información y las Comunicaciones.

Habrá que tener en cuenta aspectos como:

- Plan de formación
- Evaluación de la red, sus equipos y sus versiones de software

- Posibles nuevas adquisiciones, fabricantes y modelos
- Evaluación de Sistemas Operativos
- Evaluación de aplicaciones propias y de terceros
- El plan de direccionamiento de la red
- Conexión a los proveedores de servicios de internet y otros enlaces (otras oficinas, clientes, proveedores)
- Plan de inversión

2.4.4 IPv6 para ISP

Las redes de los proveedores de servicios de Internet (ISPs) pueden ser consideradas como un super conjunto de las redes empresariales, sobre todo en las grandes corporaciones. La diferencia radica en que los bancos tienen que atender sólo a los requisitos de tráfico entre las redes de sus propias oficinas, mientras que un ISP atiende cientos, miles o millones de clientes diferentes.

Afortunadamente los protocolos utilizados en estas redes y en concreto MPLS y derivados, facilitaron esta labor, no solo desde el punto de vista de IPv4, sino también desde el punto de vista del despliegue de IPv6.

Los ISPs pueden contar sólo con una red, en ocasiones extendida a través de múltiples países o regiones geográficas, pero a veces también cuentan con centros de datos (Data Centers), donde alojar servicios propios y/o de clientes. Dentro de esta última categoría, se podría contemplar a las organizaciones que aun no teniendo red propia. Estas, conectan a otros ISPs, para simplemente dar servicios de centros de datos, comúnmente denominados “alojamiento” (lógico o físico, es decir, hosting o housing).

Esto tiene importantes implicaciones en la forma en la que se ha de desplegar IPv6 en dichas redes, pues puede que sea necesario separar ciertas infraestructuras o equipamientos para diferenciar los equipos propios alojados, de los que son propiedad de los clientes.

En cuanto a las redes en sí mismas, hay que diferenciar diferentes tipos de redes (redes fijas, redes móviles), diferentes tecnologías (fibra, cobre, WiMax, WIFI, LMDS, etc.), así como también diferentes partes de la red (troncal, distribución, agregación, acceso, etc.).

CAPITULO 3: ATM - MODO DE TRANSFERENCIA ASINCRONICO

A mediados de la década del 80 se comenzó a trabajar en la segunda generación de la red ISDN (Red Digital de Servicios Integrados), conocida como la ISDN de banda ancha (ISDN-BA).

Con la idea de soportar nuevas aplicaciones, como el video o la imagen de alta definición, la extensión del ancho de banda por encima de los 150Mbit/s se hiso evidente. Surgieron desde esta premisa nuevas técnicas -basadas en el tratamiento de células sobre un medio sincrónico de transmisión (SDH/Jerarquía Digital Sincrónica) y de conmutación (ATM/ Modo de Transferencia Asincrónico) que constituyeron los fundamentos de la nueva ISDN-BA.

Para aprovechar al máximo la capacidad de transmisión que ofrecían las redes SDH se necesitaba una técnica de conmutación capaz de tratar cualquier tipo de información y que al mismo tiempo optimizara la utilización del ancho de banda, siempre sobre la base de asignación bajo demanda.

Se definió entonces el formato del paquete ATM, compuesto por una cabecera de 5 bytes y un campo de información de 48 bytes, como muestra la figura 3.1.

Donde:

- Campo de control de flujo genérico o GFC (*Generic Flow Control*). La cabecera del tipo UNI (comunicación entre dispositivos finales ATM), a diferencia de la NNI (comunicación entre conmutadores ATM), no soporta el GFC.
- Identificador del tipo de carga o PTI (*Payload Type Identifier*). Indica en el primer bit si la celda contiene datos de usuario o datos de control. Si la celda contiene datos de usuario, el segundo bit indica congestión, y el tercer bit indica si la celda es la última en una serie de celdas que representan una única trama AAL5.

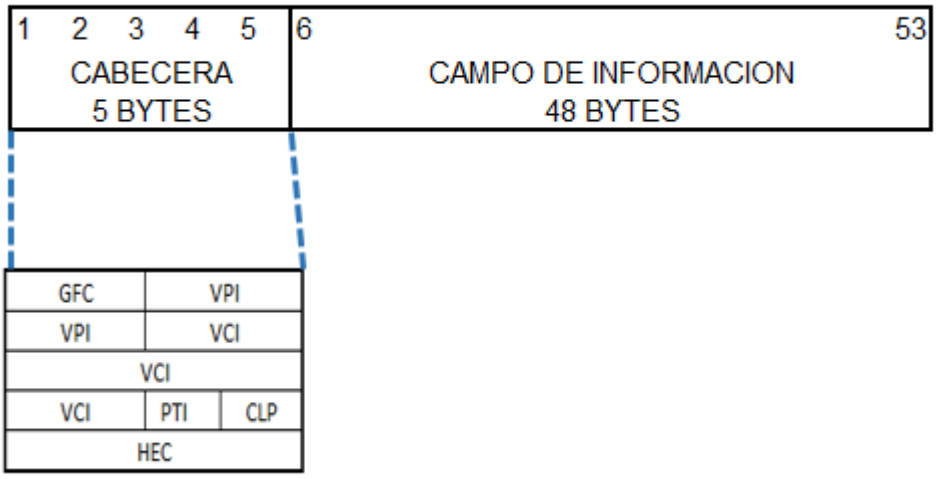


Figura 3.1.- Formato de celda ATM

- Identificador de canal virtual o VCI (*Virtual Channel Identifier*) e identificador de camino virtual o VPI (*Virtual Path Identifier*). Identifican el siguiente destino de la celda cuando pasa a través de varios conmutadores ATM. Un camino virtual o VP (*Virtual Path*) no es más que la multiplexación de diversos flujos de tráfico sobre un mismo medio de transmisión, y es identificado por el VPI. Un camino de transmisión es un conjunto de VPs. En ATM cada uno de estos VPs es más tarde multiplexado en un cierto número de canales virtuales o VCs (*Virtual Channels*), identificados mediante los VCIs. Un VP es, por lo tanto, un conjunto de VCs, cada uno de los cuales es conmutado de forma transparente a través de la red ATM en base a un VPI común. Los VCIs y VPIs sólo tienen un significado local a lo largo de un enlace en particular y se hace una correspondencia, cuando sea apropiado, en cada conmutador.
- Prioridad de pérdida de celda o CLP (*Cell Loss Priority*). Indica si la celda debe ser descartada en el caso de que haya congestión en su tránsito por la red. Si el CLP es igual a 1, la celda debe ser descartada antes que las celdas de la misma conexión con el CLP igual a 0.
- Campo de control de errores o HEC (*Header Error Check*). Calcula el código de redundancia cíclica sobre la cabecera de la celda. Se utiliza para localizar errores en la cabecera y corregirlos, si el número de ellos no es mayor que 2; en caso contrario, cuando existan más de 2 errores, la celda se descarta.

Al ser basado ATM en paquetes de longitud reducida y fija, se simplificó en gran

medida el diseño de conmutadores. Se redujo el retardo de proceso y se disminuyó su variabilidad, lo que resultó esencial para aquellos servicios de voz y video. Al ser cada paquete de longitud fija también implicó el uso de buffers de longitud fijos para gestionar el tráfico y evitar congestiones y, por expansión, técnicas de control más sencillas.

3.1 CONCEPTOS BASICOS ATM

La tecnología ATM (Asyncronous Transfer Mode) es una tecnología de conmutación de celdas que utiliza la multiplexación por división de tiempo asincrónico, permitiendo una ganancia estadística a la agregación de tráfico de múltiples aplicaciones. Las celdas son unidades de transferencia de información en ATM. Estas celdas se caracterizaron por tener una longitud fija de 53 octetos, lo que permitió que la conmutación sea realizada por el hardware, consiguiendo alcanzar altas velocidades fácilmente escalables (2, 34, 155 y 622Mbit/s)

ATM es una técnica de trasferencia rápida de información binaria de cualquier naturaleza, basada en la transmisión de celdas de longitud fija, sobre las actuales redes plesiócronas (PDH) y/o sincrónicas (SDH). Debido a su naturaleza asincrónica, un flujo de celdas ATM puede ser transportado como una serie de bytes estandarizados, para una trama PDH como un contenedor SDH; de esta manera no es necesario realizar grandes inversiones en infraestructura de red.

Antes de la emisión de una celda es establecida una conexión virtual extremo a extremo mediante un proceso de control que acepta o rechaza la misma, en base al grado de servicio solicitado y otros parámetros definidos por el usuario.

Como ATM es una tecnología orientada a conexión, la señalización constituye uno de los aspectos fundamentales, ya que se pone en marcha siempre al querer establecer una conexión. Solamente que el destino acepte la llamada, por medio de un proceso de negociación entre los extremos, se establece la apertura de una conexión virtual.

Cada conexión virtual es identificada por un número, cuyo significado es solo local, es decir que está asociado a cada enlace. Esta función de identificación es ejecutada por dos sub-campos de la cabecera ATM: el VCI y el VPI. El VCI identifica a un VC específico de un determinado VP. El VC es un concepto usado para describir un transporte unidireccional de celdas ATM, mientras que un VP es un conjunto de VC unidireccionales que transportan celdas ATM.

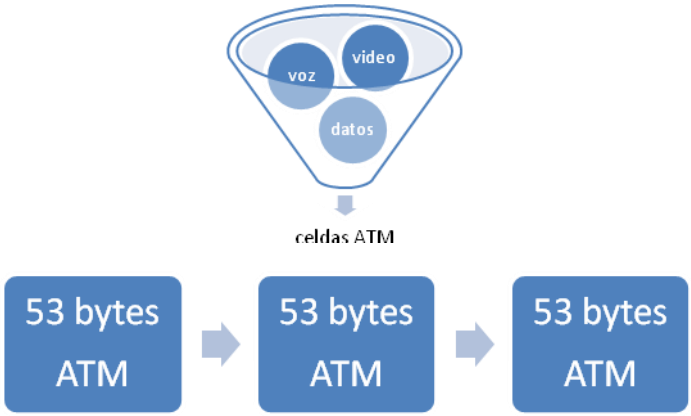


Figura 3.2.- Capacidad de transporte ATM

El propósito de los VPs y VCs es el de usar los conceptos de enlace virtual y conexión virtual. Los VPs permiten que la capacidad del medio físico sea dividida en un número de canales con velocidades variables. Los VC permiten una subdivisión de la capacidad de un VP. La conmutación ATM se lleva a cabo siempre primero en VP y luego en los VC.

Un camino virtual (VP) es un conjunto de circuitos virtuales (VC) que poseen los mismos puntos finales, concepto que fue desarrollado para las redes de alta velocidad con el fin de disminuir el costo del manejo de las señales de control. (X25, Frame Relay)

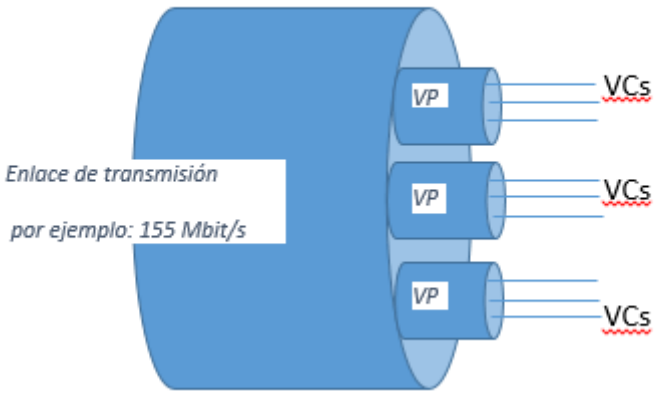


Figura 3.3.- Circuitos y caminos virtuales en ATM

Las conexiones virtuales ATM pueden proporcionarse utilizando gestión de red, mediante canales virtuales permanentes (PVC – Permanent Virtual Channel) así mismo, los

canales virtuales pueden establecerse dinámicamente utilizando procedimientos de señalización ATM.

3.2 SEÑALIZACION ATM

La señalización es un proceso mediante el cual los usuarios ATM y la red intercambian información de control, peticiones para el uso de los recursos de la red y negociaciones para el uso de parámetros de circuitos. El par VPI y VCI y el ancho de banda requerido son escogidos como resultado de un intercambio de una negociación exitosa.

De este proceso de negociación se destaca que no existe un canal de negociación específico, sino que existe un canal virtual independiente para cada terminal. En lugar de negociar el acceso a un canal, lo que se negocia es la asignación de VPI/VCI que determina la conexión virtual entre extremos.

La figura 3.4 muestra los mensajes de extremo a extremo SETUP (establecer) y CONNECT (conexión) utilizados para conexiones punto a punto. Los otros mensajes como CALL PROCEDDING (llamada en progreso) y CONNECT ASK (conexión reconocida) tienen solo significado local. Estos mensajes son protegidos utilizando temporizadores de supervisión, cuando termina el temporizador, la llamada terminará si no existe respuesta.

3.3 NIVELES PROPIOS DE ATM

El modelo ATM consta de tres niveles que siguen la estructura de capas del modelo OSI, estos definen como los distintos tipos de tráficos se pueden mezclar en la misma red. Estos tres niveles son: Nivel de adaptación, Nivel ATM y Nivel de transporte.

3.3.1 NIVEL DE ADAPTACION

Este nivel es el superior y establece la relación entre el dispositivo que genera el tráfico y el siguiente nivel. Le da a ATM la flexibilidad para transportar distintos tipos de servicios dentro del mismo formato. El principal propósito de este nivel es solucionar diferencia existente entre el requerido por el usuario y los disponibles en el nivel de AAL (ATM Adaptation Layer)

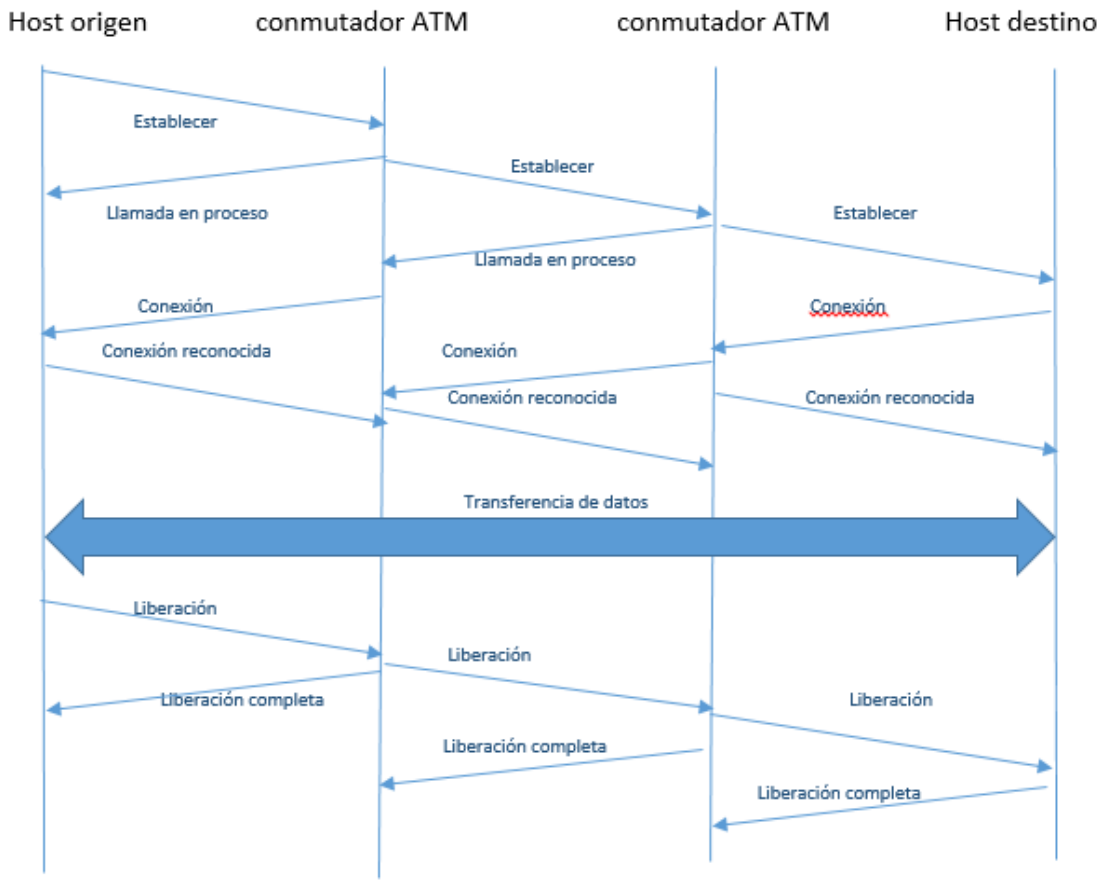


Figura 3.4.- Establecimiento y liberación de una conexión en ATM

Las AAL son cinco, divididas en función de las características del tráfico a manejar: AAL 1 (servicio de emulación de circuitos, con velocidad binaria constante y orientado a conexión), AAL 2 (video bajo demanda con velocidad binaria variable y orientado a conexión), AAL 3/4 (frame relay y SMDS con y sin conexión) AAL 5 (versión mejorada a la anterior para LANs de alta velocidad).

- AAL 1

  Se usan para la transferencia constante de bits lo cual es dependiente del retardo. Por lo tanto ATM provee un determinado ancho de banda para toda la comunicación. Se utilizan para aplicaciones tales como videoconferencias y videotelefonía.

- AAL 2

  Se utilizan para servicios orientados a conexión y utilizan una tasa de transferencia de bits variables. Las aplicaciones que más se adaptan a este tipo de servicio son las que no requieren un ancho de banda constante, por ejemplo transferencias de

datos, ya que estas requieren una alta tasa de transferencia durante cortos periodos de tiempo.

- AAL 3
  Las aplicaciones que mejor se adaptan son aquellas que requieren una velocidad de transmisión variable orientas a conexión y no son dependientes del retardo. Existen redes ATM que utilizan este servicio para soportar Frame Relay.

- AAL 4
  Diseñado para el transporte de datos a velocidades variables independientemente del tráfico y en modo sin conexión. Es decir, puede transferir datos sin necesidad del establecimiento de la conexión con el extremo remoto.

En la figura 3.5 resume los diferentes servicios que ofrece el nivel de adaptación de ATM

3.3.2 NIVEL ATM

El nivel ATM es el responsable de añadir el campo de cabecera para establecer los mecanismos de encaminamiento, control de flujo y corrección de errores. Es decir, añade a los 48 bytes de información los 5 bytes con la información necesaria para que la celda se encamine por la red ATM y llegue a su destino.

Existe una pequeña diferencia en el tamaño en bits de cada campo de la cabecera dependiendo si se trata de una celda UNI (User Node Interface – interface nodo/usuario) o NNI (Network Node Interface – interface entre nodos de red).

3.3.3 NIVEL DE TRANSPORTE

El nivel de transporte físico se subdivide en dos subniveles: “convergencia de transmisión” que se encarga de los aspectos independientes del medio de transmisión empleado y “nivel medio físico” que establece las características del medio físico a emplear y el tipo de transmisión

	servicios del nivel de adaptacion (clase de Servicios RDSI-BA)			
	AAL 1 (A)	AAL 2 (B)	AAL 3 ©	AAL 4 (D)
Relación de tiempo entre Origen y Destino	Requerida		No Requerida	
Velocidad de transferencia	Constante	Variable		
Modo de conexión	Orientado a conexión			Sin conexión

Figura 3.5.- Tabla de clasificación de servicios en ATM

CAPITULO 4: MULTI-PROTOCOLO DE CONMUTACION DE ETIQUETAS MPLS

4.1 IP vs ATM

La convivencia de las tecnologías IP y ATM, fue en sus inicios un tema bastante candente. El hecho de que en muchos casos las redes LAN que utilizaban el protocolo IP y los backbones sobre las que se venían sosteniendo, estaban implementadas en ATM, creaban legítimas WAN sobre ATM. El problema radicaba en los costos reales que acarreaba crear una u otra red, así como también, los servicios que eran capaces de soportar y el tiempo de respuesta que podrían llegar a proporcionar.

En aquel momento parecía ser que para la necesidad de servicios de datos (como conexiones a Internet, teletrabajo u otros similares) la opción clara era la de una red sobre IP, dado que el hardware y software requerido era existente y a muy bajo costo. Mientras tanto, las redes ATM se presentaban como una solución idónea para toda una serie de nuevos servicios que recientemente se estaban asomando, como videoconferencias o vídeo bajo demanda, que necesariamente requerían de cierta QoS.

Paralelamente se intentaba adaptar la tecnología IP para poder ofrecer este tipo de servicios, pero todas aquellas adaptaciones no se encontraban todavía disponibles en su gran mayoría, mientras que los estándares ATM ya estaban probados con éxito en diferentes entornos.

Como existían gran cantidad de redes ATM, difícilmente podía IP sustituirla, por lo que lo más conveniente fue que se siguieran entrelazando y cubriendo sus carencias mutuas, creando una compleja fusión de protocolos estándares y dispositivos.

Proponemos entonces dar un vistazo a las tecnologías que precedieron integración de capa 2 y capa 3, a fin de poder desarrollar y justificar la solución “de capa intermedia” que propone MPLS. Estas tecnologías son:

- IP sobre ATM
- Conmutación IP

4.1.1 IP sobre ATM

A mediados de los años 90 internet generó un explosivo crecimiento, donde el Protocolo de Internet IP fue ganado terreno sobre otros protocolos de red que se encontraban en uso (IPX, appletalk, etc) Esto produjo un rápido déficit en el ancho de banda de los enlaces entre enrutadores, ya que estaban construidos por líneas dedicadas.

La congestión y saturación de las redes fue solucionado en primera instancia por el incremento de números de enlaces y su capacidad de transmisión. Del mismo modo luego se planteó la necesidad de aprovechar mejor los recursos de red, con los protocolos de encaminamiento del momento basados en métricas de número de saltos, los cuales no resultaron capaces de implementar tales necesidades.

Esto llevó a que necesitaran aumentar la capacidad de los enrutadores, tratando de combinar la eficacia y rentabilidad. A mediados de los 90 comenzaban su despliegue las redes ATM, que, por un lado proporcionaban mayores velocidades de transmisión y, además, los circuitos virtuales ATM posibilitaban las implementaciones de soluciones de ingeniería de tráfico.

El funcionamiento de IP sobre ATM brindó la superposición de la topología virtual IP sobre una topología real de conmutadores ATM. Cada conmutador se comunicaba con el resto de la red mediante Circuitos Virtuales Permanentes (PVC) Estos se establecen en función de intercambiar etiquetas entre cada conmutador de red, por lo tanto asociando etiquetas entre todos los elementos ATM, se determinan los PVC.

La figura 4.1 representa al modelo IP sobre ATM con la sepación de funciones en lo que respecta a enrutamiento IP de capa 3 (control y envío de paquetes) y lo que es conmutación de capa 2 (señalización y envío de celdas). Aunque se trata de la misma estructura física, en realidad son dos redes separadas, con diferentes funcionalidades y tecnologias.

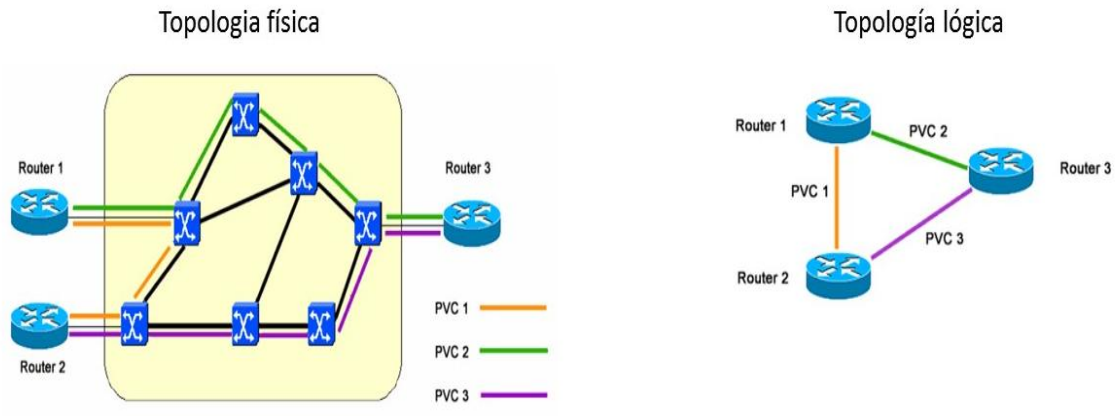


Figura 4.1.- IP sobre ATM

A continuación se detallará las ventajas y desventajas de montar una red IP sobre ATM.

Ventajas:

La mayor ventaja que presentó este modelo fue la disponibilidad de un ancho de banda a precio competitivo y la rapidez del transporte de datos que proporcionaban los conmutadores. Los caminos físicos de los PVCs se calculaban manualmente a través de la necesidad del tráfico IP. El punto de encuentro entre IP y ATM se realizaba en la información de enrutamiento que intercambiaban los enrutadores, acoplando los PVCs, ya que dicha información corresponde al protocolo interno IGP. Lo habitual no era más que entre enrutadores exista un PVC principal y otro de back up, en caso que fallara, el cambio era automático.

Desventajas:

La principal desventaja era gestionar dos redes diferentes, por un lado la infraestructura ATM y por el otro una red lógica IP superpuesta, lo que implicaba mayores costos. Además a esto se le incrementaba una cabecera del 20% que causaba el transporte de datagramas IP sobre las celdas ATM, lo cual provocaba una reducción proporcional del ancho de banda disponible. Por otro lado la red IP sobre ATM presentó problemas en su crecimiento exponencial, al incrementar la cantidad de nodos IP sobre una red superpuesta, dado por la formula n x (n-1). Es decir, si existía una red de cinco nodos externos, esta precisaba 5 x 4 =20 PVCs (uno en cada sentido de transmisión) al agregar un sexto nodo, se incrementaba en 10 los PVCs para mantener la misma estructura (6 x 5 =30)

4.1.2 Conmutación IP

Nació a partir de los requerimientos de mantener una convergencia entre el enrutamiento IP y la conmutación ATM. Dicha convergencia continúo hacia IP en todas las aplicaciones que surgieron. A esas técnicas se las denominaron conmutación IP (IP switching).

Una serie de tecnologías privadas como ser IP Switching de Ip Silon Network, Tag Switching de Cisco, Aggregate Route-base IP Switching de IBM, Cell Switching Route de Toshiba presentaban un problema, su interoperabilidad, ya que usaban distintas plataformas para la conmutación de capa 2 y el encaminamiento de capa 3. Esto llevó a la IETF a adoptar un estándar denominado MPLS.

Todas las técnicas de IP switching se basaban en dos funciones básicas comunes:

- La separación entre las funciones de control y de envío
- El intercambio de etiquetas para el envío de datos

Para el primer punto, los componentes de control utilizaban los protocolos estándares de encaminamiento como IS-IS,BGP, OSPF, etc, para el intercambio de información con otros routers y de esta manera construían y mantenían las tablas de enrutamiento. La componente de envío al llegar un paquete buscaba en su tabla de envío, mantenida por la componente de control, a fin de tomar la decisión de encaminamiento de cada paquete a través del hardware de conmutación.

El mecanismo de envío se implementó mediante el intercambio de etiquetas. (Similar a ATM) La diferencia radicaba en que lo que se enviaba por la interfaz física eran paquetes “etiquetados”. Estas etiquetas solo “marcaban” a un paquete, mediante una cabecera que identifica una clase equivalente de envío (FEC – Forwarding Equivalence Class). Una FEC consistía en un conjunto de paquetes que se enviaban por el mismo camino aun mientras sus destinos fueran diferentes. Una etiqueta solo tenía significado local y, por consiguiente, no modificaba la información de la cabecera original de los paquetes. Tan solo los encapsulaba, asignando el tráfico a los correspondientes FEC. (Figura 4.2)

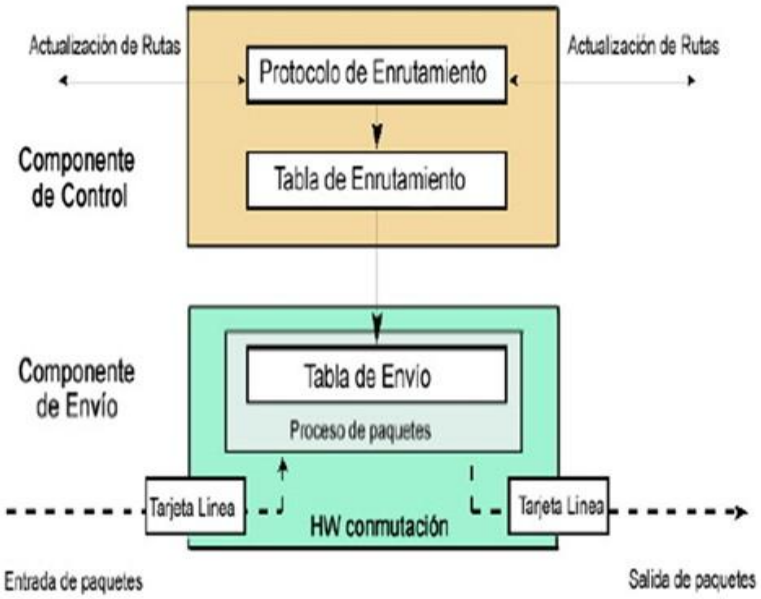


Figura 4.2.- Componente de Control y envío

El mecanismo de envío se implementó mediante el intercambio de etiquetas. (Similar a ATM) La diferencia radicaba en que lo que se enviaba por la interfaz física eran paquetes "etiquetados". Estas etiquetas solo "marcaban" a un paquete, mediante una cabecera que identifica una clase equivalente de envío (FEC – Forwarding Equivalence Class). Una FEC consistía en un conjunto de paquetes que se enviaban por el mismo camino aun mientras sus destinos fueran diferentes. Una etiqueta solo tenía significado local y, por consiguiente, no modificaba la información de la cabecera original de los paquetes. Tan solo los encapsulaba, asignando el tráfico a los correspondientes FEC. (Figura 4.3)

4.2 MPLS – Multiprotocol Label Switching

Los objetivos del IETF en la elaboración del estándar MPLS eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no solo ATM.
- MPLS debía soportar el envío de paquetes bajo demanda
- MPLS debía ser compatible con el Modelo de Servicios Integrados.
- MPLS debía permitir el crecimiento constante de internet
- MPLS debía ser compatible con los procedimientos de operación, mantenimiento, administración de las actuales rede IP.

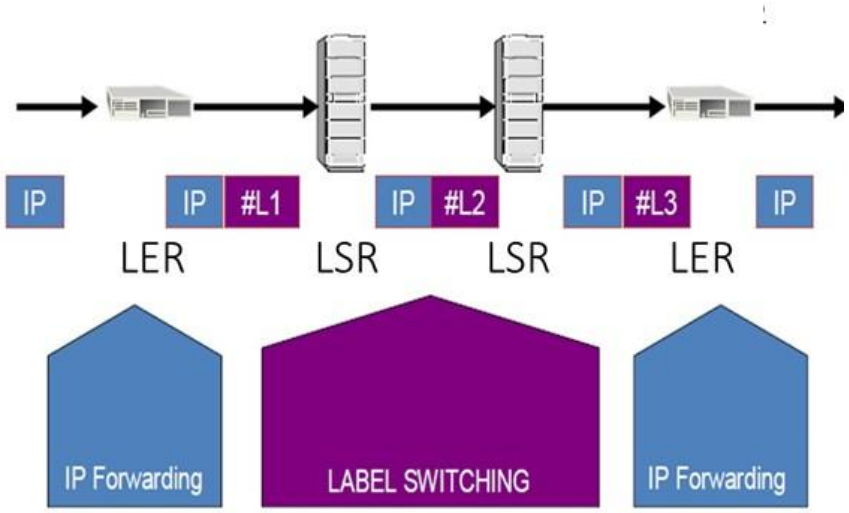


Figura 4.3 – Etiquetado en la frontera, intercambio en el medio

Antes de explicar el funcionamiento de una red MPLS deben ser aclarados varios conceptos básicos sobre esta tecnología, que además son adaptables a cualquier tecnología de conmutación.

Enrutamiento: son las acciones tomadas para transportar un paquete de datos en una red. Se realiza mediante protocolos de enrutamiento como RIP y OSPF que permiten saber cuál es la dirección del próximo salto para llegar al destino.

Conmutación: es la transferencia de datos desde un puerto de entrada a uno de salida de una maquina perteneciente a un red.

Conmutación de etiquetas: se lo llama al intercambio de etiquetas, combinado con mecanismos de control IP y un sistema de distribución de etiquetas.

La componente de control: crea y mantiene la tabla de envíos para el nodo en uso. Debe trabajar en conjunto con las componentes de control de otros nodos para distribuir la información de enrutamiento de manera consistente y segura. Además, es encargado de asegurar los procedimientos para crear las tablas de envíos locales.

La componente de envío: realiza los envíos de paquetes utilizando la tabla de envío.

Tabla de envío: (forwarding table) contiene la información para ejecutar la función de conmutación a la componente de envío.

Equivalencia de Clase de Envío (FEC – Forwarding Equivalence Class): Conjunto de paquetes que comparten los mismos atributos (dirección de destino, VPN, etc) y/o aquellos paquetes que requieren un mismo servicio (multicast, QoS), enviados sobre el mismo camino a través de una red, aun cuando los destinos finales sean distintos. Todos los paquetes que forman parte de FEC siguen el mismo LSP (Label Switched Path).

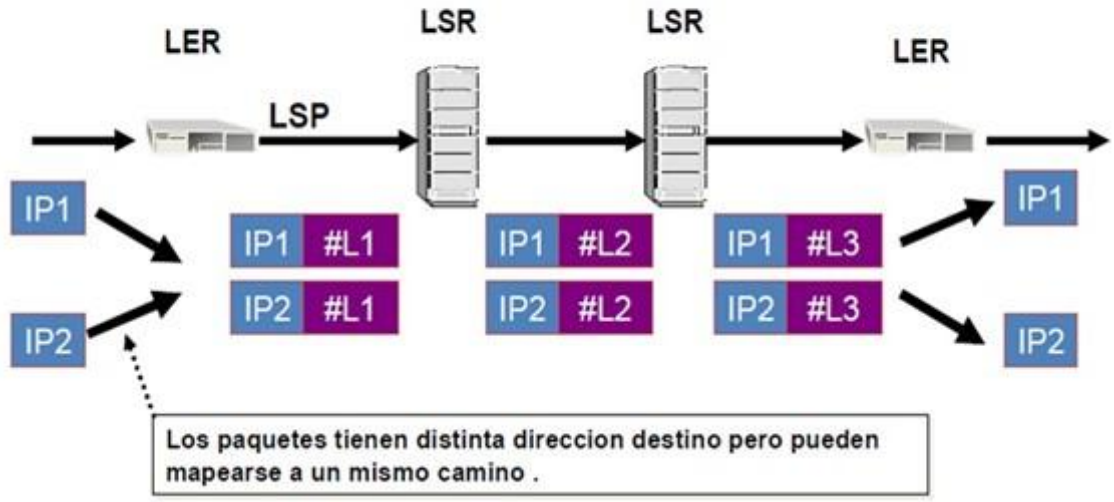


Figura 4.4.- Equivalencia de Clases de Envío

Etiqueta (Label): es un identificador corto asociadas a un FEC a través de un procesamiento de ordenamiento. Las etiquetas tienen solo significado local para cada uno de los enlaces de datos y no poseen carácter global como lo tiene una dirección IP. Además, un paquete puede tener varias etiquetas apiladas, que le dan jerarquía a los mismos al pasar de un dominio interior a otro.

Camino de Etiqueta Conmutada (LSP – Label Switched Path): es el camino por el cual ocurre la transmisión de datos. Son una secuencia de etiquetas entre los nodos dentro del dominio de MPLS, desde el origen hasta el final.

Dominio MPLS: porción de la red que entiende MPLS

Router de Etiqueta de Frontera (LER – Label Edge Router) son los Router que opera en los límites de acceso a la red MPLS, como también dentro del dominio MPLS. Utiliza la información de enrutamiento para asignar etiquetas a datagramas y entonces enviarlos al dominio MPLS luego de establecer los LSP utilizando el protocolo de señalización de

etiqueta (LSP – Label Signalling Protocol) su rol es asignar y remover etiquetas cuando el tráfico entra o sale del dominio MPLS respectivamente. También pueden ser denominados como Edge-LSR

Router de Etiqueta Conmutada (LSR – Label Switching Router): es un dispositivo de la red de alta velocidad que posee un componente de control IP y otro componente para el intercambio de etiquetas

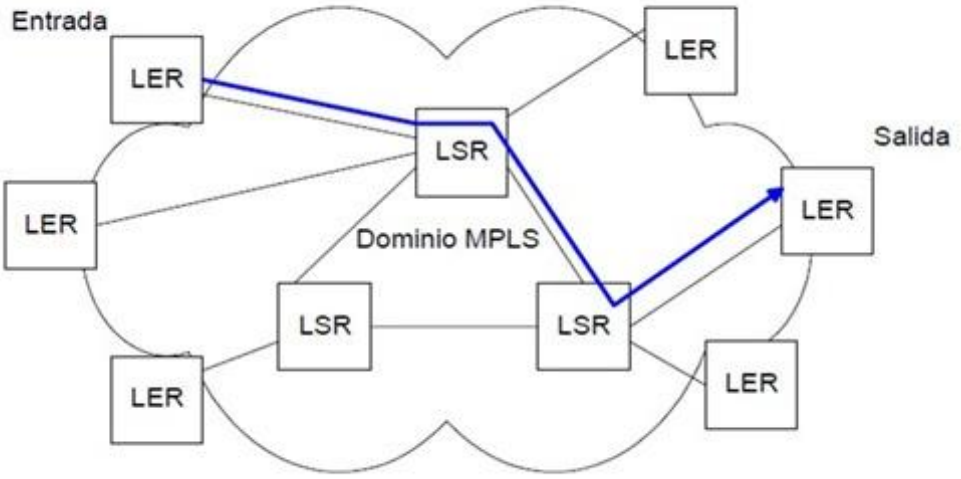


Figura 4.5 – Conceptos MPLS

4.3 Descripción de la red MPLS

La tecnología MPLS opera basada en la función de envío y control de paquetes. Básicamente, el funcionamiento del protocolo MPLS debe seguir los siguientes pasos.

- Creación de distribución de etiquetas
- Creación y actualización de listas de envíos
- Creación de LSPs
- Envío de paquetes
- Agregar etiquetas a los paquetes según la información de las tablas.

4.3.1 Funcionamiento del envío de paquetes en MPLS

MPLS se encuentra fundado en la asignación e intercambio de etiquetas, permitiendo en una red establecer un camino virtual o LSP. Estos LSPs son simplex por naturaleza, por lo tanto, si un enlace es dúplex se precisan dos LSPs. Los LSR (Label Switching Router) son enrutadores especializado en el envío de paquetes etiquetados.

Estas etiquetas son obtenidas de las tablas de envío, que son previamente creadas por la componente de control en base a la información recibida del enrutador vecino. Cada entrada de la tabla contiene un par de etiquetas de entrada/salida correspondiente a cada interfaz de entrada y salida, como se muestra figura 4.6

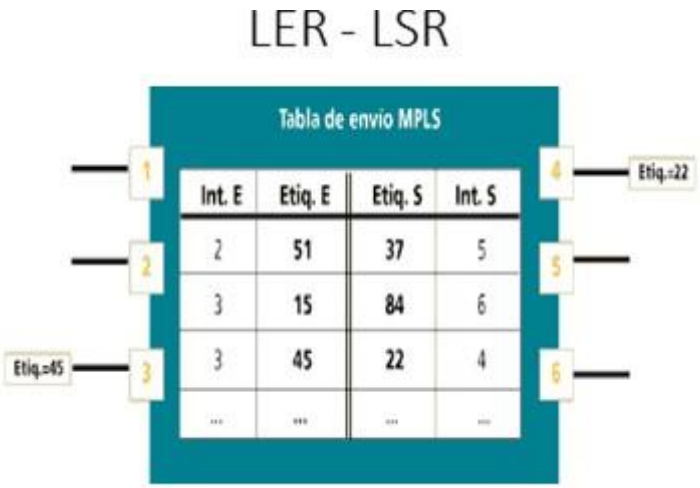


Figura 4.6.- Tabla de envío MPLS

En la figura 4.7 podemos ver que ingresa un paquete IP con una dirección de destino. El router frontera lo toma y consulta su tabla de enrutamiento, asignado al paquete la FEC definida por el grupo. Asimismo, este LER le asigna una etiqueta y envía el paquete al router siguiente (LSR) de la correspondiente LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP y solamente analizan la etiqueta de entrada, luego consultan la tabla de etiquetas y la reemplazan por una nueva de acuerdo al algoritmo de intercambio de etiquetas. Al llegar LER de cola (salida), este observa que el siguiente salto lo saca del dominio MPLS, por lo que quita la cabecera MPLS y envía el paquete utilizando el enrutamiento convencional.

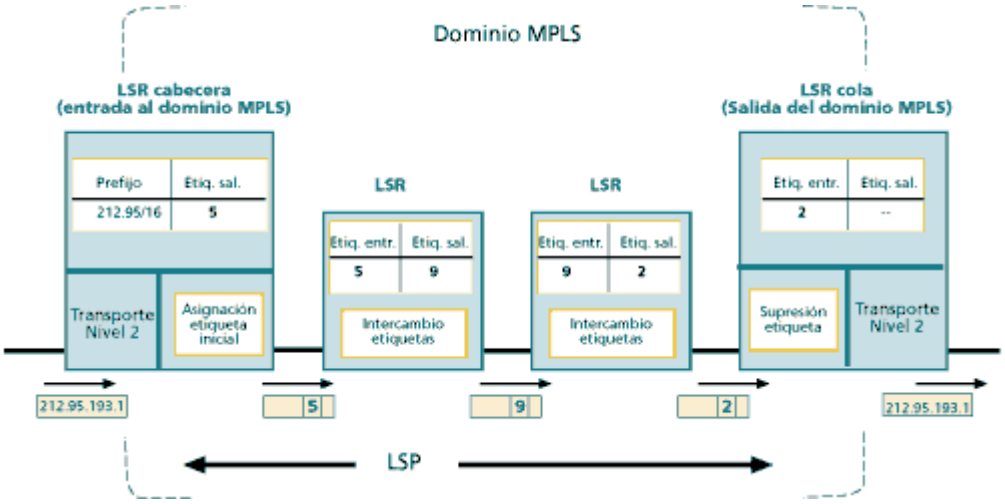


Figura 4.7.– Conceptos de MPLS

4.3.2 Control de paquetes en MPLS

Se desarrollará ahora dos puntos importantes, como son generadas las tablas de envío que establecen los LSP y como es distribuida la información de las etiquetas a los LSRs.

MPLS fue desarrollado con el fin de aprovechar la información proporcionada por los protocolos internos (RIP, OSPF, IS-IS, etc) logrando con esto establecer los caminos virtuales, es así como para cada ruta IP se va creando un “camino de etiquetas” vinculando de esta manera una entrada y una salida en cada tabla de un LSR.

La arquitectura MPLS no utiliza un único protocolo para la distribución de etiquetas entre nodos, sino que además emplea algunos protocolos con extensiones para soportar MPLS como el caso de RSVP y BGP, conocidas sus extensiones como MPLS-RSVP_TUNNELS y BGP-MPLS. Igualmente existen protocolos específicos para la distribución de etiquetas, como lo es el LDP (Label Distribution Protocol) y CR-LDP (Constraint Based Routing Label).

En forma genérica, cada protocolo se caracteriza por:

- LDP: mapea los destino IP en etiquetas
- RSVP y CR-LDP: usado para ingeniería de tráfico y reserva de recursos.
- BGP: para etiquetas externas (VPN)

4.4 Funcionamiento global de MPLS

Mediante la figura 4.8 se puede ver el sistema global del funcionamiento MPLS. La red proporciona una arquitectura de transporte donde a cada enrutadores de frontera es presentado como un único salto, como si fuera toda una única malla, unida directamente o por los PVCs de ATM. Esta unión a un solo salto se realiza mediante los correspondientes LSPs.

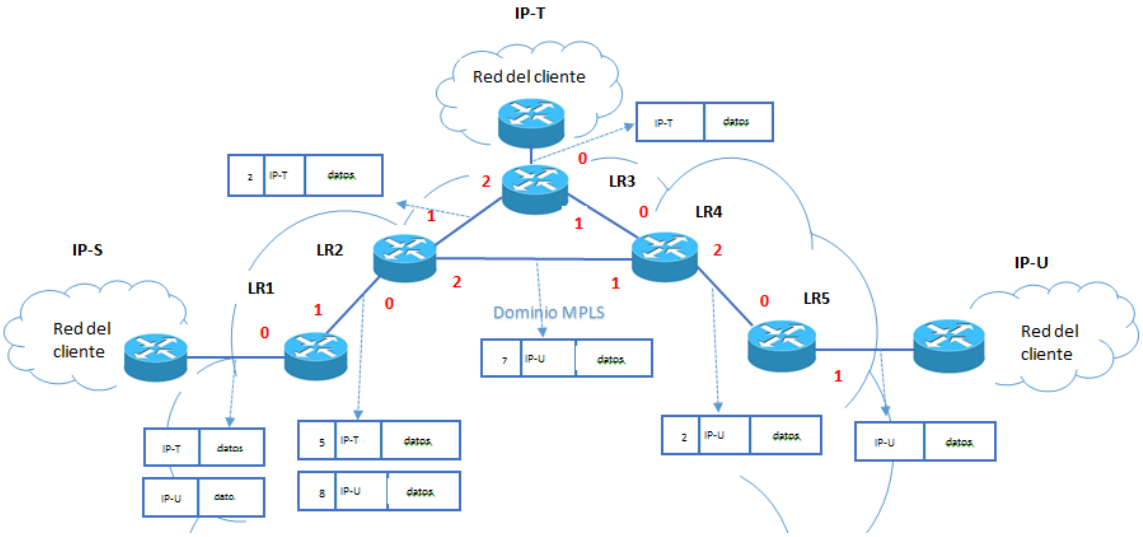


Figura 4.8.- funcionamiento global de la red MPLS

El primer paso *es* crear las tablas de enrutamiento de manera automática. Para ello son utilizados los protocolos de pasarela internos como OSPF, IS-IS, RIP, etc. Con esta información, el protocolo LDP (protocolo de distribución de etiquetas) utiliza estas tablas para determinar los valores de las etiquetas de los dispositivos adyacentes estableciendo los LSPs. Las etiquetas son asignadas de manera automática, contrariamente como lo hace ATM con los circuitos virtuales permanentes (PVC) que requieren una asignación manual VPI/VCI (Identificador de Camino/Circuito Virtual). Una vez un que ingresa un paquete por el Edge-LSR o LER al dominio MPLS, este procede a determinar cuáles servicios son requeridos (por ejemplo QoS o manejo de ancho de banda, etc). Luego selecciona y asigna una etiqueta a la cabecera del paquete y es entregado al backbone.

Una vez realizados estos pasos, el LSR se encarga de leer la etiqueta del paquete y cambiarla por una nueva de su propia tabla de enrutamiento, permitiendo a su vez separar los diferentes tipos de tráfico, como tráfico de mejor esfuerzo o tráfico de camino crítico. Al ser las etiquetas de MPLS de uso local se hace imposible el agotamiento de estas, además

de hacerlo una solución escalable. Esta característica es esencial para implementar servicios avanzados de IP tales como: QoS, VPNs, ingeniería de tráfico (TI).

Figura 4.9.- Funcionamiento de la red MPLS

En la figura 4.9 se presenta un ejemplo para examinar la manera en que los paquetes son enviados a través de la red MPLS, y conjuntamente con la figura 4.10 se muestran las tablas de envío de cada LSR involucrado. *Por último,* LER de salida elimina la etiqueta, lee la cabecera IP del paquete y se encarga de enviar el paquete al destino final.

4.5 Cabecera MPLS

La cabecera MPLS se compone de 32 bits de longitud, distribuidos en cuatro campos, cada uno con diferentes funciones como se muestra en la figura 4.10:

- Valor Etiqueta: este campo lleva el valor de la etiqueta de MPLS. Tiene una longitud de 20 bit, por lo que puede dar un total de 2^{20} = 1.048.576 valores. Aunque en realidad los primero 16 valores se encuentran reservados. Como fue mencionado anteriormente, al ser etiquetas de uso interno (dentro de la Red MPLS) es nula la probabilidad de que estas se agoten.

- Campo Stack (S): Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

- Campo TTL (Time To Live): al igual que el protocolo IP, este campo sirve como un contador de saltos a fin de evitar bucles o loops que se puedan generar. Al llegar a cero en algún LSR, el paquete es automáticamente descartado

tabla LR1				
etiqueta entrada	interface entrada	IP destino	interface salida	etiqueta salida
NA	0	IP T	1	5
NA	0	IP U	1	8

tabla LR2				
etiqueta entrada	interface entrada	IP destino	interface salida	etiqueta salida
5	0	IP T	1	2
8	0	IP U	2	7

tabla LR3				
etiqueta entrada	interface entrada	IP destino	interface salida	etiqueta salida
2	2	IP T	0	NA

tabla LR4				
etiqueta entrada	interface entrada	IP destino	interface salida	etiqueta salida
7	1	IP U	2	9

tabla LR5				
etiqueta entrada	interface entrada	IP destino	interface salida	etiqueta salida
9	0	IP U	1	NA

Figura 4.10.- tabla etiquetas e interfaces

- Campo EXP: conocido como campo de QoS, consta de 3 bit lo que propone un total de 2^3 = 8 distintos tipos de posibles valores de tráfico. La idea es minimizar el retardo en ciertos paquetes que son muy sensibles a él (como el caso de voz sobre IP) y penalizar con un poco de retardo el tráfico menos sensible (web HTTP).

Como se puede notar, ningún campo es útil para determinar el próximo salto, salvo el valor del campo de etiqueta, pero todos ellos son indispensables a la hora de ser tratados en el paso de LSR.

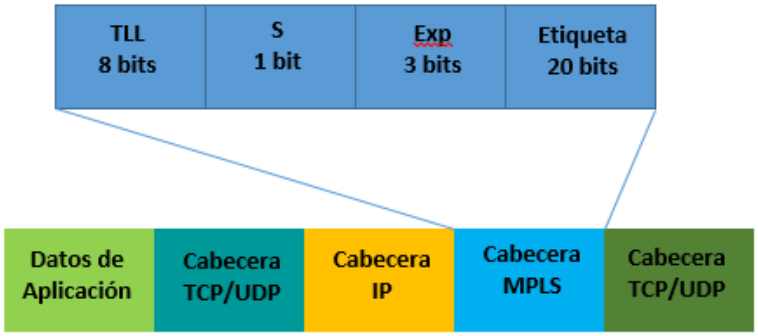


Figura 4.11.- Cabecera MPLS

La decisión de asignación de etiquetas pueden ser basadas en los siguientes criterios de envió:

- Enrutamiento de destino unicast
- Ingeniería de trafico
- Multicast
- Red Virtual Privada (VPN)
- QoS

4.6 Método de distribución de etiquetas

Es importante conocer la forma en que es llevada a cabo la distribución de etiquetas hacia los LSR y que protocolos son utilizados para tal fin. Un router MPLS debe conocer las "reglas" para poder asignar o intercambiar etiquetas. Si bien los router convencionales suelen ser programados para determinar que harán con un determinado paquete; MPLS cuenta con una "asignación dinámica" de reglas, permitiendo mayor flexibilidad. Existen entonces dos alternativas diferentes:

La primera de ellas es la manera independiente: es cuando cada router ha "escuchado" estas reglas, creando su propia tabla de envió y distribuyendo esta información a otros routers. Mediante esto es posible determinar que no existe en la red un administrador de etiquetas centralizado.

El segundo métodos de distribución de etiquetas se denominado control ordenado: el LER de salida es el encargado de distribuir las etiquetas, siendo este proceso en sentido contrario al envío de paquetes. El control ordenado ofrece ventajas de mejor ingeniería de tráfico y mejor control de la red. Sin embrago, puede presentar mayores tiempos de convergencias, convirtiendo al LER de salida en el único punto susceptible a fallas.

A su vez, el método de control ordenado puede ser dividido en dos:

- Transferencia de bajada no solicitada
- Transferencia de bajada solicitada

La diferencia está en que el primer caso, ya sea un tiempo determinado o cuando cambie la base de información de etiquetas es cuando un LSR de salida distribuye la información para actualizar tablas de envió. Mientras en que el segundo caso se da si un LSR en particular solicita una actualización.

Los protocolos utilizados para la distribución de etiquetas ya han sido mencionados en el punto 4.4 de este capítulo.

4.7 Aplicaciones de MPLS

Las aplicaciones que MPLS tiene hoy en día son:

- Ingeniería de trafico
- Diferenciación de niveles de servicio mediante clases (QoS)
- Servicio de Redes Virtuales Privadas

4.7.1 Ingeniería de tráfico (TE)

La ingeniería de tráfico es encargada de procurar la optimización de la performance de la red operativa. Implica la aplicación de la tecnología y la aplicación de los principios científicos a la medición, caracterización, modelado y control del tráfico que circula por la red.

Su principal ventaja es que ayuda a identificar y estructurar las metas y prioridades en términos de mejorar la calidad del servicio brindado a los usuarios finales. También el concepto de TE ayuda a la medición y análisis del cumplimiento de estas metas.

La TE se dividió en dos ramas:

- TE Orientada a tráfico: su prioridad se centró en lo que refiere al transporte de datos; minimizando perdidas de paquetes, el retardo de cada uno de ellos y obteniendo acuerdos de niveles para brindar calidad de servicio.
- TE Orientada a recursos: su objetivo es la optimización de los recursos de red y el ancho de banda. Busca no saturar partes de la red mientras que otras permanecen subutilizadas.

Igualmente ambas ramas convergen en un único objetivo, minimizar la congestión. En resumen la TE provee por ende, capacidades para realizar lo siguiente:

- Mapear caminos primarios alrededor de cuellos de botellas conocidos.
- Lograr el uso eficiente del ancho de banda.
- Maximizar la eficacia operacional
- Mejorar las características de la performance del tráfico orientado de la red, minimizando perdidas de paquetes y periodos prolongados de congestión.
- Mejorar los límites de las estadísticas de la performance de la red (tasa de perdida, variación del delay, delay de transferencia)
- Proveer un control preciso sobre como el tráfico es enrutado.

A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran rudimentarios. Los flujos de tráfico siguen el camino a destino más corto, que es calculado por el algoritmo que presentan los Protocolos de Gateway Interior (IGP). En caso de congestión de algún enlace el problema se resolvía en añadir más capacidad a los enlaces. Lo que propone la ingeniería de tráfico es la desviación de tráfico de los enlaces más congestionados a los enlaces más ociosos, aunque estos estén lejos del camino más corto. En la figura 3.11 se compara las dos rutas para el mismo par de nodos origen y destino.

MPLS es una herramienta efectiva para ser aplicada en grades redes, ya que:

- El administrador de red puede establecer rutas específicas por LSRs concretos, especificando el camino exacto de un LSP.

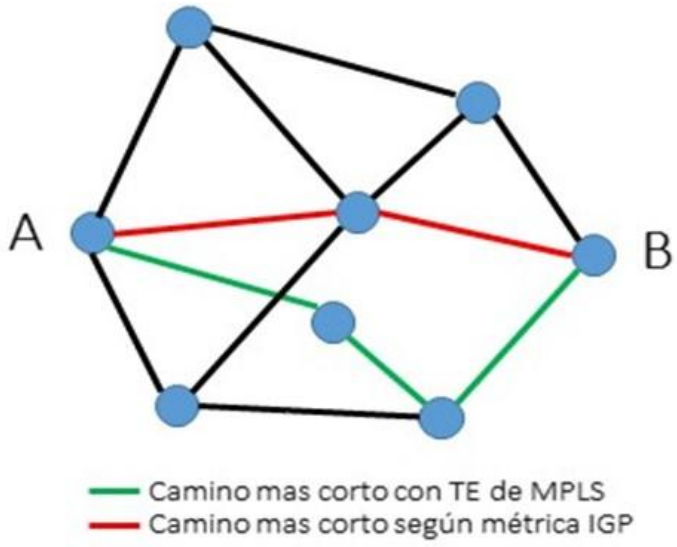


Figura 4.12.- Caminos más cortos según tecnologías diferentes

- Permite obtener estadísticas de uso por cada LSP en detalle. Es decir, cuanto trafico cursa y de qué tipo. Esto puede ser útil, al permitir re planificar la red de forma de ofrecer un uso más eficiente de los recursos.
- Permite hacer encaminamiento restringido, seleccionando rutas específicas para tráfico con requerimientos específicos.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, ofreciendo una mayor calidad de servicio a los clientes.

4.7.2 Calidad de servicio (QoS)

Es llamada QoS al grado de satisfacción de un usuario sobre los servicios de prestaciones o aplicaciones contratados por una o varias identidades.

Como se mencionó anteriormente, con el crecimiento de internet fue necesario comenzar a desarrollar Ingeniería de Red, por los tanto los enlaces existentes debían ser mejorados y crecidos en capacidad para adecuarse a la nueva demanda.

Se comenzó aplicar Ingeniería de Tráfico con el fin de optimizar la red. Las nuevas aplicaciones necesitaron retardo y ancho de banda asegurado, jitter mínimo, una probabilidad de perdida determinada, entre otras cosas. Para lograrlo fue necesario de

diferentes arquitecturas capaces de proporcionar una calidad de servicio como las propuestas con MPLS.

Para aplicar QoS se debe poder gestionarlo correctamente y para eso son utilizadas VLANs, separando los distintos tipos de tráfico brindándoles diferentes niveles de prioridad.

Las ventajas de utilizar QoS son:

- Buena planificación de la red.
- Poder gestionar los flujos de datos.
- Garantizar el ancho de banda suficiente para las aplicaciones críticas.

Mientras que la desventaja de usar QoS:

- Complicaciones en la gestión y el diseño de la red.

Para determinar los parámetros de calidad primero y principal, se debe conocer a que servicio pertenece el flujo de datos ya que estos afectan de diferentes maneras.

Existen diferentes factores en las redes IP que determinan su comportamiento en cuanto a la calidad de servicio ofrecida.

Son descriptos brevemente algunos de ellos:

- *Retardo de transferencia de paquetes IP* (IPTD): corresponde al retardo de transmisión de un paquete IP. Es el tiempo (t_2-t_1) que transcurre entre dos eventos de del paquetes IP de referencia.

- *Retardo Medio de la Transferencia de los paquetes IP*: es el resultado de la media aritmética teniendo en cuenta todos los retardos que puede sufrir un paquete en la red lo que proporciona una idea del rendimiento de la misma.

- *Varianza del retardo de paquetes de información* (IPDV): Hace referencia al jitter o la variación del retardo, el mismo es aleatorio, por lo tanto es un dato importante en el caso del tráfico sensible al retardo.

- *Tasa de error de los paquetes IP* (IPER): Corresponde a la cantidad de paquetes que fueron descartados del total trasmitido, ya sea por congestión de los nodos,

porque el tiempo de vida del mismo haya expirado, por la falla de algún nodo en la trasmisión, etc

$$IPER = 1 - (1 - BER)^{\text{Tamaño de paquetes x 8}}$$

Donde,

BER: corresponde a la tasa de errores de bits, una vez que haya sido aplicado el esquema de corrección de errores en recepción (FEC)

La IPER para un sistema que cumpla la recomendación UIT-R puede llegar a tolerar hasta 1×10^{-2}

- *Tasa de paquete IP expurios* (SPR): es el índice de cuantificación de paquetes falsos al egreso, durante un determinado período de tiempo que son generados por errores en la capa física o nodos intermedios.

- *Porcentaje de indisponibilidad del servicio IP* (IPU): índice de tiempo indisponible en base al total del servicio programado.

4.7.2.1 Requerimientos para aplicaciones

La *ITU-T* definió los requerimientos de tráfico y nivel de servicio que los clientes deben percibir para seis clases de servicio. Estos parámetros fueron diseñados para conexiones del tipo *E1* 2.048 Mbps.

Tanto la tecnología de capa de enlace como la del medio de trasmisión serán provistas por el ISP (Proveedor de Servicio de Internet). La clase es independiente de la tecnología de acceso al medio que se disponga en la red ISP.

A continuación mediante la tabla 4.2 se detallan los requerimientos de calidad para cada Clase y aplicaciones en las que se utiliza:

Parámetros de Rendimiento	**Clases de Calidad de Servicio**					
	Clase 0	Clase 1	Clase 2	Clase 3	Clase 4	Clase 5
IPTD	100 ms	400 ms	100 ms	400 ms	1000 ms	-
IPDV	50 ms	50 ms	-	-	-	-
IPLR	$1E^{-03}$	$1E^{-03}$	$1E^{-03}$	$1E^{-03}$	$1E^{-03}$	-
IPER	$1E^{-04}$					-
Aplicaciones	En tiempo real, sensible al retardo y jitter (VoIP, VTC)	En tiempo real, sensible al retardo y jitter (VoIP, VTC ambos con menor calidad e interacción)	Transacción de datos de alta interacción a pesar de no ser en tiempo real	Datos de transacciones con parámetros menos rígidos	Para datos de baja perdida (señalización, transacción de corta duración, video continuo, videostreaming)	Aplicaciones tradicionales de las redes IP como ser email, FTP, HTTP, etc

Figura 4.13.- Requerimiento de calidad

Además hay dos clases que se encuentran bajo estudio, diseñadas para soportar aplicaciones de alto flujo.

Clase 6 de Emulación de circuitos TDM con alta interacción. Se requiere como retardo máximo 100 ms y una variación de retardo de 50 ms; una tasa de pérdida menor IPLR de 10^{-6}. En este grupo se incluye un parámetro de *Radio de Reordenamiento* IPRR (Packet Reordering Ratio), campo que se aplica en datagramas TCP para el reordenamiento en destino. Esta clase se aplica a Televisión de Alta Calidad en Internet, Transferencias TCP de alta capacidad y emulaciones TDM.

Clase 7 de Emulación de Circuitos TDM. Requiere como máximo un retardo promedio de 400 ms y una variación de retardo de 50 ms. La tasa de perdida IPLR no debe superar los 10^{-5} y una tasa de error IPER inferior a 10^{-6}. Este grupo también cuanta con el parámetro de *Radio de Reordenamiento* IPRR. Solo se diferencia de la anterior en que se aplica para emulaciones TDM con una interacción y sensibilidad mayor que la clase anterior.

4.7.2.2 Arquitectura de QoS sobre IP

Existen tres arquitecturas de QoS sobre IP. Ellas son

- Arquitectura Int-Serv
- Arquitectura Diff-Serv
- Arquitectura mixta

4.7.2.2.1 Arquitectura INT-SERV

En esta arquitectura el concepto de flujo juega un papel importante y está definido como un tráfico continuo de datagramas. Un flujo es unidireccional y es la unidad más pequeña a la que se le puede aplicar QoS y pueden ser agrupados en clases como fue mencionado anteriormente.

Para esta arquitectura son definidos tres tipos de servicios:

- Servicio Garantizado (Guaranteed Rate Service): Garantiza un caudal mínimo y un retardo máximo. Se comporta como un Circuito Virtual, es decir que los recursos se encuentran dedicados al cliente.
- Servicio de Carga Controlada (Controled Load Service): Los recursos son solicitados a la red y si esta los posee los asigna de manera dinámica cada vez que los necesita. Debe proporcionar un buen tiempo de respuesta, pero sin garantía estricta. Pueden producirse eventualmente retardos.

Esta arquitectura, dispone del protocolo RSVP (Protocolo de Reservación de Recursos) para señalizar y reservar la QoS necesaria para cada flujo de datos antes de que las aplicaciones comiencen a operar hasta que esta lleguen a su fin, o hasta que el ancho de banda requerido sobrepase el límite reservado para la aplicación.

Al no ser RSVP un protocolo de encaminamiento, se ha pensado para que trabaje conjuntamente con estos. Los protocolos de encaminamiento que determinan por donde se reenviarán los paquetes, mientras que RSVP se preocupa por mantener la calidad durante el reenvío.

Este protocolo es orientado a conexión, ya que los routers involucrados deben guardar una cierta información de estado de cada flujo para el cual realizan la reserva. Por ejemplo para realizar una sesión de videoconferencia se utiliza este mecanismo, siempre y cuando la red IP involucrada soporte esta aplicación y garantice un determinado ancho de banda.

Los routers deben contar con cuatro elementos, *Control de Admisión,* mediante este elemento comprueba que la red cumpla con los requisitos para la petición; *Política de Control,* determina si el usuario tiene permisos para la petición realizada. Si una de estas dos condiciones no se cumplen, se envía un notificación de *Error* a quien ha realizado la reserva. Pero, si se cumplen ambas (Control de Admisión y la Política de Control), entonces se procede al *Clasificador de Paquetes, quien cumple con* analizar los campos de dirección y puerto para determinar a qué clase pertenece; como último elemento se encuentra el *Planificador de Paquetes, quien debe* aplicar un algoritmo para gestionar la trasmisión de los paquetes por un enlace de salida.

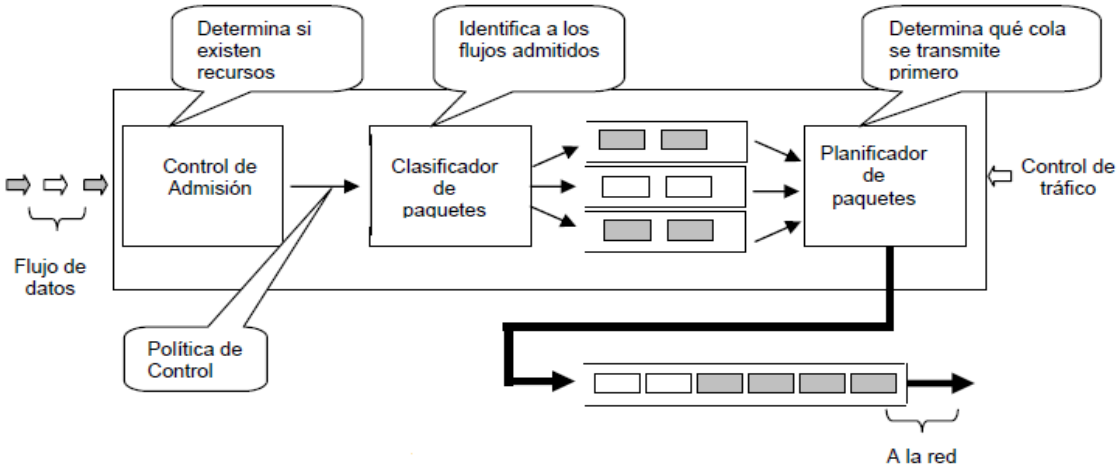


Figura 4.14.- Arquitectura INT-SERV

Funcionamiento del protocolo RSVP:

Este protocolo utiliza varios mensajes para concretar la reserva de recursos, los más importantes son *Path* y *Resv*.

El emisor se encarga de enviar un mensaje *Path* al destino, para marcar la ruta entre este y el receptor, además de la viabilidad de la solicitud para este trayecto. Cada router guarda la dirección IP origen de donde reciben este mensaje para luego reconstruir el camino de regreso. Un mensaje Path incluye:

Mensaje PATH	Descripción
Phop	Dirección del último nodo RSVP
Sender Template	Dirección IP del emisor y opcionalmente puerto
Sender Tspec	Define las características del tráfico
Adspec	Opcional (información actualizada por cada router)

Figura 4.14.- Estructura del campo Path

Con la llegada de este mensaje el receptor puede medir el tipo de servicio que es capaz de soportar la red. En cambio sí un error es detectado por el receptor, este, debe enviar un mensaje PathErr informando al emisor que no es posible ninguna acción.

En cambio, sí es correcto, el router debe:

- Actualizar la dirección del emisor en Sender Template. Si la ruta no existe, la crea.
- Actualizar los contadores de limpieza de ruta a su valor inicial.

Una vez que las condiciones están dadas, el receptor procede a reservar los recursos enviando un mensaje *Resv* con las especificaciones de tráfico recibidas del emisor, o sea, las especificaciones requeridas por el receptor (tipo de servicio solicitado y un filtro que selecciona los paquetes con determinadas características)

Cuando el router recibe un mensaje *Resv*, este puede aceptar o no la reserva. Si es aceptada, el realiza la reserva y el mensaje *Resv* continua al siguiente router en la dirección del emisor. En el caso negativo, es enviando un mensaje de error al receptor (*ResvErr*).

Mensaje RESV	Descripción
Estilo de Reserva	Tipo de Reserva a utilizar
FilterSpec	Especificaciones de Filtro
FlowSpec	Rspec y especificación de tráfico Tspec
ResvConf	Opcional (envía un objeto de confirmación con la dirección IP del Receptor)

Figura 4.15.- Estructura del campo RESV

Esta propuesta de arquitectura si bien ofrece QoS, resulta compleja, ya qué debe cada uno de los routers almacenar la información del estado de flujo de datos, congestionando cada uno de los puntos de la red y haciéndolas redes bastante costosas a diferencia de la arquitectura Diff-Serv que se explica a continuación.

4.7.2.2.2 Arquitectura DIFF-SERV

Formada por diferentes tecnologías por medio de la cual los proveedores pueden ofrecer diferentes niveles de QoS para varios clientes o tráficos de información. Se encuentra basada en la división del tráfico por clases y la asignación de prioridad a cada paquete. A diferencia de Int-Serv, esta arquitectura no necesita que se encuentre implementada sobre todos los nodos, lo que brinda una mayor estabilidad, al ser la información sobre calidad de servicio escrita sobre los datagramas y no en los routers.

La primera tarea del grupo de DiffServ fue re-especificar el byte conocido como el campo de los Servicios Diferenciados y es marcado con un patrón específico de bits llamado código DS, usado para indicar cómo cada router debe tratar al paquete. Para enfatizar el hecho de que ninguna información de sesión se necesita guardar, este tratamiento es conocido como Per-Hop Behavior (PHB).

El campo DS se estructura de la siguiente forma:

Subcampo	Longitud (bits)
DSCP (Differentiated Servcies CodePoint)	6
ECN (Explicit Congestion Notification)	2

Figura 4.16.- Estructura del campo 'Differentiated Services'

El subcampo ECN notifica las situaciones de congestión y el subcampo DSCP permite definir en principio hasta 2^6 = 64 posibles categorías de tráfico. Los valores de DSCP se dividen en los tres grupos:

CodePoint	Posibles Valores	Uso
XXXXX0	32	Estandar
XXXX11	16	Local / Experimental
XXXX01	16	Reservado

Figura 4.17.- Códigos posibles para el campo DS

En DiffServ se definen tres tipos de servicio, que son los siguientes:

- Encaminamiento Expeditivo, su función es proveer las herramientas para proporcionar un servicio de extremo a extremo con baja pérdida, bajo retardo, bajo jitter y un ancho de banda asegurado.

  Cuando un paquete se aproxima antes de su tiempo programado de llegada, los nodos de acceso e internos, pueden tratar el paquete de la siguiente forma, los nodos de acceso por lo general reenvían el paquete en el próximo tiempo configurado o; descartan el paquete evitando el ensanchamiento de ancho de

banda del que se tiene configurado. En cambio los nodos internos reenvían el paquete en forma inmediata para evitar un retardo acumulado.

Al ser necesario un control de la tasa de trasmisión, el servicio que ofrece es similar a una línea dedicada con bajos retardos y baja variación en el ancho de banda.

- Encaminamiento Asegurado: Define cuatro clases a las cuales se les tiene que asignar espacio en el buffer y un ancho de banda independiente en cada nodo. Cada clase cuenta con tres niveles, Baja, Media y Alta probabilidad de descarte.

- Comportamiento por Omisión; todo paquete que no tenga una especificación de comportamiento que deben llevar utilizando el servicio del mejor esfuerzo. En este servicio no se ofrece ningún tipo de garantías.

El campo DS es una incorporación reciente en la cabecera IP. Anteriormente existía en su lugar un campo denominado TOS o 'Tipo de Servicio' que tenía la siguiente estructura, donde:

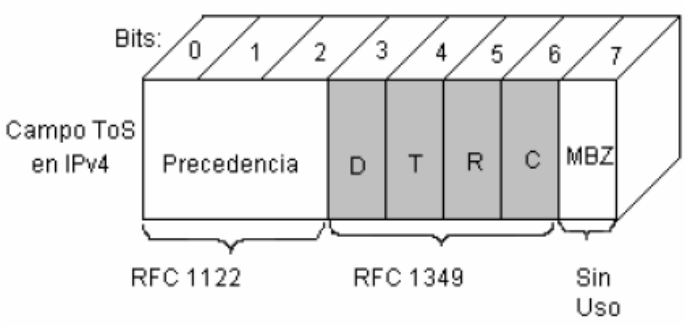


Figura 4.18.- Campos de ToS para IPv4

- Campo Precedencia: Permitía especificar una prioridad de 0 a 7 para el datagrama, donde todos sus bits en 1 indicaban máxima prioridad.
- Campo Tipo de Servicio (ToS): Se compone de 8 bits y utiliza los bits D, T, R y C para especificar el tipo de transporte para el datagrama.
    - bit D se utiliza para solicitar mínimo retardo,
    - bit T determina un máximo desempeño,
    - bit R es para solicitar una máxima confiabilidad y por último,
    - bit C es implementado para solicitar un bajo costo

Especificación de los tipos de Nodo Diff-Serv:

Existen dos tipos de Nodos:

- Nodos externos DS
  Los nodos externos son los encargados de acondicionar el tráfico y clasificar los paquetes. Para la clasificación se basan en la dirección IP con sus puertos (origen y destino), protocolo de transporte y DSCP. A este clasificador se lo conoce como MF (clasificador Multi Campo).
  Los nodos de salida deberán acondicionar el tráfico trasferido hacia otros dominios DS conectados.
- Nodos internos DS
  Los nodos internos se conectan a nodos externos o internos de su propio dominio.

Vemos que Diff-Serv trata a cada uno de los paquetes enviados a la red en forma independiente y no necesita asignar estados ni establecer procesos de señalización, es por ello que ofrece mayor escalabilidad que Int-Serv.

Elementos que componen una red Diff-Serv

Diff- Serv, se compone de los elementos que son detallados a continuación:

- *Clasificador*: Su función es guiar los paquetes hacia el mismo procedimiento de condicionamiento de tráfico que contengan similares características.
- *Medidor*: Son los encargados de informar a las funciones de acondicionamiento para que determinen una acción para cada paquete que se encuentre dentro o fuera de un determinado perfil de tráfico.
- *Marcador*: Configurado para marcar los paquetes en base a un conjunto de códigos DS para luego seleccionar el PBH más adecuado.
- *Acondicionador*: Posé un tamaño de cola finito, con el fin de descartar paquetes cuando la cola se encuentre llena para así poder mantener el retardo de los paquetes bajo.
- *Descartador*: Encargado de descartar paquetes con el fin de evitar el congestionamiento y poder cumplir con los requisitos de perfil de tráfico.

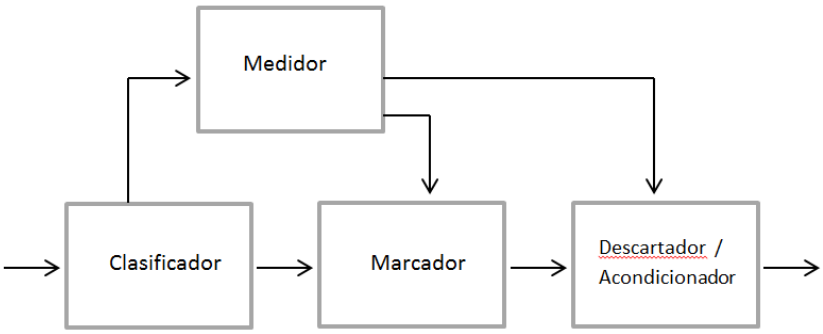


Figura 4.19.- Componentes de red Diff-Serv

La ventajas de este modelo son en primer lugar la Escalabilidad porque mantiene informado el estado de muchos circuitos virtuales; como segundo lugar el Funcionamiento, ya que el contenido de los paquetes es revisado una sola vez para ser clasificado y todas las decisiones de QoS se toman en base a un campo fijo de la cabecera, reduciendo el procesamiento y por último el sistema posee un Costo de gestión reducido.

Como desventaja existen la No Reserva de Ancho de Banda, por lo que la garantía de servicios puede ser imparcial en los nodos y la ausencia de Control de Admisión, que hace que las aplicaciones se congestionen unas con otras.

4.7.2.2.3 Combinación de INT-SERV con DIFF-SERV

Como ya se ha analizado, el modelo Int-Serv es mucho más complejo lo cual puede no ser lo más óptimo para los routers internos de la red IP, por ello estos utilizan Diff-Serv.

Mediante el modelo Int-Serv se trata la QoS a través de flujos. Una vez que el flujo haya pasado por el control de admisión, es sometido a recibir una clasificación de servicio proporcionando un ancho de banda y límite de retardo punto a punto. Como consecuencia del manejo de flujo y señalización, se presentan los problemas en cuanto a la escalabilidad en Int-Serv. Es aquí donde aparece la arquitectura Diff-Serv que utiliza la Marcación de paquetes de acuerdo a un PHB (Comportamiento por Saltos)

No hay que olvidar los dispositivos Interworking llamados ED (Dispositivos Externos) que juegan un papel importante en la red, cumpliendo el papel de router de frontera.

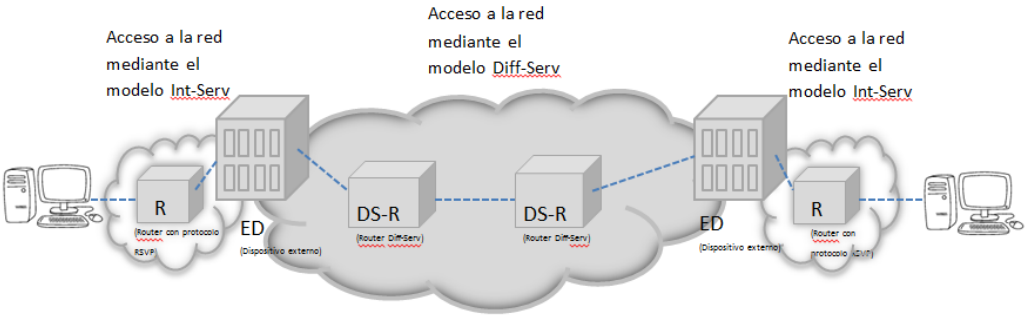


Figura 4.20.- Red de arquitectura mixta

4.7.3 Redes Virtuales Privadas - VPN

Las VPNs son la base de las compañías para crear y administrar servicios de valor agregado como servicios de telefonía y trasmisión de datos. Se construyen basándose en conexiones realizadas sobre una infraestructura compartida.

Funcionamiento:

Cada sitio cliente se conecta a la red del proveedor de servicios (SP) a través de una interfaz utilizando una tabla de enrutamiento virtual y renvío VPN (VRF) en el router frontera del proveedor (PE). Esta última permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar simultáneamente. VRF actúa como un router lógico, utilizando solo una tabla de enrutamiento; además requiere de una tabla de renvío donde indicar el siguiente salto para cada paquete de datos y las normas y protocoles de enrutamiento a utilizar.

El dispositivo de router frontera de cliente (CE), que solicitó el servicio, conecta directamente al router frontera del proveedor (PE). Después de que ambos establecieron la adyacencia, el CE informa las rutas locales del sitio VPN y se encargó de asimilar las rutas remotas del PE, este intercambio es realizado mediante enrutamiento estático o utilizando protocolos de enrutamiento como RIP, OSPF, EIGRP o EBGP.

Figura 4.21.- VPN

Cada router frontera de proveedor (PE) procede a mantener una VRF para cada sitio al que se encuentra conectado. Además se debe tener en cuenta los enrutadores internos del proveedor (P) que actúan como LSR de MPLS, enviando e intercambiando etiquetas. Estos últimos son indiferentes a las VPNs.

Se necesita de dos flujos de control para poder establecer una VPN:

- El primero es el intercambio de información de enrutamiento entre sitios remotos, que se realiza a través del protocolo gateway de frontera (BGP)
- El segundo flujo es el establecimiento de las rutas conmutadas por etiquetas (LSR) a través del protocolo de distribución de etiquetas (LDP).

Una vez realizado estos flujos de control, es posible el intercambio de datos entre sitios remotos.

Cabe destacar que los métodos utilizados para el intercambio de información pueden ser:

- Ruteo Estático: se configuran manualmente y tienen un único punto de salida
- Ruteo RIP: CE emplea RIP para comunicarle a PE cuales son los prefijos alcanzables desde el punto en que se encuentra.
- Ruteo OSPF: CE emplea OSPF para comunicarle a PE cuales son los prefijos alcanzables desde el punto en que se encuentra. Aplicable solo a VPNs con un único punto de salida.
- Ruteo BGP: CE emplea BGP para comunicarle a PE cuales son los prefijos alcanzables a través de él. Aplicable a VPNs con un único punto de salida y VPNs transitorias.

Para el punto de vista técnico BGP resulta el método más recomendable ya que fue diseñado para que funcione como un transporte de información de ruteo entre sistemas que son manejados por diferentes administradores.

4.7.3.1 Intercambio de información de enrutamiento mediante BGP

En las redes VPN MPLS, los routers frontera de proveedor obtienen el prefijo IP de los routers frontera de cliente mediante una sesión BGP o RIP. Luego el router frontera de proveedor lo convierte en un prefijo añadiendo 8 bits de distintivo de ruta (RD) que sirve como identificación de dirección del cliente sin importar donde se encuentre. El distintivo de ruta RD, se obtiene a través del VRF del PE en cuestión.

Todo paquete que viaja a través de la red de Backbone contiene dos etiquetas, una con la dirección del router PE y la otra con la información de cómo se debe reenviar el paquete al router CE. Al recibir un paquete el router frontera de proveedor lee y procede a quitar la etiqueta, enviando el paquete a la dirección indicada en la segunda etiqueta.

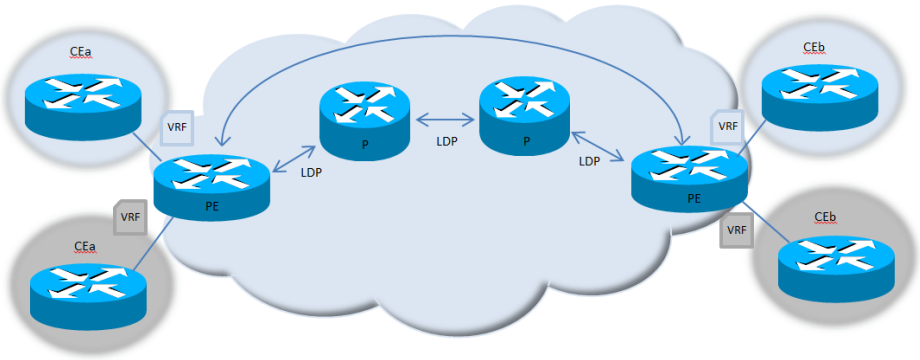


Figura 4.22.- Uso de BGP

4.7.3.2 Tipos de VPN: Configuración y Mantenimiento

Los mecanismos de configuración y operación varían según la tecnología VPN a utilizar.

- VPN del tipo ATM ó Frame Reley consiste en la generación de circuitos virtuales (VC) sobre una red pública el cual debe configurarse desde el equipo origen del

cliente, pasando por todos los equipos de la red hasta el equipo destino del cliente, lo cual lo hace una red difícil de llevar a la práctica.

- VPN de túnel IPSec, corresponde a una topología “hub-and-spoke” (centralizada), por lo que solo se deberá configurar los equipos del cliente apuntando al túnel IPSec hacia la casa central y resolver la autenticación de los túneles y usuarios e forma local o con un servidor de claves. La desventaja es que como el sistema anterior se realiza en forma manual y no hay un gestor de la misma.

- VPN MPLS, al no estar orientado a conexión, se puede conectar solo haciendo que al cliente ser parte de la misma VPN, al configurar solamente el CE. Este sistema recién comienza a integrarse al mercado.

4.7.3.3 Principales ventajas de VPN-MPLS

- Escalabilidad

Las redes VPN tradicionales con conexiones virtuales (VC) son difícilmente escalables, o sea, difíciles de crecer y poco flexibles. Para solucionar esto VPN MPLS ha utilizado el modelo Puerto a Puerto (P2P) el cual requiere que el cliente sea asociado a un solo router PE, haciendo innecesaria la utilización de túneles o circuitos virtuales.

Para asegurar la escalabilidad debe cumplirse que el router PE mantenga las rutas de todas las VPNs subscriptas a este y a su vez los routers P no deben mantener ninguna ruta VPN. Así se permitirá añadir futuras VPNs sin provocar congestión.

- Seguridad

Se entiende como seguridad a la posibilidad de proteger las redes de clientes de posibles ataques que afecten la disponibilidad del servicio y el resguardo de datos a posibles modificaciones o visualización.

Se puede garantizar que por más que varias VPNs con diferentes tipos de tráfico comparta el mismo camino físico o lógico, nunca se superpondrán. Si bien el tráfico fluye a nivel de capa 3, lo realiza emulando una capa 2 al aplicar etiquetas, permitiendo aislar el tráfico entre clientes.

- Gestión

Al no ser orientadas a conexión, no es necesario conocer la topología, ni tipo de conexiones de la red, por lo que es posible añadir sitios a la intranet formando grupos privados.

En cuanto al direccionamiento de las VPNs, se pueden utilizar direcciones privadas (que no se encuentran registradas) para navegar gratuitamente en la red pública de internet, gracias a que la VPN proporciona una vista pública y privada de la dirección. Debemos entender que la creación de VPNs se acopla al sistema MPLS y no actúa como superposición a este.

- QoS

Se debe asegurar la priorización del tráfico crítico o sensible al retardo sin despreciar el resto, gestionando el ancho de banda asignado a cada tipo de tráfico.
MPLS soporta la diferenciación de tráfico de una forma estandarizada, implementando herramientas.
Una característica importante es la posibilidad de proporcionar Clases de Servicios (CoS). Como se mencionó anteriormente el tráfico que ingresa es clasificado y etiquetado dependiendo de las políticas que fueron puestas por los suscriptores. Una vez clasificado es transportado por el núcleo de red.

4.7.3.4 Clasificación de VPN según su grupo

Existen diferentes formas de clasificar las VPNs, según sus grupos:

- VPN Sitio a Sitio (site-to-site): Utilizado para conectar diferentes sitios a un enrutador CE, el cual puede ser administrado por un proveedor de servicios o personal de la misma empresa. Este tipo de VPN se puede construir tanto para capa 2 como para capa 3.
- VPN tipo Tele-trabajador (Telecommuter): Utilizado para redes pequeñas o subscriptores individuales que conectan a través de una red ajena a una gran red. Este tipo de VPN se puede comparar con el servicio de Roaming en telefonía celular donde el cliente no siempre está en su ciudad de origen pero necesita transmitir información de voz desde cualquier parte que se encuentre.

- VPN Intermediaria (Wholesale): En este caso la VPN es usada por el proveedor para transportar el tráfico del subscritor, al proveedor de servicio de su elección.

Otro tipo de clasificación depende de donde comience la red, si en la instalación del cliente o en la red del proveedor:

- VPN Basada en PE de Cliente: En este caso la VPN comienza y termina en los enrutadores CE. El túnel es creado entre los dos dispositivos, por lo que la red solo pasa a ser un transporte de paquetes IP.

- VPN Basada en Red: En este caso la red comienza en el PE del proveedor y puede terminar tanto en otro PE del proveedor como en un CE del cliente. La información de ruteo es enviada desde el CE al PE, este último construye la tabla de ruteo basándose en la información recibida.

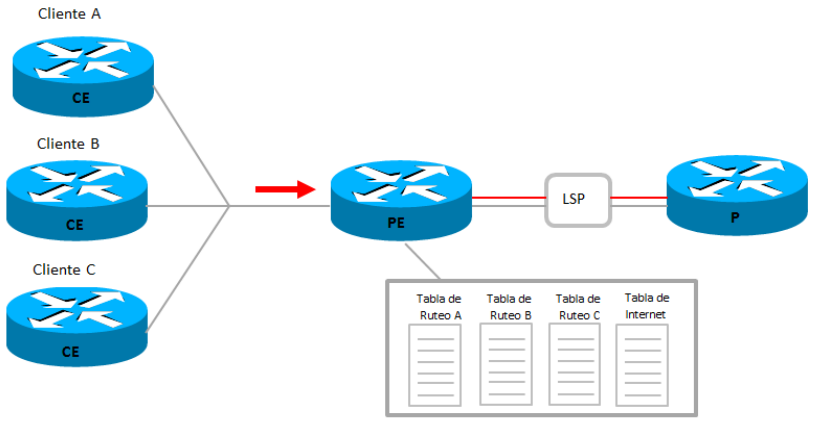


Figura 4.23.- Tablas de enrutamiento en base a la clasificación

CAPITULO 5: IMPLEMENTACION MPLS Y ANALISIS

5.1 Migración hacia MPLS

Las compañías de telefonía móvil se basaron en redes PDH y SDH que para transportar información TDM generadas por las Estaciones Base 2G; a las cuales se le acopló pocos años después la tecnología 3G y sus Nodos B ATM.

Paralelamente en la Red Fija ya se había asentado ATM como una tecnología madura que poseía una alta fidelidad y proveía QoS con el fin de poder procesar señales de voz y dato simultáneamente con la visión de un gran crecimiento a futuro del tráfico de datos. Por este motivo, las empresas móviles se vieron en la necesidad de incorporar ATM en sus redes troncales de Trasmisión de Acceso para poder soportar los tráficos de voz y dato de los Nodos B ATM que TDM no podría realizar.

El crecimiento de los servicios basados en IP y la aparición de MPLS cambiaron todas las perspectivas de la red. Los operadores vieron la ventaja de migrar sus redes de datos a IP/MPLS/Ethernet que permitía a una única infraestructura soportar todos los servicios existentes, lo que facilitó la tarea de operación y mantenimiento, la cual se simplificaba, y por lo tanto llevó a una reducción de costos (CAPEX y OPEX). Además de permitir la continuidad de los servicios preexistentes de la red, proporcionó soporte para futuras redes como LTE, convergencia de fijo-móvil, VoWi-Fi, VoIP, VPN sobre IP, etc.

En las redes móviles existen varias tecnologías presentes como GSM, GPRS, EDGE, UMTS y HSPA cada una con requisitos diferentes que se deben ser tenidos en cuenta a la hora de migrar la red TDM y ATM existentes. Para poder garantizar la continuidad de los servicios es importante asegurar una baja latencia y QoS, el encaminamiento IP no será necesario, ya que el encargado de esto debe ser MPLS, que procede a encaminar los paquetes a la nube MPLS en base a etiquetas de un nivel inferior. Por este motivo la mejor solución fue crear un núcleo MPLS separado de la red ATM y utilizar VPNs de Capa 2 mediante Pseudowires, migrando los servicios existentes a la misma. Por otro lado la red SDH se ha mantuvo para dar servicio al tráfico de BTS y los nodos B hasta lograr integrar toda la tecnología IP o adaptar los equipos SDH para transportar paquetes (STM-N no canalizados).

5.1.1 Pseudowires Emulation (PWE3)

El Pseudowires Emulation (PWE3) fue diseñado como una tecnología de trasmisión de servicios en capa 2 para brindar túneles sobre redes de conmutación de paquetes (IP o MPLS) para transportar señales TDM, ATM, Frame Relay y Ethernet. PWE3 permitió interconectar la red tradicional y la conmutación de paquetes; accediendo que los servicios de la red tradicional atraviesen la red de paquetes de alta capacidad conservando sus atributos.

Existen 2 clases de Pseudowires utilizados en la práctica:

- Los circuitos CES TDM que surgieron para transportar el tráfico TDM de las BTS a través de MPLS o tráfico Ethernet y;
- Los PW ATM, usados para transportar el tráfico desde el Nodo B hasta la RNC a través de la Red de Paquetes MPLS.

Con la aparición de Radioenlaces Ethernet que contienen puertos Fast Ethernet y Gigabit Ethernet dejó de ser necesario la utilización de PWE3 de capa 2 en el caso de que los Nodo B llegase a la red MPLS mediante puertos Ethernet; en este caso se dice que el Nodo B es Full-IP y utiliza L3VPN que es un modelo de VPN punto a punto que utiliza los LSPs MPLS para transportar los datos y el protocolo BGP, para intercambiar los datos de encaminamiento entre los LSRs implicados la ruta de cada VPN. En la Práctica se ha creado una L3VPN por cada equipo MPLS conectado a una RNC y se añadió una nueva configuración por cada Nodo B ingresado a un equipo MPLS con origen en esa misma RNC.

5.1.2 Redes Privadas Virtuales (VPN)

Como hemos mencionado anteriormente, las VPN son servicios ofrecidos por las operadoras, a clientes empresariales que permiten contratar cierta capacidad ya sea PDH o Ethernet en forma permanente y exclusiva. Estas redes facilitaron la comunicación de voz, dato, texto e imagen entre los equipos terminales.

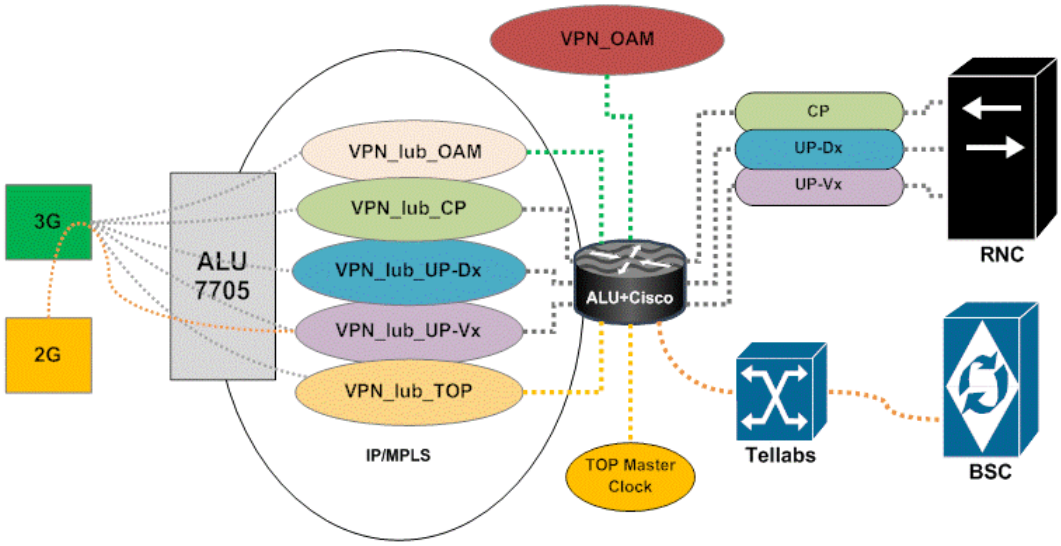


Figura 5.1.- Tráfico encapsulado en VPN´s

Parámetros a tener presentes para el diseño de una red MPLS

- Corresponde utilizar señalización MPLS LDP (Protocolo de Distribución de Etiquetas) en los nodos del Core.
- Se debe implementar Ingeniería de tráfico para brindar la capacidad de resolver un gran número de rutas BGP4, el cual fue diseñado específicamente para administrar el intercambio de información de enrutamiento entre diferentes sistemas autónomos, como por ejemplo el enrutamiento de conexiones hacia Internet; permitiendo generar rutas LSPs que proporcionen crecimiento y escalabilidad.
- Los nodos Borde, deben soportar la agregación de diferentes tráficos y diferentes protocolos de enrutamiento.

5.2 Pasos para Migrar una Red MPLS

La Migración de la Red MPLS conlleva varios pasos antes de realizarlo; como analizar el estado actual en que se encuentra y sus nuevas necesidades; solicitar y evaluar las propuestas de diferentes proveedores. Una vez verificados estos pasos, se procede a la implementación.

- Como primer instancia se debe analizar las necesidades, como la cantidad de sitios, el Ancho de Banda requerido, los tipos de dispositivos existente y sus

configuraciones, las aplicaciones empleadas y sus características (como sensibilidad, su variación durante el día/año, etc), que planea a corto/largo plazo se disponen para proveer los requerimientos de capacidad y por último, tener en cuenta la garantía de servicio que a prestar, ya sea con un proveedor de servicio propio o tercerizado.

- Como siguiente paso sigue presupuestar, en el cual se debe considerar los siguientes puntos; tiempo de antelación necesario para la migración, el cual dependerá de la zona geográfica, cantidad de sitios y estado actual de la red (el mínimo es de 6 meses); un importante punto a tener en cuenta es la tecnología de Acceso (si se realiza sobre conexión de FO o sobre par de cobre, si existen conexiones inalámbricas, con Ethernet Nativa o IP, etc); se deberá ver de disponer una herramienta de monitoreo de servicios; un punto no menos importante es ver si se solicitará una Interface Network to Network (NNI) del mismo operador o arrendada, ya que esta última opción no es la más indicada porque no todos los operadores ofrecen estándar de calidad extremo a extremo.

- Recién aquí es cuando se procede a realizar la implementación. En este punto es importante si se tiene previsto migrar a Voz sobre IP, prever un incremento de ancho de banda para acomodar el tráfico en voz y video. Se deberá considerar la planificación y ampliaciones de capacidad ya sea añadiendo nuevos sitios o incrementando el ancho de banda de los existentes. Para ello, se deberá valuar costos y tiempo de implementación. Se debe tener en cuenta la necesidad de personal idóneo, ya que serán necesarios para la gestión, configuración y arquitectura; personal que conozca los protocolos de encaminamiento.

5.3 MPLS sobre la Red de Acceso

Como sabemos, la Red de Acceso es la encargada de llevar los datos generados por los usuarios desde sus móviles a la BSC o RNC, para de allí terminar en la red Troncal.

La Red de acceso fue dividida en dos grandes grupos, la Red de Acceso Radio y la Red de Trasmisión de Acceso.

Las empresas de servicios implementaron una red MPLS en los puntos con alta concentración de tráfico y conectados entre sí mediante diferentes medios físicos (Fibra óptica, Radioenlace con capacidad Ethernet y xDSL) a través de los cuales se han creado

los caminos para enlazar los centros de conmutación, donde se encuentra la RNC, BTS o Media Gateways.

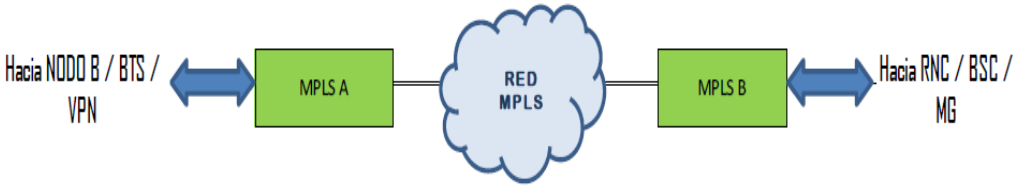


Figura 5.2.- Red MPLS

Generalmente suelen ser instalados dos equipos MPLS por cada RNC , con el fin de dar protección y distribuir la carga, hacia cada centro de conmutación donde se encuentra la RNC, BSC o Media Gateways a la que se han interconectado mediante puertos GE (Giga Ethernet) o STM-1 no canalizadas para ATM.

Entre los equipos MPLS y los centros de conmutación, se pueden ubicar los túneles LSP, uno principal y otro de protección, con tantos saltos como sean necesarios.

Como se comentó anteriormente, la inclusión de MPLS a la red existente comenzó de forma paulatina, hasta en un futuro lograr la total migración, por lo que los equipos MPLS deberán soportar una serie de servicios y disponer de las siguientes interfaces:

- Servicios Ethernet, como E-Line y E-LAN, el primero se trata de una línea virtual punto a punto, mientras que el segundo es una línea virtual multipunto a multipunto. Ambas son de nivel 2 y se diferencian mediante VLAN. La Red MPLS debe ser configurada para ofrecer a este servicio protección (túneles 1+1, Ingeniería de Tráfico), calidad (DiffServ o QoS Jerárquica) y OAM eficiente.

  Otro Servicio es el E-Aggr o E-Tree; un servicio punta a punto bidireccional convergente. Por ejemplo, en los servicios 3G, los nodos B convergen para transmitir a la RNC. A este flujo, se lo consideró un servicio de punto de convergencia entre la RNC-red MPLS, en donde se debe especificar el Ancho de Banda, para poder brindar QoS y asegurar los servicios.

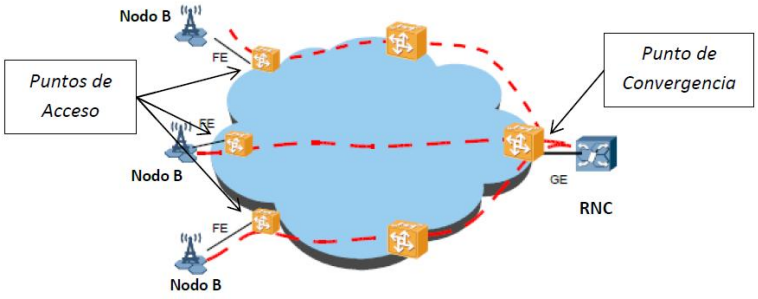


Figura 5.3.- Punto de convergencia desde la red MPLS hacia el RNC

- Servicios ATM, como la Emulación ATM y la Emulación IMA. En la Emulación ATM, la celda es encapsulada en pseudowire para poder ser transportada al nodo destino, donde luego es recuperado el flujo de la celda inicial. Mientras que la Emulación de Multiplexación Inversa para ATM, consiste en transportar ATM sobre circuitos E1 (PDH) o VC-12 (SDH) permitiendo utilizar la infraestructura TDM existente para ATM. Este método, es utilizado para transportar los datos generados por los nodos B ATM a través de la Red de Acceso TDM.
  Para cada Nodo B es creado un grupo de IMA sobre varias E1s (como máximo 8 E1s) que viajan agrupados hasta la interfaz UNI de MPLS donde al llegar comienza la emulación PWE3 del servicio ATM.

- Servicio TDM, como CES E1, utilizado para tráfico TDM proveniente de las BTS 2G o VPNs de voz, que debe ser enviado a través de la red de paquetes de forma trasparente para el usuario. La emulación de E1s puede ser realizada de forma estructurada o no estructurada. En el primer caso, el equipo recibe la trama y la información de los timeslot; procesa la cabecera, extrae la carga y encapsula cada canal de timeslot en la carga de los paquetes, siguiendo una secuencia para que cada canal sea fijo y conocido. En cambio de la forma no estructurada, el equipo toma la señal como un flujo constante de bits emulándose todo el ancho de banda de la señal TDM y enviándose tanto la cabecera como carga de forma trasparente. En el primer caso como podemos ver se puede ahorrar ancho de banda de trasmisión. Ambos métodos requieren un nivel alto de sincronización del reloj que debe ser proporcionado por el equipo MPLS.

La Normalización de las Interfaces es importante para permitir el acceso de los diferentes tipos de información y en los formatos existentes, como ser:

- Interfaz UNI (Interfaz de Red - Usuario) que es la interfaz entre la Red de Acceso y la red MPLS, empleada para el acceso de los servicios de usuario a la red de paquetes. En este grupo pueden encontrarse interfaces TDM E1, IMA E1, ATM STM-1, Fast-Ethernet, Gigabit-Ethernet y STM-1 canalizado para acceso de IMA/CES.
- Interfaz NNI (Interfaz Red – Red) que comprende la interfaz entre equipos MPLS que suelen ser enlaces de FO o Radioenlaces. La tecnología de transporte usada son Packet over SONET/SDH STM-1/4, Gigabit Ethernet, MLPPP E1 y STM-1 canalizado para MLPPP.

5.3.1 Creación de MLPPP

MLPPP (Multilink point to point protocol) consiste en agrupar flujos E1 o VC-12 de 2 Mbps creando un único enlace lógico de mayor capacidad, compartiendo la carga de tráfico y ofreciendo back-up, con el fin, que si un enlace falla, la carga es repartida conmutando hacia los enlaces operativos sin sufrir cortes.

Con esta tecnología se logró unir varias E1s y aumentar progresivamente la capacidad sin necesidad de incrementar el ancho de banda a una E3 (34 Mbps) para velocidad PDH, lo que significaría un costo elevado.

MLPPP se ha usado para transporte de señales TDM (E1 y VC-12) de BTS y servicios IMA ATM o ATM STM-1 de nodos B. Sin embargo hoy en día los Radioenlaces lograron admitir interfaces Fast-Ethernet (100 Mbps) y Giga-Ethernet (1000 Mbps) para envío de paquetes con un bajo costo por lo que este sistema ha quedado obsoleto.

Pongamos como ejemplo dos equipos MPLS conectados físicamente mediante un tramo SDH y un radio PDH de 32 E1s. Se necesitó crear un túnel LSP entre los equipos MPLS utilizando MLPPP para conseguir mayor capacidad. Cada equipo MPLS se conectó a un equipo multiplexor/desmultiplexor SDH mediante FO y este mismo unido al radioenlace mediante puertos E1s. Se definieron 20 enlaces lógicos de 2 Mbps cada uno y se creó un Multilink PPP por lo que se dispuso de un solo tubo de 40 Mbps, logrando que al definirse por último LPS, ya no verían 20 enlaces, sino un tubo de 40 Mbps.

Este tipo de tecnología prácticamente se utilizó para ser atravesado por paquetes MPLS de múltiples Nodos B y BTS simulando un único enlace común.

A diferencia, también se ha utilizado la tecnología IMA, solo que esta fue creada para cada Nodo B individualmente con un tráfico máximo de 8 E1s, llegando hasta la entrada de la red MPLS.

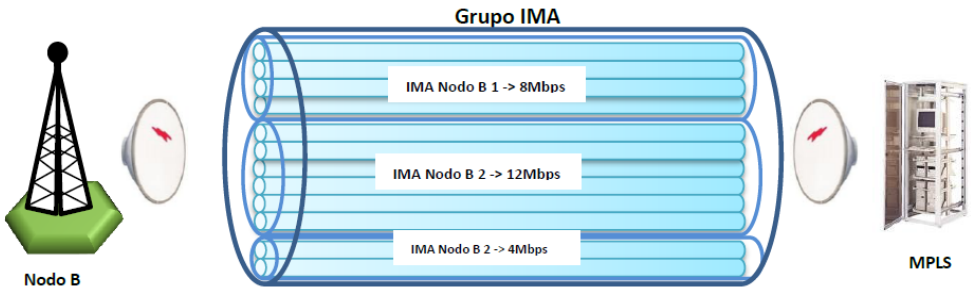


Figura 5.4.- Tecnología IMA para MPLS

5.3.2 Enlaces Ethernet

Este medio se presentó como un único tubo de gran Ancho de Banda para transportar todos los Nodos B y BTSs sin necesidad de protocolos intermedios (a excepción de PWE3).

Este tipo de tecnología permitió crear nodos Full-IP logrando extender la capacidad antigua de 8 E1s (16 Mbps) a 100 Mbps (siempre y cuando los nodos intermedios también sean de 100 Mbps). Para los puertos Gigabits Ethernet se pueden crear LPSs de 1Gbps siempre y cuando estén conectados a la fibra óptica.

El inconveniente en este método se presentó cuando se quiso introducir tráfico TDM generado por la estaciones base 2G o VPNs de voz sobre un LSP Ethernet, ya que fue necesario crear un circuito CES para cada E1 y siendo su capacidad mucho mayor a 2.048 Mbps que tiene las E1s por lo que en muchas ocasiones fue más conveniente enviar por separado el tráfico TDM hasta la red SDH.

Esto resultó interesante, ya que ofrecía protección ante la caída de alguna de las redes, permitiendo no dejar sin cobertura una zona, resultando una pérdida de servicio para muchos usuarios.

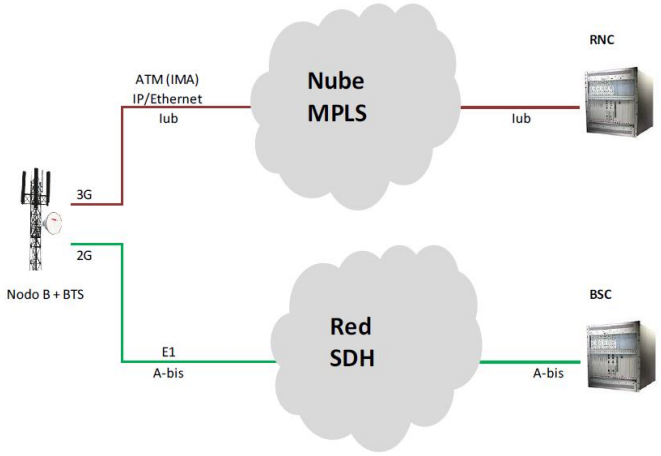


Figura 5.5.- Tráfico TDM Vs Tráfico ATM/IP

5.3.3 Pack over SONET/SDH (POS)

Disponiendo de una estructura SDH, una forma sencilla de enviar los paquetes fue introduciéndolos en un contenedor llamado POS que requiere la existencia de una capa intermedia llamada PPP (Point to Point Protocol) el cual dio acceso para transportar datagramas multiprotocolo sobre enlaces punto a punto.

Fue utilizada la encapsulación del protocolo PPP para mapear datagramas IP dentro de las tramas SDH/SONET. Este, es un protocolo altamente escalable y una alternativa para trafico ATM sobre SDH para redes IP/MPLS, además permite suprimir la necesidad de conmutadores ATM.

La alternativa POS se ha empleado en redes WAN o redes móviles donde ya existe una red SDH implementada. Hoy en día se pueden encuentrar algunos escenarios como este, aunque la tendencia es a eliminarlos, gracias a que existen alternativas mejores como la plataforma Ethernet.

Como desventaja POS, no permitió establecer circuitos virtuales como ATM por lo que no ofrecía QoS, pero si podía ser una buena opción para en escenario de Fibra Óptica en instalaciones WDM (Multiplexación por División de Longitud de Onda) que logra transportar varios canales ópticos sobre una misma fibra, el cual no nos explayaremos ya que queda fuera de nuestro proyecto.

5.4 Caso Práctico: Vuelcos de tecnologias Dual Iub a Full IP

El escenario de análisis, se compuso por celdas con nodos B distribuidos en distintas localidades de la provincia de Córdoba correspondientes a una de las empresas que brindan el servicio de telefonía móvil en nuestro país, y que han pasado por el plan de migración de dual Iub a Full IP.

Las celdas de referencia, ordenadas cronológicamente con la fecha de migración, son las que se detallan en la figura 5.6:

Nemónico de la celda	Localidad	Fecha de vuelco
CO001	Marcos Juárez	abr-12
CO004	Villa María	abr-12
CO106	Bell Ville	abr-12
CO008	Córdoba	jun-12
CO065	Rio IV	oct-12
CO201	La Rosada	ene-13
CO230	Villa Allende	sep-13
CO204	San Francisco	nov-13
CO558	Quisquisacate	abr-14
CO150	Saldan	jul-14

Figura 5.6.- Celdas del mismo ALM

Es importante mencionar que el estudio se basó principalmente en el análisis de datos estadísticos que se muestran en forma gráfica, conocidos como KPI (del inglés Key Performance Indicator, o Indicador clave de desempeño.)

Cinco de las diez celdas seleccionadas pertenecen a una misma cadena de transmisión, comenzando en un extremo con la celda CO558 formado por un Nodo B con tecnología Dual Iub encargado de brindar cobertura de comunicación móvil a Quisquisacate, y que debía atravesar la red de transmisión hasta la RNC ubicada en la ciudad de Córdoba (CO008).

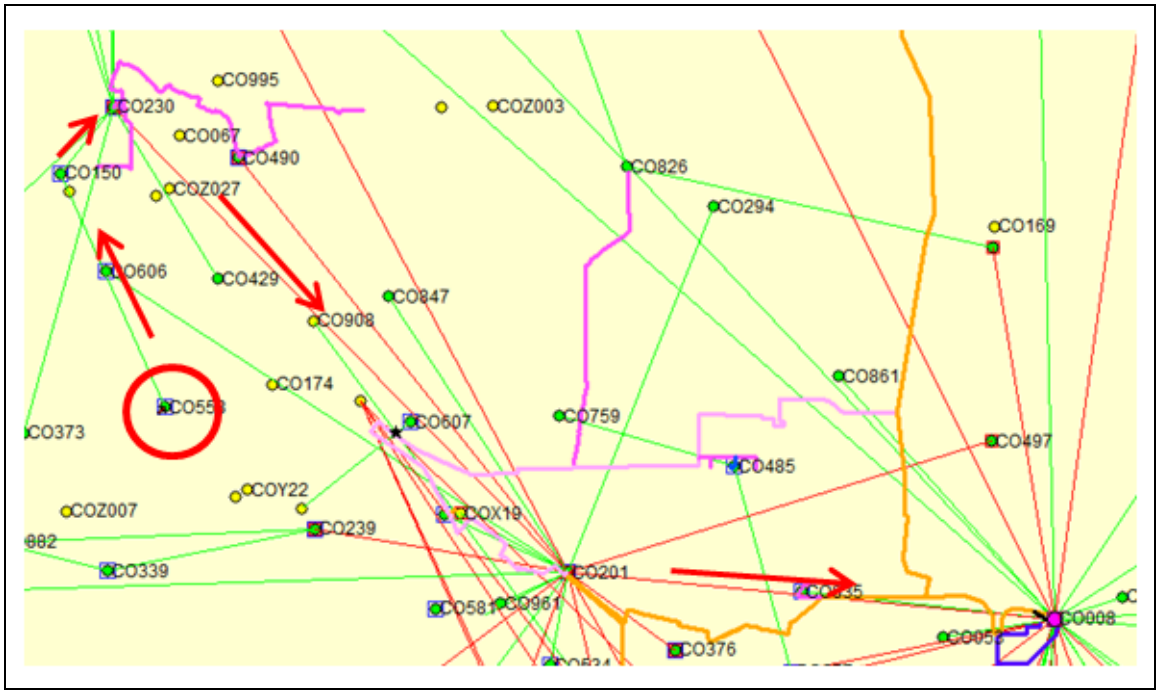


Figura 5.7.- Mapa de ubicación de celdas

En su primer paso, a través de un enlace PDH 1+0 llega a la celda CO150 (Saldan) quien se suma y a través de un enlaces PDH 1+1 (para soportar el tráfico de ambas celdas) pueden llegar a CO230 (Villa Allende). Desde este punto la tecnología empleada es SDH 2+1 por los que atraviesa las celdas CO201 (la Rosada) y llegando de esta manera al CO008.

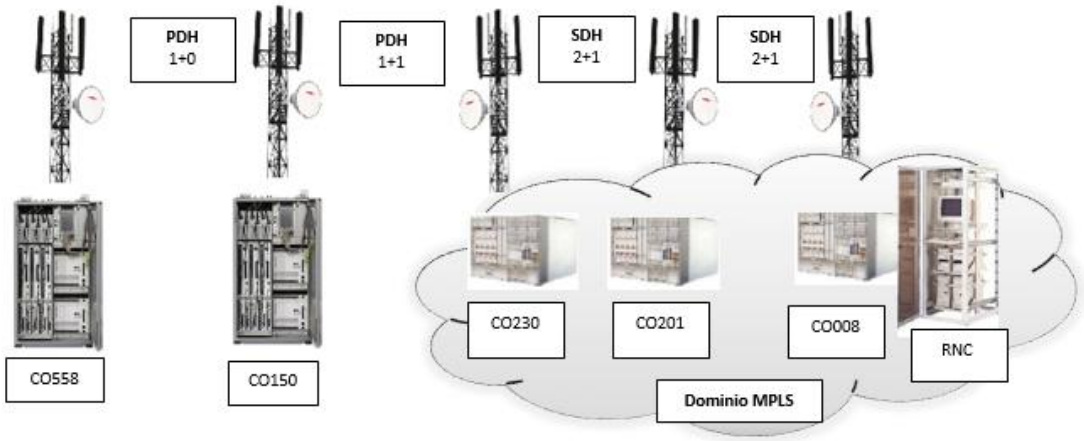


Figura 5.8.- Representación gráfica de la red analizada

El criterio de selección utilizado se basó en observar y evaluar el impacto del cambio de tecnología en forma local de cada celda, como así también verificar si hubo afecciones en la migración de una celda con respecto a una celda vecina.

El periodo de evaluación de cada sitio se centró en la fecha de vuelco, observando aproximadamente 6 meses antes y 6 meses después del mismo. Las restantes celdas se seleccionaron de modo tal que no estén vinculas entre sí, sobre una misma cadena de transmisión.

En forma genérica, común a todas las celdas seleccionadas, sabemos que el Nodo B es el encargado de enviar celdas ATM generadas por los niveles superiores del Nodo B hacia N enlaces E1 en forma secuencial, permitiendo tener una capacidad virtual de aproximadamente N x 2 Mbps. En nuestro el ejemplo tomado para el análisis de celdas de una misma cadena de transmisión, a lo largo de la ruta se fueron reservando recursos de N en N. Como la interfaz Iub que presentada tiene 4 enlace lógicos E1, entonces fueron necesarios 4 contenedores en la jerarquía y 4 conexiones físicas entre puertos E1, etc. Procedentemente, esta agrupación de E1s fue realizada mediante el protocolo IMA (Multiplexación Inversa de ATM), llegando al primer equipo MPLS que se encontraba en la ruta hacia la RNC. En el ejemplo, se encuentra ubicado en CO230 Villa Allende, donde ingresa a la nube MPLS.

Si el equipo MPLS posee sus LSPs configurados, el tráfico generado en el Nodo B atraviesa la nube mediante un PSWE3 IMA, hasta llegar al equipo MPLS ubicado al otro extremo de la red (CO008 Córdoba ECP). Al llegar la trama es desarmada, enviando solamente la trama ATM hasta la RNC.

Sin embargo, se puede presentar el caso en que el ancho de banda se encuentre saturado, por lo que parte del tráfico no podría ser cursado, siendo necesario asignar más recursos a la red. Para tomar una decisión sería necesario analizar lo siguiente:

- **La cantidad de tramas E1 disponibles en el Nodo B** (en el caso de las WBTS Nokia se dispone de hasta 8 E1s) por lo que la capacidad máxima de la interface Iub puede soportar hasta 16 Mbps. Como se han utilizado 4 E1s, se dispone de solamente las 4 E1s restantes.
- **La capacidad del Radio PDH**, solía surgir inconvenientes porque la asignación de recursos es estática, si hay más de un Nodo B conectado a este, que comparten la misma ruta. Si uno de los nodos no utiliza el total de su capacidad asignada, esta no

puede ser aprovechada por otro nodo que la esté necesitando. Una posible solución es ampliar la capacidad del radio, pero para ello habría que estudiar varios factores (Configuración hardware/software, si el espectro radioeléctrico pueda soportar una ampliación de canales sin interferencias, etc).

En el caso analizado no fue un inconveniente, ya que el equipo que se dispuso cuenta con 16 E1s y 2 puertos Fast Ethernet (100 Mbps).

- **La existencia de puertos libres** en todo el trayecto desde el Nodo B hasta la RNC.

Ya que se dispuso de puertos Ethernet en todo el trayecto, se decidió cambiar la celda de Dual 3G a Full IP. La ventaja de disponer una Iub totalmente IP, son de un mayor ancho de banda (permitiendo mayor velocidad de banda ancha móvil), convergencia de servicios y redes, etc.

Es por este motivo la tendencia a sustituir los equipos PDH/ATM por equipos Ethernet/IP.

Como se vio, en el enlace presentado, el tráfico de la celda terminal atravesaba 2 radios enlaces antes de entrar a la red MPLS donde se conecta directamente a la RNC. El Nodo B y el radioenlace se vinculan mediante puestos Fast Ethernet (FE) por lo que soportan hasta 100 Mbps. En el caso de atravesar una cadena de radioenlaces el de menor capacidad será el limitante para determinar el ancho de banda disponible en el Nodo B. Los equipos de radio y MPLS pueden ser conectados mediante puertos FE o GE en función de los nodos B que compartirán ese enlace de entrada al MPLS por ejemplo un puerto GE soporta hasta 13 nodos, mientras que un FE soporta hasta 5 nodos. Esto significa que un mismo enlace Ethernet entre un radio y el MPLS puede ser compartido por enlaces lógicos de varios Nodos B simultáneamente gracias a la multiplexación estadística.

Al ser una red basada en IP, todos los elementos implicados tanto la ruta de datos, como en la gestión de los Nodos B Full IP, deben disponer de una dirección IP con el fin de que los paquetes sean enrutados correctamente.

Para la Gestión Full IP, cada uno de los Nodos B presentados para este estudio, son los encargados de marcar los paquetes de la interfaz Iub con una VLAN y los de gestión con otra VLAN de manera que en la red MPLS se crean dos L3VPN, una para el tráfico Iub dirigido a la RNC y otro para el tráfico de gestión dirigido a los gestores de la red corporativa.

En cuanto al sincronismo del sistema Full IP, al eliminar los enlaces ATM, es decir las E1s se perdió la fuente de sincronismo del Nodo B, por lo tanto fue necesario una señal

de sincronismo externa para poder sincronizar el oscilador interno del nodo. Una opcion es proporcionar un equipo externo para brindar la fuente de un reloj a un máximo de 512 nodos B llamado IPCLK Server, incluso es aconsejable utilizar redundancia con dos IPCLK Server por cada 512 Nodos B Full IP.

Una vez definido el camino IP, se procede a borrar la configuración ATM para liberar recursos tanto en la RNC como en el Nodo B.

Ya en foco con el analisis, se comineza exponiendo la situacion del CO558. Recordando que su fecha de vuelco fue en abril de 2014, se pudo cuantificar en primera instancia el procentaje de acceso y conexiónes fallidas por parte del cliente hacia la red. En esta instancia se observó que el cambio fue notorio. La consecuencia de esto, como se mencionó anteriormente, fue la eliminacion total del protocolo ATM. La placa de Transmicion del Nodo B dialoga directamente contra la RNC mediante un medio 100% IP. Esto permitió omitir la utilizacion de los VC (Virtual Channel) para voz, un limitante que no se encuentra presente ahora. Si bien se ha dejado en claro, que para que una celda tome mas trafico es importante crecer la parte de Acceso, en el caso presentado, las condiciones de Hardware del acceso del Nodo B eran optimas para el escenario y se observaron una gran saturacion en los indicadores no solo de Iub, sino de usuario.

Retomando a lo referente del grafico, se observó que el porcentaje de conexiones no establecidas disminuyo noteblemente, a esto se los llama cotidianamente como disminucion en la accecibilidad de la celda. En el evento observado cuando la grafica cae a cero, es asociado a los trabajos que se realizaron en campo para migrar los servicios de la plataforma TDM + Ethernet a una plataforma 100% Ethernet.

Figura 5.9.- llamadas no cursadas – UCO558

Otro parametro importante es aquel que cuantifica la capacidad de la celda por cantidad de usuarios. Se observo que el número de usuarios simultaneos que la celda atiende no aumentó significativamente y es debido a que esto se encuentra limitado por el módulo de sistemas, el cual continua siendo la misma que para Dual Iub. Lo que si se percibió es una optimisación en el tráfico de bajada de datos (HSDPA). Se diferenciaron picos donde la cantidad maxima de usuarios de tráfico de datos aumento significativamente, llegando a un máximo de 90 usuarios aproximadamente.

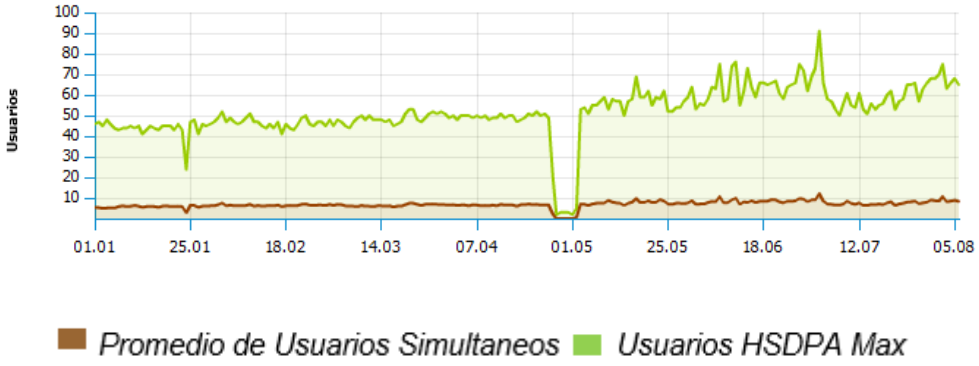


Figura 5.10.- Usuarios HSDPA – UCO558

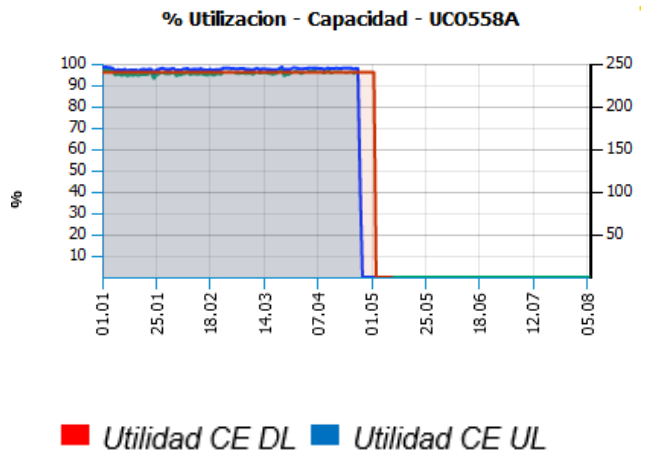
Figura 5.11.- Usuarios HSUPA – UCO558

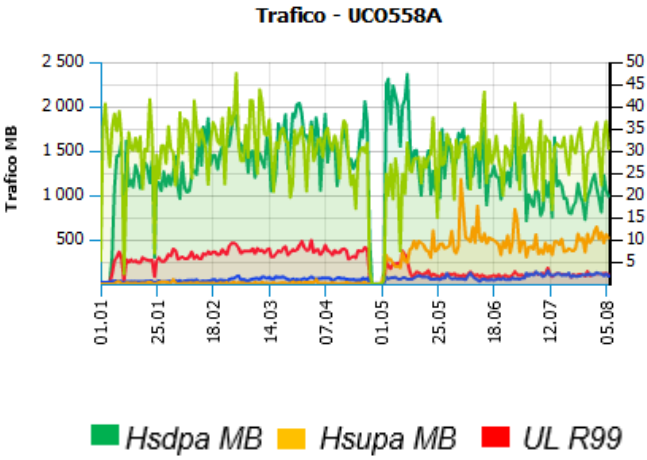
En el caso del tráfico de datos de subida, se presentó un significativo aumento, ya que la red dispuso ahora 100 Mbps para transmisión de datos, por lo que el tiempo de respuesta de los paquetes resultó mucho mayor que el que se disponia en una E1, al utilizar solo tráfico Ethernet, sin tener que estar migrando a otro medio de trasmission generando retardos entre uno y otro.

Una vez implementado el tráfico puramente Ethernet, se eliminó el tráfico de datos R99 (voz mas datos a una tasa de 384 Kbps) y se incrementó la tasa de datos HSPA, que provee velocidades de hasta 84 Mbps de Downlink y 22 Mbps de Uplink; logrando disminuir el tiempo de respuesta de usuarios.

A continuación, se presentan gráficos reales de como cambiaron los parámetros en una celda que pasó de ser Dual a Full IP, viendo como cayó la utilización de R99 y se incrementó el tráfico HSPA en cada uno de los sectores de la celda.

Sector A





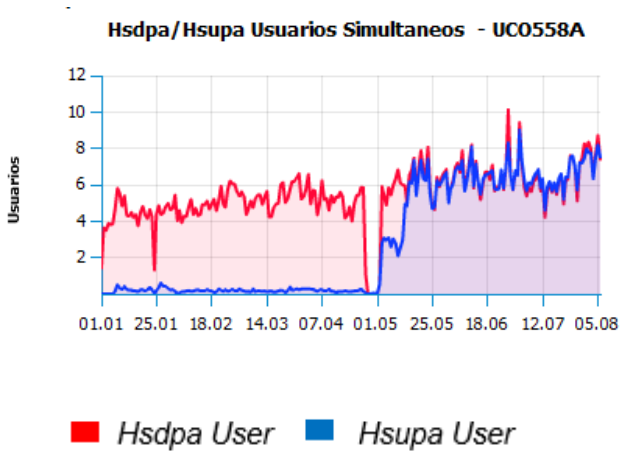
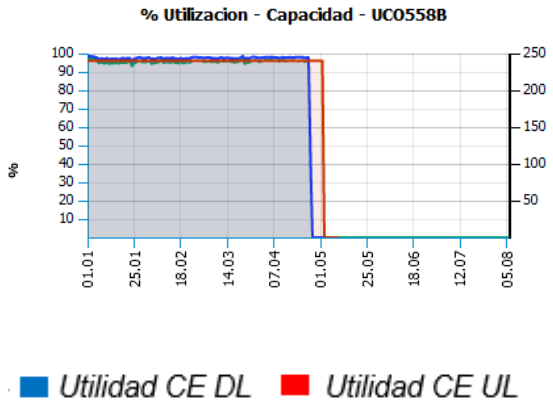


Figura 5.12.- Kpi – UCO558A

El primer gráfico se presenta el cambio a partir de la migración a Eth, dejando de utilizarse los channel element para el R99, mientras que en el segundo y tercer gráfico se observa como aumentó el tráfico en Mb tanto de subida como de bajada, al no enviarse mas datos por la celda ATM. Lo mismo sucedió en los sectores B y C pertenecientes a la misma celda.

Sector B



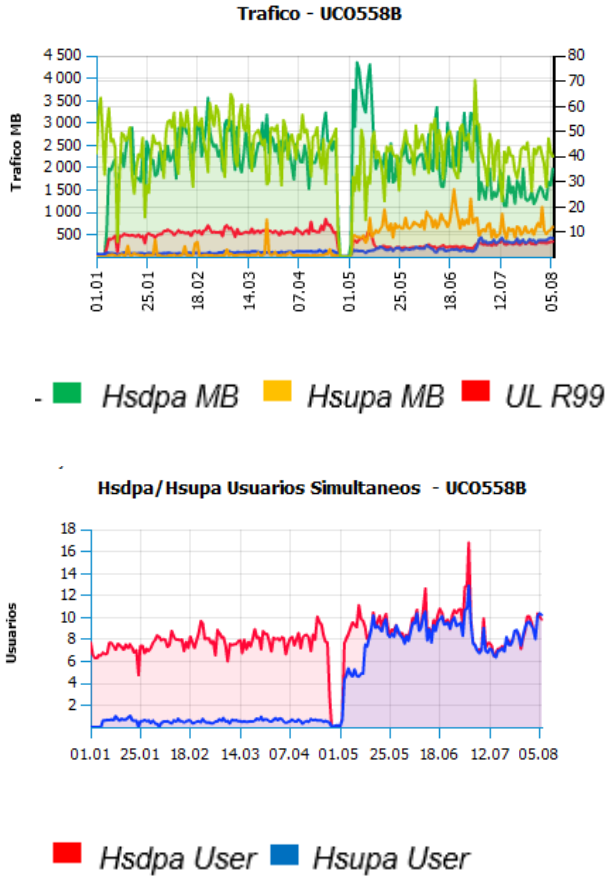
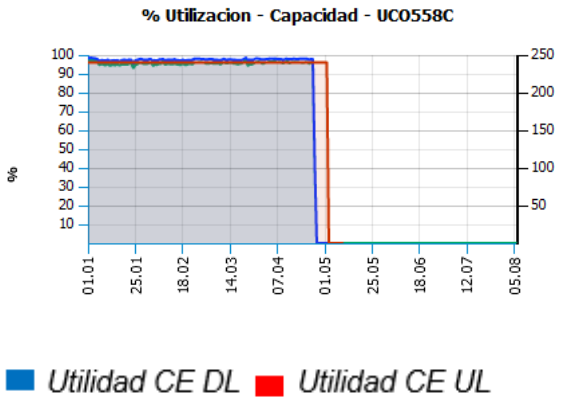


Figura 5.13.- Kpi UCO558B

Sector C



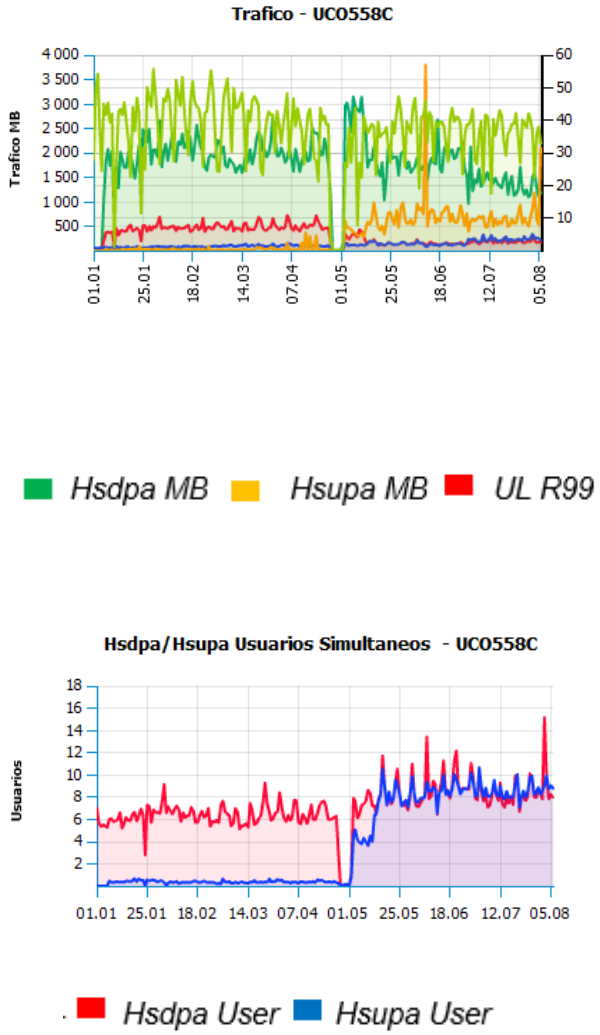


Figura 5.14.- Kpi UCO558C

Al continuar la cadena de transmisión que tuvo comienzo en CO558, nos situa en CO150 (Saldan) donde se examinaron los mismo graficos que el caso anterior. La intencion al analisar el comportamiento de una misma cadena es poder divisar si un cambio en una celda A puede influenciar en su celdas vecinas B

Se presentan los mismo graficos que el caso anterior, y teniendo en cuenta las fechas de los vuelcos en ambas celdas. CO558 en abril de 2014 y el CO150 en junio del mismo año:

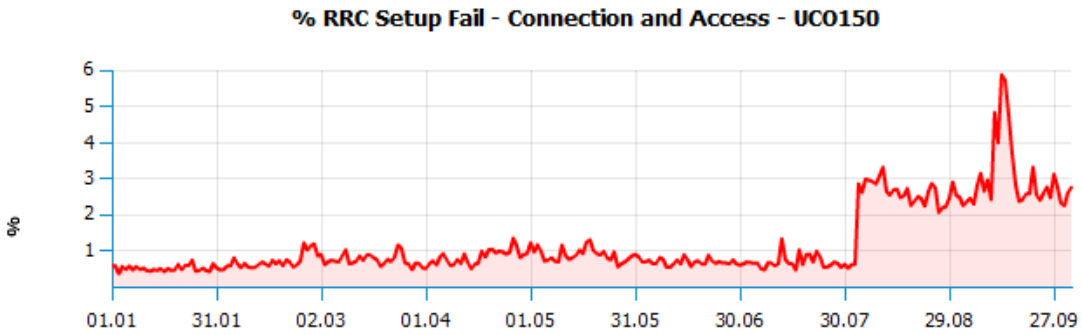


Figura 5.15.- % llamadas no cursadas – UCO150

A simple vista es notablemente en la fecha del vuelco de la celda como el porcentaje de rechazo de acceso y conexión de usuarios a la red se cuadriplico, pasando de un 0,7% de promedio a un 2,8%. Sin embargo, al posicionarse uno en la fecha del vuelco de la celda vecina CO558, se puede observar que no ha tenido influencia alguna.

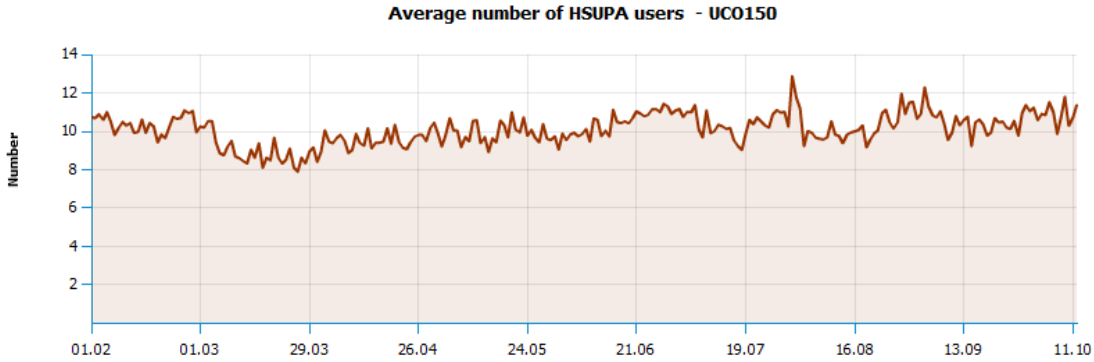


Figura 5.16.- Ususarios promedio HSUPA – UCO150

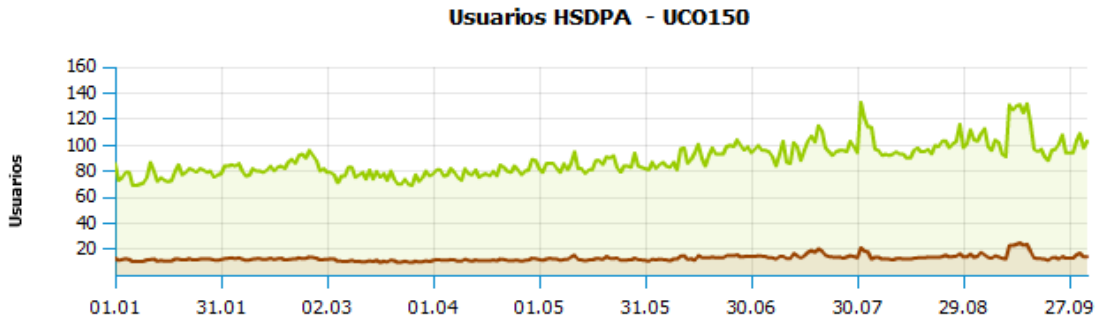


Figura 5.17.- Usuarios HSDPA – UCO150

En cuanto a los usuarios de datos, apenas fue notorio en la gráfica de downlink un incremento en catidad de usuarios, mientras que en la gráfica de uplink el numero de usuarios promedio en el celda continuó presentando las mismas variaciones, estos se muestró independientes del cambio.

A pesar de que estos datos no aparentaron ser muy demostrativos, esta celda justificó en forma inmediata el cambio de tecnologia mediante el incremento que presentaron los potenciales usuarios de datos en el zona a la fecha del vuelco. Este es un dato que puede ser reflejado por la proyeccion estadistica de trafico a cursar por esta celda. Para un analisis mas completo sobre este ultimo tema es necesario disponer de informacion adicional proveniente del area de marketing, donde pueda brindar datos de densidad de poblacion y probabilidades de inserción tecnologica, datos que no estan en el alcance de este trabajo.

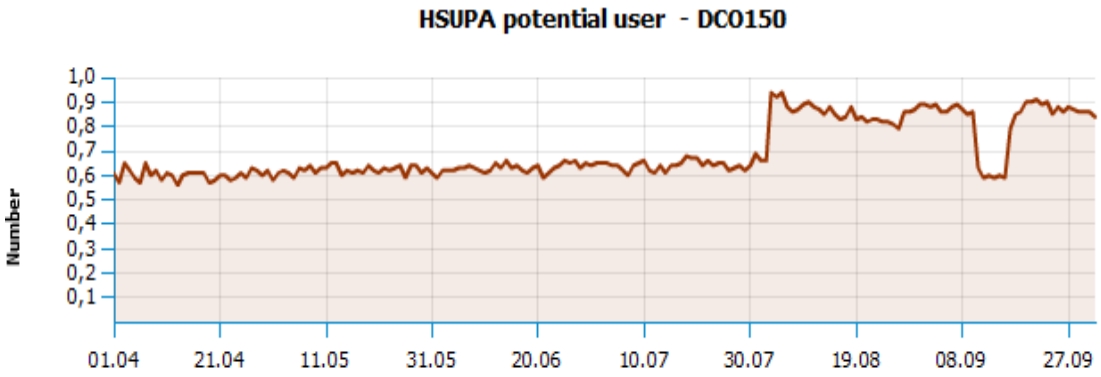


Figura 5.18.- Potenciales usuarios de Uplink

Se tuvo la oportunidad de evaluar a este sitio desde la interface Iub (Tx), donde se pudo observar el incremento del porcentaje de utilización que ha crecido de un 12% a un promedio de 18%. Se presentaron eventos que llamaron la atención al evaluar estos parámetros, en este caso se advirtieron dos picos que llevaron a un valor de 0 (cero) a este parámetro. En primera instancia podríamos pensar que probablemente en esas fechas el vínculo estuvo caído.

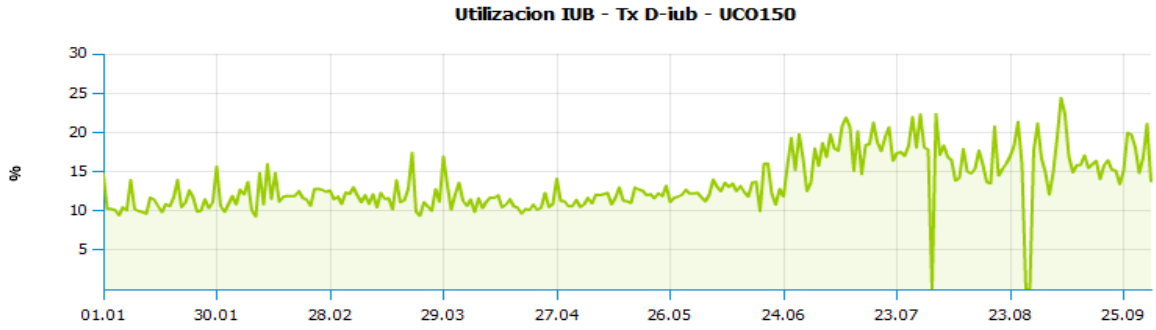


Figura 5.19.- Utilización Iub

Sin embargo, se pudo mapear el grafico anterior con algún otro parámetro como ser el throughput (medidos en Mbps) y, además teniendo en cuenta el incremento de datos que se subieron desde la red en la fecha del vuelvo vimos que los picos “hacia abajo” coinciden, por lo tanto se llegó a la conclusión que el problema se encontraba en la transmisión y no en la celda.

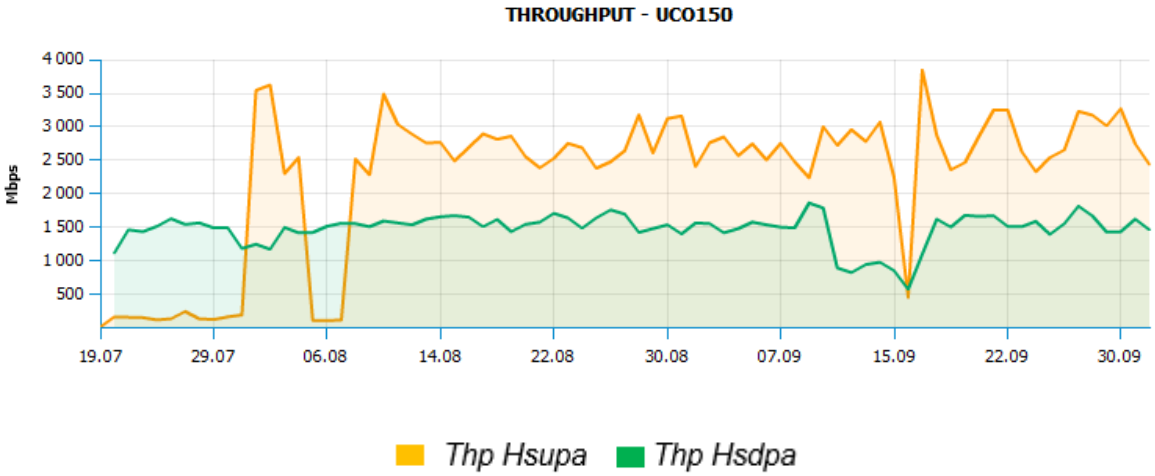


Figura 5.20.- fujo de datos UCO150

La transmisión de datos de subida (HSUPA) no estuvo disponible, mientras que en el HSDPA se mantuvo operativo. Si bien, es sabido que una caída del vínculo de transmisión es acusada por una alarma dedicada, solo mirando estos datos estadísticos se puede

deducir que el vínculo no estuvo caído, suposición que habíamos llegado anteriormente en el indicador de porcentaje de utilización de la Iub en transmisión. Pero si se presentó problemas en la transmisión de datos desde la celda hacia la RNC.

Continuando con la cadena de transmisión, es el turno a la celda CO230, de la localidad de Villa Allende. Recordemos que su fecha del vuelco fue en septiembre del 2014.

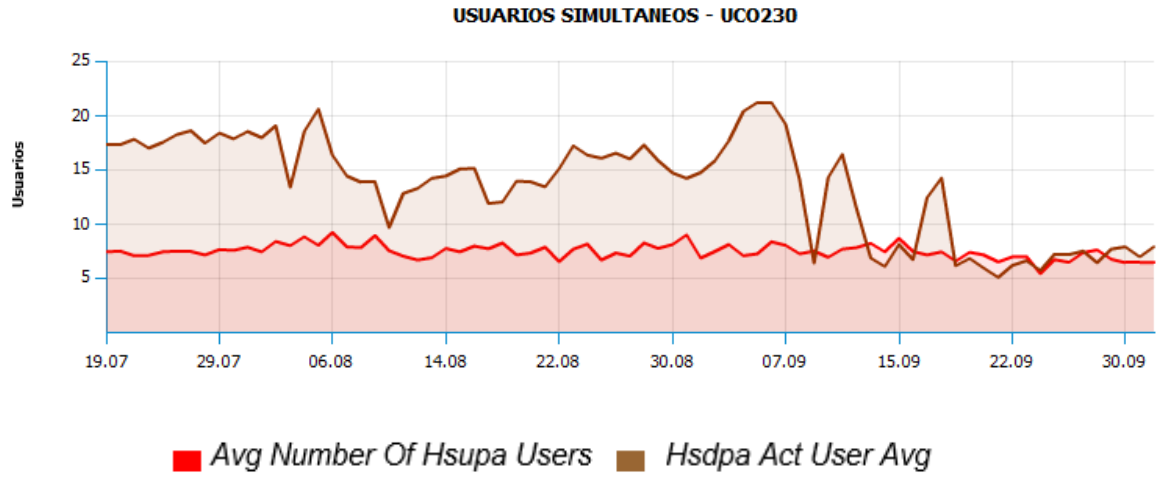


Figura 5.21.- Cantidad de usuarios simultaneos – UCO230

Analizando el grafico de usuarios simultáneos de datos, se pudo ver que en la fecha del vuelco los usuarios promedio de downlink cayeron notablemente, mientras en uplink se mantuvo una variación estadística permanente.

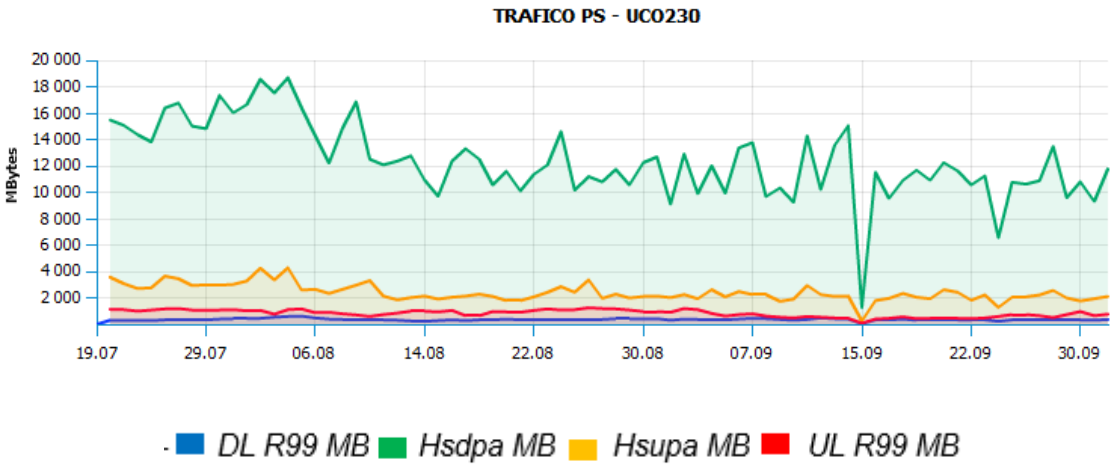


Figura 5.22.- Tráfico de paquetes UCO 230

Este grafico expone las características del tráfico de datos en 2G y 3G. En principio suponemos que la fecha del vuelco exacta fue el 15/9 ya que como vimos anteriormente el tráfico llega al valor de 0. En líneas generales se notó que las gráficas presenta una pequeña pendiente negativa, lo cual implicó una reducción del tráfico de datos. En este caso, no fue notorio que el cambio a full IP haya influenciado en el servicio, ni para mejor ni para peor. Demográficamente este sitio se encuentra en una localidad más densamente poblada que el caso de su celda vecina CO150. Mientras que aquí se pudieron apreciar picos de 18000 MBytes en la celda vecina los picos llegaron a valores de 3500 MBytes.

Otro grafico que muestra que el cambio ha sido transparente para esta celda es el de usuarios potenciales de uplink, con una leve pendiente creciente de este parámetro proviene desde antes de la fecha del vuelco.

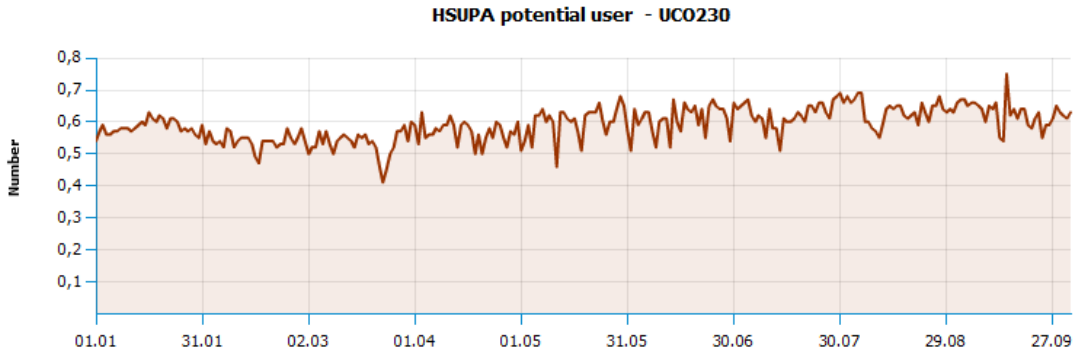


Figura 5.23.- HSUPA potenciales usuarios

Es el turno del CO201, denominado “La Rosada”. Su fecha del vuelco fue en septiembre del 2013. Empezamos por la gráfica que más llamó la atención: la no accesibilidad para HSUPA. Que de alguna forma complementaria al gráfico del crecimiento del tráfico de HSUPA que hemos visto para otras celdas.

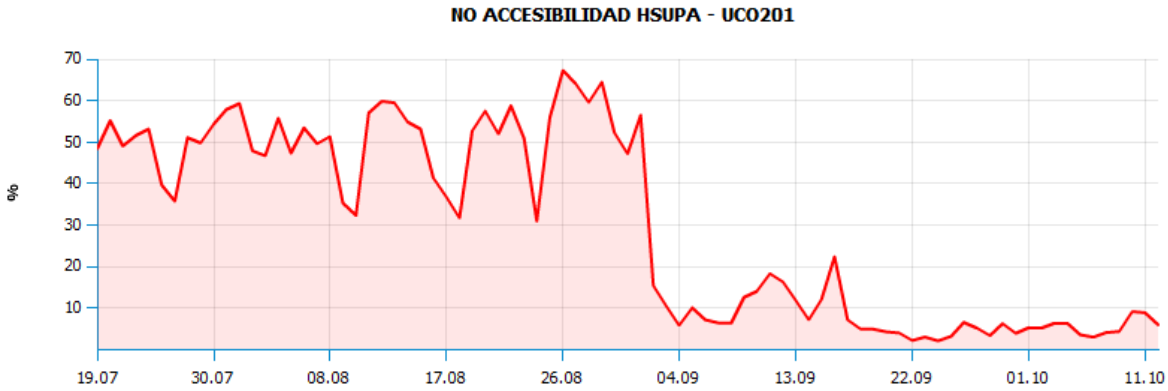


Figura 5.24.- No Accesibilidad HSUPA

Hubo un cambio abrupto ya que pasó de promediar el 48,3% a promediar el 9%. Fácilmente se podría decir que el cambio sí tuvo efecto. En cambio la no accesibilidad de HSDPA presentó un comportamiento diferente.

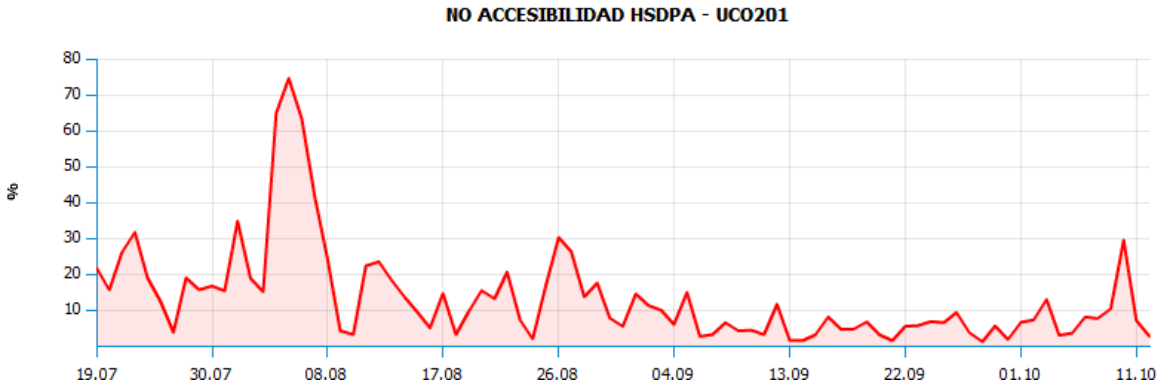


Figura 5.25.- No Accesibilidad Hsdpa Rate

En este parámetro se manifestó el cambio a Full IP en sus picos. Luego del cambio, los picos obtuvieron menores valores.

Llegando al final de la cadena de transmisión, se encuentra CO008. El cambio a Full IP fue realizado en junio del 2012. Parámetros donde se han observado cambios son:

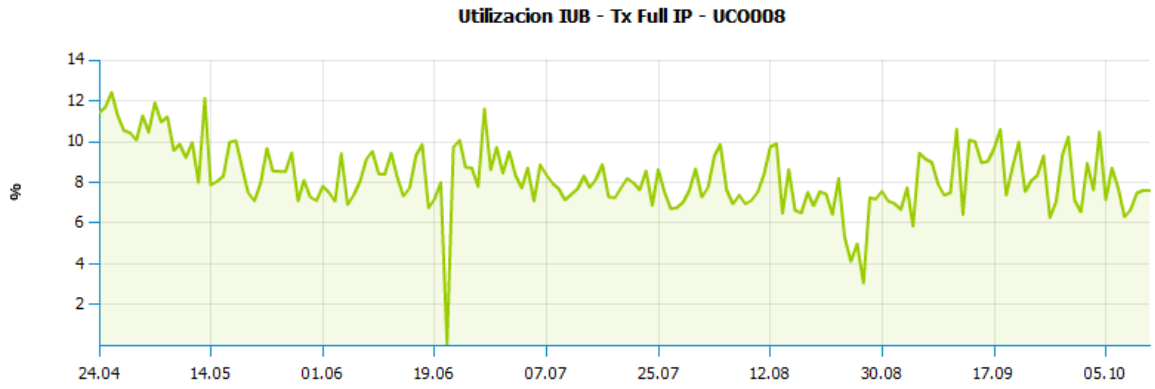


Figura 5.26.- Utilización Iub

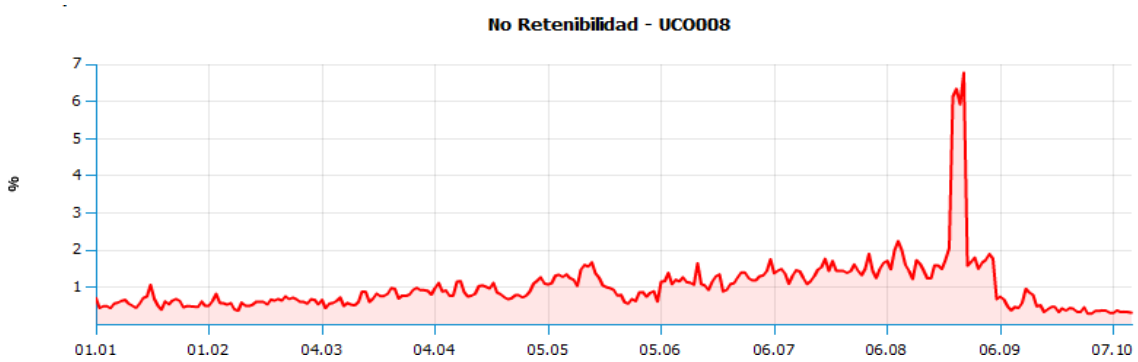


Figura 5.27.- % No Rentabilidad – HSDPA

Como ya se ha observado, sobre el grafico de usuarios de downlink, se advirtió que se mantuvo constante a pesar del cambio de tecnología de los sitios asociados a este.

El porcentaje de utilización de la interface Iub presentó una leve liberación de recursos luego de la migración en CO558, más allá de los picos a cero que pueden ser vinculados a una alarma de caída de la interface.

En el último caso, se demostró mediante un gráfico la “No rentabilidad” del sitio, se debe tener presente que corresponde a una RNC que concentra todo el tráfico. Si bien, este es un paramento netamente vinculado con el aspecto económico y con el cual podemos reflejar la reducción de costos al emplear nuevas tecnologías, ya que una aproximación a los costos de inversión para un Nodo B 3G es de 30.000 USD; de los cuales el 30% corresponden a servicios. La diferencia con un nodo B Full IP radica en los beneficios ya que el costo de inversión es el mismo para ambos casos, pero la capacidad del segundo es

superior al traficar una mayor cantidad de datos, pero como se detalló anteriormente, la mantención operativa de una red puramente Ethernet es menos costosa y la posibilidad de solucionar inconvenientes en forma remota es una gran ventaja que estas redes presentan.

También podemos destacar que existe una amplia incongruencia en las estadisticas de las llamadas caídas y el bajo porcentaje de utilización de las interfaces Iub. Esto se debe a dos motivos:

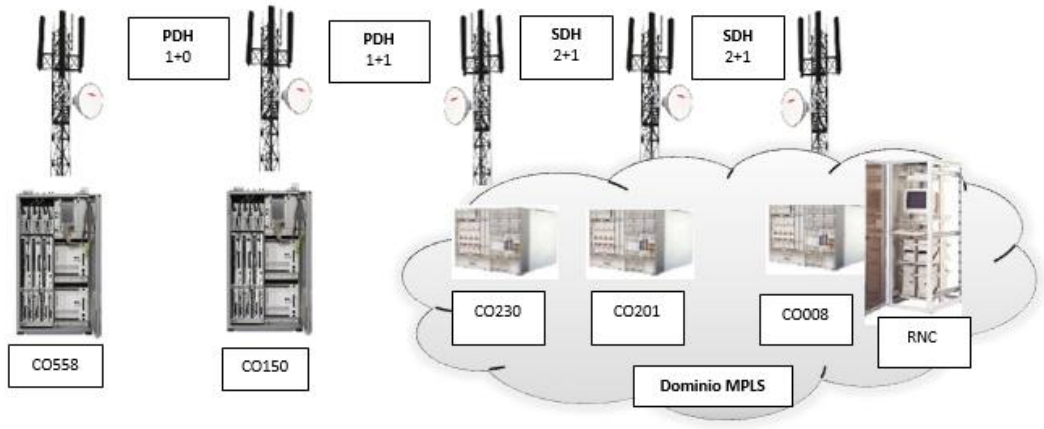
Las capacidades de utilización en la Iub oscilan entre el 12% y el 30%, el cuello de botella se encuentra en la interfaz Uu, debido a que el problema yace a nivel de RF a causa de escasa disponibilidad del espectro y al incremento del tráfico de datos ingresando a la red para ser cursados. Por estos valores bajos de utilización de Iub, la ingeniería de trafico hoy es solo aplicable para priorizar tráfico y no a solucionar problemas de congestión.

CAPITULO 6: IMPACTO ECONOMICO, SOCIAL Y AMBIENTAL

6.1 Evaluación económica

Se consideraron dos modelos alternativos para poder hacer el upgrade completo de toda la red descripta en el caso de estudio. Antes de presentar las propuestas, creemos conveniente retomar la descripción del segmento de red actual.

Como puede verse en la siguiente figura, anterior al upgrade la red cuenta con Full IP desde el sitio CO008 (Córdoba ECP) hasta CO230 (Villa Allende). En cuanto a medios de transmisión la red esta compuesta por fibra óptica en el primer salto, continuando por un enlace de radio SDH para el segundo salto, y sus dos últimos saltos con enlaces de radio PDH.



Al contar con una red de Tx existente hasta CO558 (Quisquisacate) para los servicios de 2G y 3G, y considerando que la existencia de Full IP hasta CO230 (Villa Allende), desde el punto de vista de la transmisión solo fue necesario crecer en capacidad el radio enlace de CO150 a CO230 para soportas el tráfico generado por los 2 sitios en CO150 y CO558 ahora con tecnologías full IP.

Los costos relacionados a estos cambios fueron los siguientes:

Tecnología	Proyectos	Tipo	CANTIDAD MODELO 1	COSTO USD MODELO 1
RF	**FULL IP**	Sitio Nuevo	2	USD 45,042.38
TX	**FIBRA OPTICA**	Construcción	0	USD -
	MICROONDAS	Upgrade	1	USD 25,664.00
		Última Milla	0	USD -
				USD 70,706.38

Teniendo en cuenta las tendencias del mercado, la actual tecnología 4G y las futuras proyecciones hemos considerado el costo de implementar fibra óptica en todo el tramo de la red estudiada con un costo aproximado por 12.86 km por un total de USD 491,600.28 dependiendo del recorrido que se realice para la canalización de la misma.

COSTOS INDIVIDUALES

FO AL NODO		
Servicios Instalación	$ 38,520.00	Serv
FO	$ 5,184.00	HW
Misceláneos	$ 1,296.00	HW
Energía	$ 7,550.00	HW
Adec espacio/energía	$ 4,000.00	Serv
IP RAN	$ 9,000.00	HW
Serv IP RAN	$ 3,000.00	Serv
Auditoria	$ 1,000.00	Serv
LOGISTICA	$ 8,751.40	Log
TOTAL	$ 78,301.40	

FO x KM		
Servicios Instalación	$ 29,000.00	Serv
FO	$ 5,120.00	HW
Misceláneos	$ 1,024.00	HW
LOGISTICA	$ 2,334.72	Log
TOTAL	$ 37,478.72	

Iluminación de sitio		
Energía	USD 7,550.00	HW
Adec espacio/energía	USD 4,000.00	Serv
DWDM	USD 150,000.00	HW
Serv DWDM	USD 12,000.00	Serv
LOGISTICA	USD 59,869.00	Log
TOTAL	USD 233,419.00	

MW BKB (4+1)			UP GRADE (2+1)
Servicios Instalación	$ 17,000.00	Serv	$ 7,000.00
RADIO	$ 72,000.00	HW	$ 10,800.00
Miscelaneos	$ 2,000.00	HW	$ 2,000.00
Energia	$ 7,550.00	HW	
Adec espacio/energía	$ 4,000.00	Serv	
Refuerzo estructura	$ 1,794.80	Serv	
Auditoria	$ 1,000.00	Serv	$ 1,000.00
LOGISTICA	$ 30,989.00	Log	$ 4,864.00
TOTAL	$ 136,333.80		$ 25,664.00

MW ACCESO (1+0)		
Servicios Instalación	$ 14,000.00	Serv
RADIO	$ 14,000.00	HW
Miscelaneos	$ 2,000.00	HW
Energia	$ 7,550.00	HW
Adec espacio/energía	$ 4,000.00	Serv
Auditoria	$ 1,000.00	Serv
LOGISTICA	$ 8,949.00	Log
TOTAL	$ 51,499.00	

FULL IP		
NODO B	$ 15,621.00	HW+SW
Miscelaneos	$ 3,400.00	HW
INSTALACION	$ 6,000.00	serv IMP
Aditoria	$ 1,000.00	Serv
LOGISTICA	$ 19,031.38	Log
TOTAL	**$ 45,042.38**	

6.2 Impacto Social

En los últimos años el mercado de la telefonía móvil ha evolucionado crecientemente y generando una expansión de las inversiones en infraestructura de redes, permitiendo a un gran número de personas ganar acceso a nuevos servicios de telecomunicaciones. Todos estos cambios conllevaron a que en la actualidad el número de líneas móviles haya superado ampliamente el número total de líneas fijas.

Esta expansión de la cobertura de los servicios ha posibilitado también el ingreso de usuarios en muchas zonas rurales y semi urbanas.

La telefonía móvil puede ser considerada un generador de innovación porque es un promotor y facilitador para la invención y producción de nuevos servicios, productos o procesos, un ejemplos de esto es la utilización de llamadas perdidas para actividades de la vida cotidiana, las operaciones bancarias móviles, tanto en zonas rurales como en zonas urbanas, etc.

La difusión de la telefonía móvil trajo cambios en la organización diaria de la vida privada y los negocios al permitir mediante la comunicación inalámbrica mayor flexibilidad de gestión y acelera los procesos que dependen de las comunicaciones. Una ventaja en la utilización de la telefonía móvil es el poder reducir los costos del acceso a la información y la incertidumbre en la toma de decisiones. Esto es válido también en los casos en que no hay barreras técnicas o de precios para el acceso a la información. Cuando este último se facilita, los negociantes pueden tomar decisiones más informadas y, en consecuencia, puede mejorar la eficiencia del mercado. Pueden reducirse los gastos de transacción y debe aumentar la transparencia del mercado.

Los teléfonos móviles se adaptaron con más facilidad entre todos los segmentos de la población que las computadoras o Internet. En realidad esto se debió a que son una tecnología sencilla con costos de aprendizaje muy bajos, en particular tratándose de

comunicaciones audibles, y con requisitos de infraestructura que los hacen comparativamente más asequibles.

Los móviles han contribuido al desarrollo, particularmente en los países y regiones más pobres, pero un móvil no ayuda a reducir la desigualdad. Sin embargo, tiene un impacto positivo sobre el empleo, en parte porque un gran porcentaje del trabajo urbano es autónomo; a partir de la localización permanente del móvil hay más trabajo. También las posibilidades de encontrar empleo aumentan gracias a que se limitan los intermediarios que controlan el trabajo.

Otra conclusión del estudio es el aumento de la seguridad de las personas tanto en medios urbanos como rurales. La posibilidad de establecer comunicaciones móvil constante mejora el sentimiento de seguridad y también la autonomía de las personas. La mayoría de las llamadas del móvil se realizan desde sitios en los que se podría llamar de otra manera.

Esta nueva capacidad de autoinformarse y autocomunicarse es de naturaleza revolucionaria, y ha dado lugar a:

a) **movimientos sociales** que no necesariamente buscan conquistar el estamento político sino introducir nuevos valores y provocar cambios de mentalidad en la sociedad (ejemplos: movimientos feministas, ecologistas y defensores de los pueblos originarios);

b) **nuevas formas de insurgencia política**, que con sus acciones pretenden afectar y contravenir la esfera política (como los movimientos de protesta organizados a través de las redes sociales; algunos ejemplos: las movilizaciones de protesta política coordinadas a través de redes sociales; las campañas políticas, etc

Por lo que podemos ver, la tendencia es un incremento exponencial de consumo de datos y cada vez mayor a través de dispositivos móviles.

6.3 Impacto Ambiental

A principios del siglo XX se produjo la expansión de las radiocomunicaciones y luego se inició un proceso de diversificación y masificación de los servicios que utilizan las tecnologías inalámbricas.

Estas comunicaciones son transmitidas mediante el espectro radioeléctrico por lo que es necesario contar con “Estructuras de Soporte de Antenas” o “Radiobases” para instalar sobre ellas las “antenas” propiamente dichas y comunicar las Radiobases, entre sí.

En el caso específico de las comunicaciones celulares, las Estructuras son necesarias para servir las llamadas hacia y desde los teléfonos móviles. Estas Estructuras de Antenas deben ubicarse necesariamente allí donde el servicio requiera ser prestado.

La distribución geográfica de las instalaciones para telecomunicaciones está íntimamente ligada al área de cobertura (superficie geográfica, de forma aproximadamente circular, en donde el servicio está disponible); en el caso de la antenas, estas dependen de la potencia necesaria de emisión, la topografía del terreno y la cantidad y tipo de construcciones existentes en ella, entre otros factores. Un estimativo de la superficie cubierta considerando: las potencias máximas de emisión y los servicios prestados en un área de topografía plana y sin construcciones, con el objeto de obtener los radios máximos teóricos del área de cobertura para la de telefonía móvil celular, es aproximadamente de un radio de 9 km. Por lo tanto se infiere que para prestar el servicio de telefonía celular móvil en un determinado espacio geográfico se necesita una cantidad significante de instalaciones de antenas. En la realidad, la brecha se amplía aún más debido a características tecnológicas propias de las redes de telefonía celular tales como su operación en forma de red de células (celdas), es decir, en vez de utilizar un transmisor de gran potencia y gran cobertura, se subdivide el área de cobertura en áreas más pequeñas llamadas celdas que tienen como elemento central a las estaciones bases y la limitación de potencia impuesta a los teléfonos móviles por razones de seguridad, entre otras.

Al analizar la distribución del área de cobertura, se obtienen los siguientes resultados:

- La distribución de cobertura coincide con la distribución de población. Esto significa una mayor cantidad de estaciones de base en las zonas de mayor densidad demográfica.

- Existen corredores de telefonía móvil que permiten mantener las comunicaciones mientras las personas se desplazan entre los centros urbanos; en consecuencia, son coincidentes con los corredores de transporte terrestre vehicular (carreteras). Esto implica presencia de estaciones de base a la vera de los caminos y mayor densidad de éstas en aquellos con mayor tránsito.

Desde la cota 0 o nivel de suelo, pueden identificarse los componentes físicos de las instalaciones:

- Los sistemas de antenas necesarios para irradiar/recibir las ondas electromagnéticas.

- Los soportes del sistema de antenas, necesarios para mantenerlas a cierta altura con el fin de ampliar el área de cobertura del servicio.

- Las casillas destinadas a contener los equipos eléctricos necesarios para brindar el servicio.

- Los cercos perimetrales

- Los caminos de acceso que posibilitan el ingreso del personal para ejecutar tareas de inspección y mantenimiento.

Surgen como elementos extras que se incorporan al paisaje, algunos de manera transitoria, como por ejemplo:

- La extracción de tierra necesaria para la construcción de las fundaciones de los soportes y las propias bases de hormigón armado.

- La maquinaria utilizada para ejecutar la obra civil y proveer los elementos de construcción e instalación de las estaciones de base.

Un aspecto importante es el impacto visual de los soportes, el cual depende de la altura que posean, a su relación con el entorno y el fondo y a que deben respetar la Ley Nacional Nº 17.285/1967 (Código aeronáutico) y la Resolución 2194/1999 (y posteriores

modificatorias) de la Comisión Nacional de Comunicaciones, que establecen señalamiento diurno y nocturno para estas estructuras:

- Diurno: pintar estructuras en franjas alternadas con colores naranja internacional y blanco de longitudes no inferiores a 0,5 m y no mayores a 6 m (primera y última color naranja internacional).

- Nocturno: iluminación color rojo aeronáutico.

Existen soluciones que permiten reducir el impacto sobre la vista, disminuyendo la intrusión al utilizar diversos camuflajes, compartiendo estructura con otros operadores o aprovechando estructuras existentes como azoteas de edificios o tanques de agua.

6.4 Controversia social, ambiental y científica

No podíamos dejar de hacer una pequeña reseña en nuestro trabajo sobre la creciente ansiedad y especulaciones respecto a los efectos de los campos electromagnéticos (CEM) en la salud, especialmente cuando se habla de impacto social y ambiental.

Hoy en día, todas las poblaciones del mundo están expuestas a CEM en mayor o menor grado, y conforme al avance de la tecnología el grado de exposición continuará en constante crecimiento.

Como parte de su mandato de proteger la salud pública, y en respuesta a la preocupación general por los efectos sobre la salud de la exposición a CEM, la Organización Mundial de la Salud (OMS) creó en 1996 el Proyecto Internacional CEM para evaluar las pruebas científicas de los posibles efectos sobre la salud de los CEM en el intervalo de frecuencia de 0 a 300 GHz.

El Proyecto CEM se encarga de fomentar las investigaciones dirigidas a rellenar importantes lagunas de conocimiento y a facilitar el desarrollo de normas aceptables internacionalmente que limiten la exposición a CEM. A través de La Comisión Internacional de Protección contra las Radiaciones No Ionizantes (ICNIRP, 1998) y el Instituto de Ingenieros Electricistas y Electrónicos (IEEE, 2005) han elaborado recomendaciones internacionales sobre los límites de exposición para ofrecer protección contra los efectos reconocidos de los campos de RF.

Es deber de las autoridades nacionales adoptar normas internacionales para proteger a los ciudadanos de los niveles perjudiciales de RF, además, de restringir el acceso a las zonas en que puedan rebasarse los límites de exposición.

A través del Proyecto Internacional CEM, la OMS había establecido un programa para supervisar las publicaciones científicas sobre los campos electromagnéticos, evaluar los efectos en la salud de la exposición a frecuencias de 0 a 300 GHz, ofrecer asesoramiento sobre los posibles peligros de los campos electromagnéticos y determinar las medidas de mitigación más idóneas. Basándose en amplios estudios internacionales, el proyecto promovió investigaciones para subsanar la falta de conocimientos. En respuesta a ello, en los 10 últimos años, diversos gobiernos e institutos de investigación nacionales han destinado más de US$ 250 millones al estudio de los campos electromagnéticos.

Aunque nada hace pensar que la exposición a campos de RF de estaciones de base y redes inalámbricas tenga efectos en la salud, la OMS sigue fomentando las investigaciones para determinar si la exposición a la RF de los teléfonos móviles puede repercutir en la salud.

Para consultar las normas de control de emisiones dedicadas fundamentalmente a la telefonía móvil, en nuestro país rige la resolución 202/95 del Ministerio de la Salud, a fin de controlar las radiaciones no ionizantes producidas por las emisiones de las estaciones radioeléctricas que influyen en la salud humana. Dicha resolución se basó en los estándares internaciones tal como la Comisión Internacional de Protección Contra Radiaciones No Ionizantes (ICNIRP), la Unión Internacional de Telecomunicaciones (Recomendación UIT-T K-61), el Comité Electrotécnico Internacional (Norma Internacional 61566/1997), el Instituto

de Ingenieros Electrónicos y Electricistas (Norma IEEE 95.3/2002), la Guía oficial para Gobiernos Locales para la seguridad en las Antenas de la Comisión Federal de Comunicaciones de los Estados Unidos de América (FCC) y el Reglamento dictado por la Agencia Nacional de Telecomunicaciones de la República Federativa de Brasil (ANATEL).

6.4.1 Definiciones

RADIACIONES NO IONIZANTES (RNI): Son aquellas radiaciones del espectro electromagnético que no tienen energía suficiente para ionizar la materia.

INTENSIDAD DE CAMPO ELÉCTRICO (E): Es la magnitud del vector campo eléctrico expresado en unidades de volts por metro (V/m).

INTENSIDAD DE CAMPO MAGNÉTICO (H): Es la magnitud del vector campo magnético expresado en unidades de amperes por metro (A/m).

CAMPOS RE-IRRADIADOS: Son campos electromagnéticos resultantes de corrientes inducidas en un objeto secundario, predominantemente conductivo, con ondas electromagnéticas incidentes sobre el mismo desde uno o más elementos de radiación primarios o antenas.

ONDA PLANA: Onda electromagnética en que los vectores de campo eléctrico y magnético son ortogonales y están localizados en un plano perpendicular a la dirección de propagación de la onda.

REGIÓN DE CAMPO CERCANO: Es la existente en las proximidades de una antena en la que los campos eléctricos y magnéticos no constituyen sustancialmente ondas planas, sino que varían considerablemente punto a punto. La región de campo cercano se subdivide a su vez en la región de campo cercano reactivo, que es más próxima al elemento radiante y que contiene la mayor parte o casi la totalidad de la energía almacenada y la región de campo cercano radiante, en la que el campo de radiación predomina sobre el campo reactivo, pero que no es sustancialmente del tipo onda plana y tiene una estructura compleja.

NOTA: Se asume que la región del campo cercano reactivo se extiende hasta una longitud de onda de la superficie de la antena.

REGIÓN DE CAMPO LEJANO: Es la región del campo radiado por una antena, donde la distribución angular de campo es esencialmente independiente de la distancia respecto a la antena. En la región del campo lejano, el campo predominante es del tipo onda plana, es decir, distribución localmente uniforme de la intensidad de campo eléctrico y de la intensidad de campo magnético en planos transversales a la dirección de propagación. El campo lejano comienza a partir de una distancia de la antena dada por el valor que resulte mayor entre 3λ y 2D2/λ, siendo λ la longitud de onda y D la mayor dimensión de la antena.

DENSIDAD DE POTENCIA (S): Es la potencia por unidad de área normal a la dirección de propagación. La unidad utilizada es el mW/cm2. Para una onda plana la densidad de potencia está relacionada con el campo eléctrico y el magnético por la impedancia del espacio libre (Zo = 377 Ω).

S = E2/Zo = H2Zo

EMISIÓN: Es la radiación producida por una única fuente de radiofrecuencia.

INMISIÓN: Es la radiación resultante del aporte de todas las fuentes de radiofrecuencias cuyos campos están presentes en el lugar.

EXPOSICIÓN: Es la situación en que se encuentra una persona sometida a campos eléctricos, magnéticos, electromagnéticos o a corrientes de contacto o inducidas asociados a campos electromagnéticos de radiofrecuencias.

EXPOSICIÓN POBLACIONAL O NO CONTROLADA: Corresponde a situaciones en las que el público en general puede estar expuesto o en las que las personas expuestas como consecuencia de su trabajo pueden no haber sido advertidas de la potencial exposición y no pueden ejercer control sobre la misma.

MÁXIMA EXPOSICIÓN PERMITIDA (MEP): Valor eficaz de campo eléctrico, magnético o de densidad de potencia equivalente a onda plana, a los que las personas pueden estar expuestos sin efectos perjudiciales y con un aceptable factor de seguridad.

PROMEDIO TEMPORAL: Promedio de las mediciones de exposición obtenidas durante un período de tiempo apropiado con el fin de determinar el cumplimiento de los límites.

POTENCIA RADIADA APARENTE (PRA): Producto de la potencia suministrada a la antena por la ganancia de antena, en una dada dirección, relativa a un dipolo de media onda.

POTENCIA ISOTRÓPICA RADIADA EQUIVALENTE (PIRE): Producto de la potencia suministrada a una antena por la ganancia de antena, en una dada dirección, relativa al radiador isotrópico.

TASA DE ABSORCION ESPESIFICA (SAR): es la medida de la cantidad de energía de RF que es absorbida por los tejidos del cuerpo humano y se expresa en W/kg. Las recomendaciones ICNIRP consideran dos tipos de SAR dentro de las restricciones básicas. El SAR de cuerpo entero que se produce en una persona por acción de las ondas emitidas por una estación base, y el SAR localizado que es el que se aplica para determinar si un teléfono móvil cumple con las recomendaciones de seguridad.

6.4.2 Valores limites

La presente tabla muestra la máxima exposición permitida poblacional, en función de la frecuencia de acuerdo con la resolución N°202/95 del ministerio de salud y acción social de la nación.

Rango de Frecuencia f (MHz)	Densidad de Potencia equivalente de onda plana S (mW/cm^2)	Campo Eléctrico E (V/m)	Campo Magnético H (A/m)
0,3-1	20	275	0,73
1-10	$20/f^2$	275/f	0,73/f
10-400	0,2	27,5	0,073
400-2.000	f/2000	$1,375f^{1/2}$	-
2.000-100.000	1	61,4	-

6.4.3 Caso real de medición

Para constatar los valores de exposición se obtuvieron los resultados de una medición de una estación base de la ciudad de Córdoba. Los valores de la misma corresponden a la medición de inmisión de densidad de potencia de radiación electromagnética total en el rango de 100 KHz y 3 GHz.

Solo para mencionar, si se considera una de la frecuencias de la estación base, por ejemplo la frecuencia de 850MHz, el límite de exposición estaría dado por

850/2000 = 0.425 mW/cm2

Punto de medición	Distancia [m]	Azimut [°]	Altura [m]	Valor de medición [µW/cm2]	Máximo admisible [µW/cm2]
1	10	0	1,8	0,157	200
2	10	300	1,8	0,171	200
3	10	240	1,8	0,069	200
4	10	180	1,8	0,061	200
5	10	120	1,8	0,24	200
6	10	60	1,8	0,147	200
7	40	0	1,8	0,269	200
8	50	300	1,8	0,226	200
9	70	240	1,8	0,058	200
10	55	180	1,8	0,098	200
11	50	120	1,8	0,186	200
12	50	60	1,8	0,26	200
13	70	120	1,8	0,301	200
14	100	180	1,8	0,047	200
15	120	220	1,8	0,382	200
16	180	280	1,8	0,162	200
17	150	190	1,8	0,172	200
18	150	300	1,8	0,22	200
19	100	290	1,8	0,24	200
20	60	0	1,8	0,261	200
21	100	60	1,8	0,627	200
22	150	80	1,8	0,538	200
23	200	120	1,8	0,345	200
24	150	0	1,8	0,517	200
25	60	0	9	19,52	200
26	100	290	9	29,45	200
27	150	300	9	29,66	200
28	70	120	9	46,45	200
29	100	180	9	63,48	200
30	130	220	9	41,54	200
31	170	280	9	19,59	200
32	150	190	9	23,16	200
33	200	120	9	21,11	200
34	150	80	9	22,08	200
35	100	60	9	60,03	200
36	120	0	9	33,94	200

Los resultados obtenidos demostraron que los niveles de densidad de potencia de radiación electromagnética registrado al momento de la medición se encuentran ampliamente por debajo de

los valores máximos establecidos por Resolución N° 202/95 del Ministerio de Salud y Acción Social de la Nación.

CONCLUSIÓN

Como se ha mencionado a lo largo de este trabajo, la demanda de tráfico en las redes 3G fue ascendiendo y paulatinamente se absorbió mediante incrementos de capacidad de enlaces E1 PDH. Sin embargo, el crecimiento exponencial en la demanda de tráfico de datos y una alta proyección a futuro, no podría ser tolerado por la actual red TDM, lo que generó la necesidad de buscar nuevas soluciones.

Cada componente de la red se ha visto en la obligación de ir evolucionando, como la interfaz de aire entre usuarios y estación base, que debió incrementar su cantidad de portadoras como también soportar una diversidad de servicios GPRS, EDGE, HSPA, etc

La interfaz de acceso a la red utilizó los protocolos de conmutación de paquetes como ATM e IP, basándose sobre la tecnología Ethernet para el transporte de los mismos, por su alta capacidad, flexibilidad y bajo costo, además de ser un estándar universal. En cuanto a la red troncal, se optó por MPLS, el cual es compatible con IP y además posee capacidad para transportar diferentes protocolos y permitir tanto QoS e ingeniería de tráfico, que hoy en día un factor importante al permitir priorizar los paquetes de mayor importancia. Esto dio la posibilidad de obtener mayor rapidez en la conmutación que se ofrecía en capa 2 pero con el encaminamiento inteligente de una capa 3, IP.

Se preveía migrar toda la red troncal a MPLS conectando como primera instancia a través de fibra óptica por su mayor capacidad de trasmisión. Como segunda opción se elegían radio enlaces con disponibilidad de puertos Ethernet/Gigaethernet. Siempre fue importante destacar que el espectro radioeléctrico es limitado, por lo que para nuestro caso hay que hacer un uso eficiente del mismo.

La principal intención, es preparar una red puramente IP, para que llegado el momento de implementar LTE, la transición pudiera realizarse en forma directa aprovechando la infraestructura existente, sin la necesidad de montar una red paralela y evitando formar cuello de botellas causados por el traspaso de la información entre diferentes tecnologías. La convergencia hacia una única tecnología habría llevado a un ahorro en los costos operativos, al no tener que disponer de personal especializado para cada una de ellas.

En la implementación de LTE, la red 3G indirectamente se vio mejorada por el incremento en su ancho de banda en el enlace final y en Core de la red, al ampliarse la capacidad -al tener más ancho de banda disponible- pudo funcionar a mayor velocidad, es decir, mejorando el acceso en HSPA y HSPA+. Mientras tanto, la tecnología 2G continúa y continuará en vigencia para zonas poco urbanizadas, esta tecnología no desaparecerá, sino que mediante códigos Pseudowires (PWE3) se integro al tráfico IP MPLS, atravesando la red hasta la RNC donde será procesado y desencapsulado.

En cuanto a la operación y el mantenimiento, se facilita, utilizando protocolo de mensaje ICMP, pudiendo encontrarse todos los equipos dentro del dominio IP, verificando su conexión o ruta mediante un simple “ping” a la dirección IP del equipo. Además puede trazarse la ruta del paquete hacia los equipos utilizando el campo TTL de la cabecera del protocolo IP mediante el comando “Traceroute” o "Tracert". Una ventaja importante, es que permite realizar cambios o correcciones en forma remota mediante un Gestor de propietario o un browser, detectando, controlando y realizando estadísticas en forma remota. De esta manera se logra un importante ahorro en el mantenimiento de servicios al no tener que disponer de personal que este constantemente asistiendo a la celda.

Un punto a destacar sobre esta implementación es que si bien fue diseñada como una instancia previa para facilitar el paso de UMTS a LTE, existieron realidades ambiguas que no eran coherentes y afectaban directamente a la evolución tecnológica. Teníamos en nuestro país políticas económicas que dificultaban las importaciones de tecnologías y las inversiones (las empresas proveedoras de servicio móvil de nuestro país son principalmente de capitales externos, y sus proveedores si eran enteramente de capitales externos). Mientras que por otro lado las estrategias de markenting y venta de las telefónicas no iban de la mano con los tiempos de implementación de la tecnología. Esto tuvo como consecuencia implementar LTE en forma abrupta y no como una red escalonada y convergente.

Como conclusión desde nuestro punto de vista personal, podemos decir que este trabajo nos ha brindado conocimientos técnicos, que conjuntamente con nuestros actuales actividades, nos permiten crecer profesionalmente y nos ha brindado una perspectiva global de varios aspectos que desconocíamos y que están incluidos en la evolución tecnológica de nuestro rubro.

Para el desarrollo de este trabajo, ambos nos hemos tenido que involucrar en cada uno de sus trabajos mas alla de los cotidiano y buscar fuentes de conocimiento para desarrollar varios temas aquí expuestos. Esto nos ha permitido enriquecernos tanto en

conocimiento como tambien afianzar todo lo que hemos aprendido a lo largo de nuestra carrera universitaria.

BIBLIOGRAFIA

- REDES UMTS. Tomás González, Bolivar Ortiz, Carlos Bonilla. Universidad Abstract https://ehumir.files.wordpress.com/2013/04/articulo-redes-umts.pdf
- Tecnologías del Siglo XXI. Tema 4.- Telefonía Móvil. Pedro M. Ruiz Martínez - http://www.um.es/aulasenior/saavedrafajardo/apuntes/doc/telefonia.pdf
- Yañez René: "Nuevas Técnicas de Redes de Transporte". XIII Convención y feria internacional Informática 2009. Febrero del 2009.
- Jose Manuel Huidobro Moya, "Redes y servicios de telecomunicaciones", Cuarta Edición, Paraninfo, 2006
- HSPA_evolution_white_paper_low_res_141220 - Copyright © 2010 Nokia Siemens Networks. All rights reserved.
- N.S. Networks, Flexi Packet Microwaves Radio: http://www.nokiasiemensnetworks.com/portfolio/products/transport-networks/microwave-transport/flexipacket-microwave
- ITU – Standardization of IMT – 2000 and System Beyond: http://www.itu.int/ITU-T/worksem/asna/presentations/Session_6/asna_0604_s6_p2_jc.pdf
- Mobile Backhaul: http://metroethernetforum.org/
- Estudio de Internet Móvil 3G (UMTS) https://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCoQFjAA&url=http%3A%2F%2Fbibdigital.epn.edu.ec%2Fbitstream%2F15000%2F2787%2F1%2FCD-0600.pdf&ei=b9l3U_fnJ9fesASSqYII&usg=AFQjCNFfmEXLjSdw9tNv7GQLnR2AcD-0Kw
- TESIS: MEDICION Y ANALISIS DE TRAFICO EN REDES MPLS - Javier Igor Doménico Luna Victoria García – UNIVERSIDAD CATOLICA DEL PERU
- REDES Y SERVICIOS DE TELECOMUNICACIONES, JOSE MANUEL HUIDORO MOYA, TERCERA EDICION, PARANINFO.

- GUIA DE ESTUDIO PARA CERTIFICACION CCNA 640-802, ERNESTO ARIGANELLO, PRIMERA EDICION, ALFAOMEGA – RA-MA
- ARTICULO IP sobre ATM - clave en la convergencia de las comunicaciones, Homero Ortega Boada, Carolina Villabona R., Wilder E. Castellanos H
- Cisco Systems. MPLS and IP Quality of Service in Service Provider ATM Networks. 2000.
- Redes Inalámbricas –Universidad de Oviedo: http://www.isa.uniovi.es/docencia/redes/Apuntes/temaWLAN.pdf
- TESIS: ESTUDIO DE LOS PROTOCOLOS DE ENRUTAMIENTO DE INTERNET Y SU UTILIZACIÓN EN LA ARQUITECTURA DE RED MPLS - Guas Ojeda, Daliah Sahily - Universidad Central de Venezuela
- REDES DE COMPUTADORAS – Tenenbaum – 3ra edición – Prentice hall 1997