Tema 3 – Redes NGN

NGN…

¿Qué son las Redes NGN? ¿Cuáles son sus características?

¿Qué servicios proporcionan estas redes? ¿Cómo lo hacen?

¿A que hace referencia VoIP? ¿En qué consiste?

¿A que hace referencia IPTV? ¿En qué consiste?

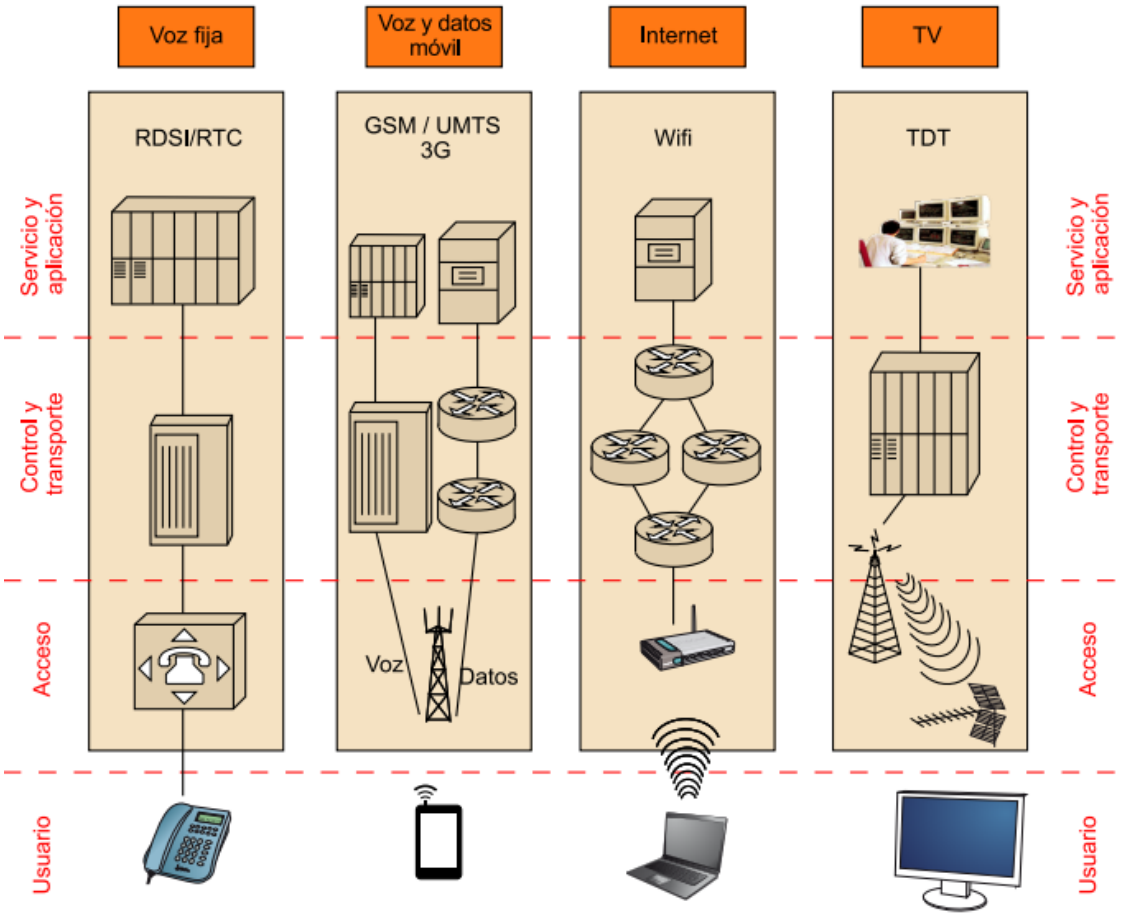
El conjunto de sistemas, tecnologías y protocolos que deben permitir emplear Internet en cualquier dispositivo, en cualquier lugar, momento y situación, es lo que denominamos redes de nueva generación (next generation networks, NGN). Las NGN son redes de banda ancha que permiten la integración de servicios de datos, voz y vídeo mediante el desarrollo de los protocolos de Internet.

De acuerdo a definiciones de la ITU-T, las redes de nueva generación NGN son:

"Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios."

Las redes de nueva generación buscan una integración de redes de voz, datos y vídeo, que utilice una tecnología en modo de transporte de paquetes (como IP) para toda clase de información. La red debe garantizar una calidad de servicio (QoS) para distintos tipos de tráfico y niveles de prioridad de datos, como el vídeo y la voz en tiempo real. Además, se quiere separar totalmente el plan de gestión de la red (señalización y control) del plan de conmutación y transporte, utilizando interfaces abiertas y estándares que permitan un despliegue rápido de todos los servicios, la posibilidad de que terceras entidades puedan crear fácilmente nuevos servicios a la vez que se mantienen los servicios tradicionales.

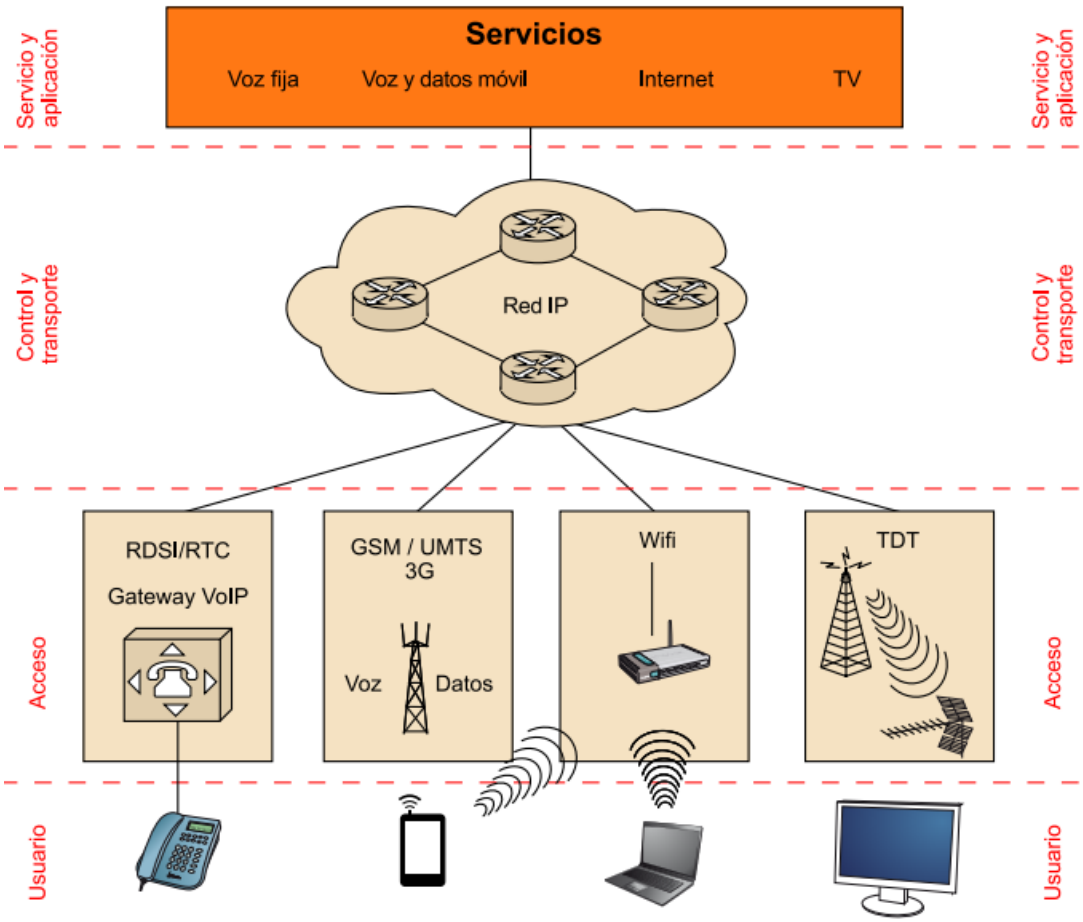
Hasta ahora, las redes y servicios de telecomunicaciones que los usuarios podían utilizar tenían una infraestructura dedicada que iba desde el propio terminal de usuario hasta la infraestructura que proveía el servicio en sí. **A esto se le llama estructura en forma de silo, donde cada red de acceso solo ofrece un tipo de servicio sin ninguna clase de integración entre ellas.** Por ejemplo, las redes de par de cobre para proporcionar el servicio telefónico básico y las redes de cable coaxil para proporcionar servicio de televisión. La única manera de hacerlas compatibles entre sí es mediante pasarelas dedicadas tanto a señalización como a tráfico útil.



Esta arquitectura obliga a mantener una infraestructura exclusiva para cada servicio, incrementando considerablemente los costes de mantenimiento y operación del operador y proveedor de servicio.

En contados casos se produce una leve integración de dos redes de acceso en un mismo servicio, como por ejemplo el caso del servicio de voz fija y móvil, cuyas infraestructuras están interconectadas para permitir llamadas de voz entre ambas redes de acceso. Aun así, la tónica general es la de cierto aislamiento entre redes en todos los niveles (usuario, control y gestión). Este hecho también afecta a la escalabilidad en el ofrecimiento de nuevos servicios, los cuales requerirían de su propia infraestructura en forma de silo.

El cambio de paradigma introduce el concepto de “una sola red para muchos servicios” (como se presenta en la imagen a continuación) en contradicción con la filosofía de la anterior arquitectura de referencia, cuyo concepto es el de “una red para un servicio”.



Las principales características de las NGN se pueden resumir en los siguientes puntos:

- Redes basadas en la conmutación de paquetes.
- La arquitectura de red consiste en una capa de transporte, control de servicios y aplicación totalmente separados e independientes. Las redes de acceso de diferentes tecnologías deben ser capaces de interconectarse a través de redes de internet. **Se plantea una convergencia en capa de transporte.**
- Utilización de interfaces abiertas (estándares abiertos).
- Integración de diferentes servicios.
- Capacidad de banda ancha con calidad de servicio extremo a extremo.
- Integración con las redes actuales.

Desde un punto de vista técnico, el término NGN engloba los siguientes elementos:

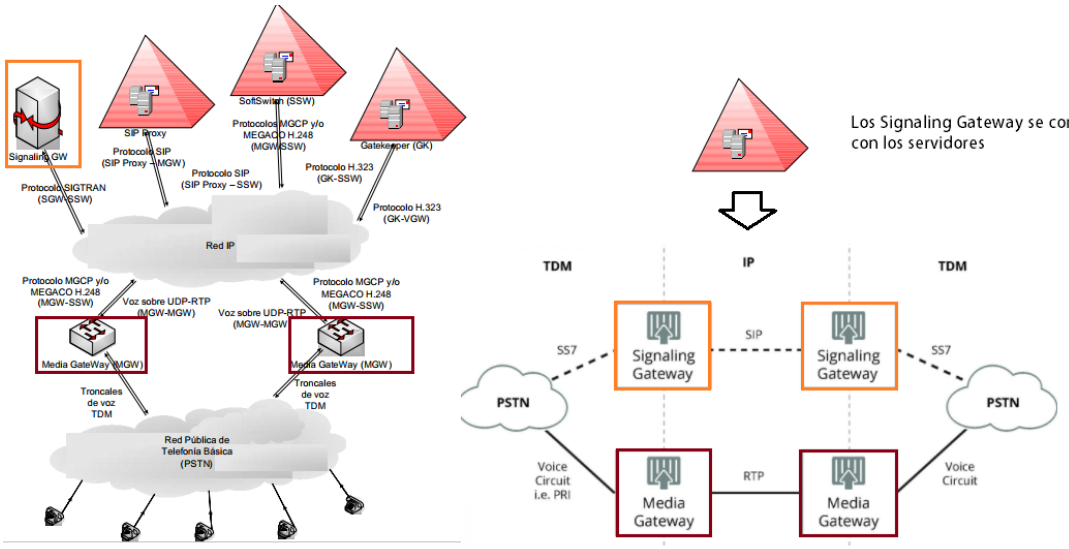
- Las redes de acceso de nueva generación, es decir, el desarrollo de tecnologías en el bucle de abonado para proporcionar alta velocidad y garantizar la entrega de los nuevos servicios. **Redes de telefonía clásica utilizan ADSL y redes de CATV utilizan cablemodem.**
- El núcleo de la red, que evoluciona como una infraestructura IP capaz de contener una multitud de servicios de vídeo, datos, etc.

Sobre las mismas redes NGN se puede brindar servicio Triple Play (telefonía, video y datos -internet-). Las nuevas tecnologías que permiten esto son las que se dan sobre plataformas IP. Las principales son: VoIP (Voz sobre IP), ToIP (Telefonía sobre IP) e IPTV (Televisión por IP).

La mayoría de las veces suele confundirse los servicios sobre VoIP con ToIP, ¿Cuál es la diferencia? Básicamente, VoIP es un servicio orientado a utilizarse sobre redes LAN y ToIP es un servicio orientado a ser utilizado sobre redes WAN.

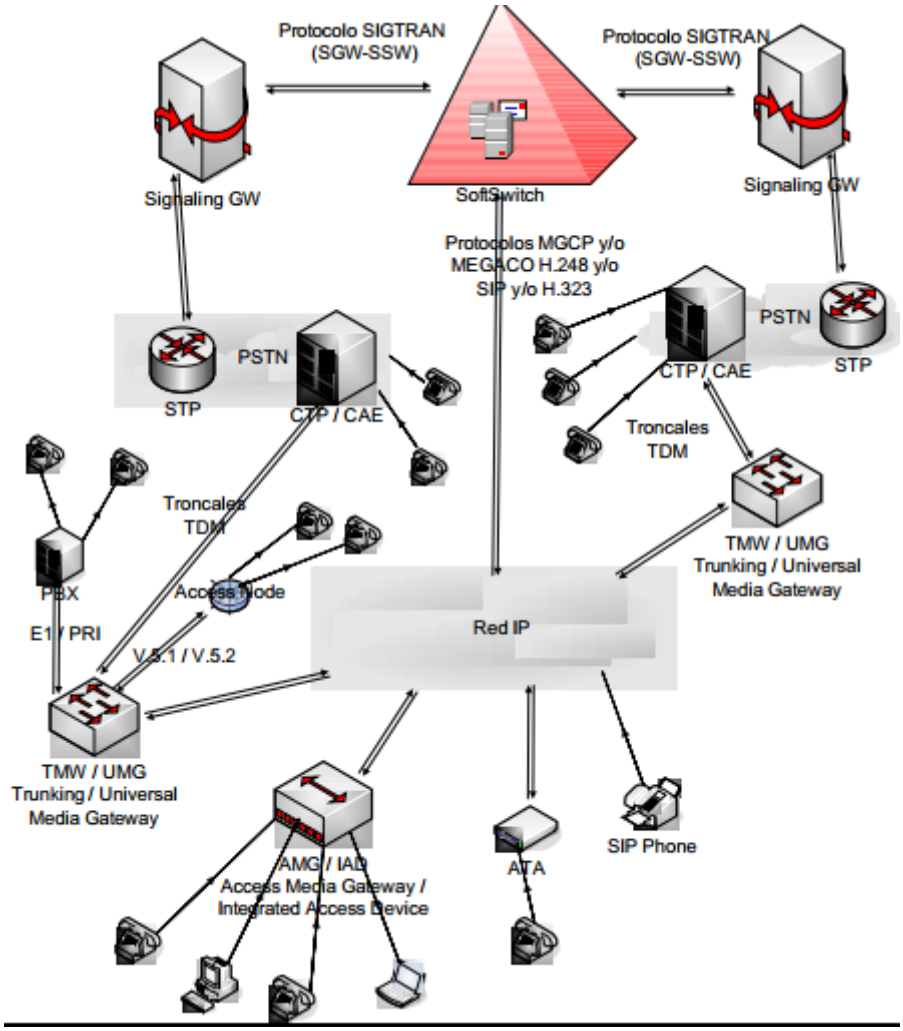
La voz sobre redes IP (VoIP – Voice over IP) inicialmente se implementó para reducir el ancho de banda mediante compresión vocal y en consecuencia para disminuir los precios en el transporte internacional. Inicialmente, toda la arquitectura de red (servidores) para proporcionar el servicio, se implementaba sobre una red LAN. Con posterioridad se migro de la LAN a la WAN con la denominación de la telefonía sobre IP (ToIP – Telephony over IP). La telefonía sobre IP supone una implementación mucho más compleja que VoIP.

- Las redes ToIP deben permitir la interoperabilidad con las redes telefónicas actuales y sus servicios agregados. Este tipo de servicios generalmente son proporcionados por redes PSTN que soportan señalización SS7 y redes inteligentes.
- Las redes ToIP plantean la existencia de un backbone de alta velocidad no bloqueante para garantizar calidad de servicio mediante herramientas de QoS. En este sentido, VoIP no tiene calidad de servicio asegurada.
- Cuando se habla de ToIP se refiere a una aplicación publica, donde el principal problema es la interoperabilidad entre redes.
- En Telefonía sobre IP se aplica el concepto ***carrier-grade.*** Que incluye aspectos como redundancia de equipamiento que permitan la máxima disponibilidad, calidad vocal (bajo retardo, jitter, errores, eco y demás), disponibilidad de servicios (valor agregado en redes PSTN mediante señalización SS7 en la IN (*inteligent Network*)).



Vemos claramente que es necesario algunos dispositivos que permitan vincular las redes de conmutación de circuitos con las redes de conmutación de paquetes (*Media Gateway y Signaling Gateway*) ya que es necesario mudar de un mundo a otro, todo lo relacionado con las señalizaciones (Signaling Gateway) y datos (Media Gateway). Además, se necesitan dispositivos controladores a nivel de red IP para proporcionar servicio de telefonía. ¿Por qué? Porque en la actualidad existen teléfonos IP que funcionan directamente sobre redes de conmutación de paquetes y estos dispositivos también deben tener la posibilidad de comunicarse con otros dispositivos IP o analógicos como los convencionales. Además, se utiliza la infraestructura de red de internet para emular un bucle de abonado que permita dar acceso al servicio de telefonía.

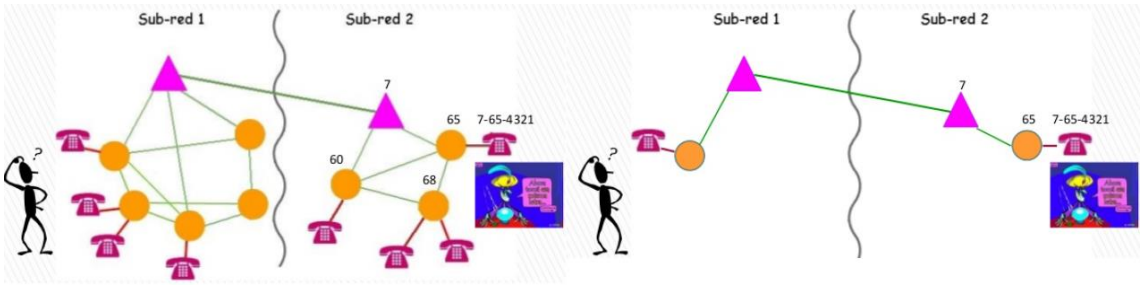
Estos equipos en la siguiente imagen aparecen como (IAD –Integrated Access Device, RGW – Residential Gateway, AGW – Access GateWay).



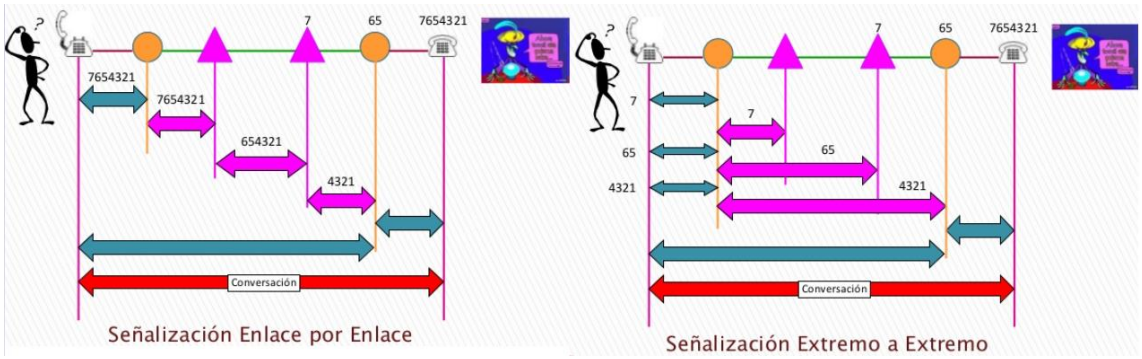
Todos los elementos mencionados anteriormente, es decir, todo este sistema presente en el mundo IP tiene como propósito funcionar de manera análoga al sistema de telefonía convencional, es decir, emular una central telefónica convencional. ¿Cómo funciona esto? Básicamente, en los sistemas de telefonía convencional podemos diferenciar dos servicios:

- Tráfico de voz de las diferentes llamadas.
- Trafico de señalización de las llamadas.

En las redes telefónicas, cuando el abonado disca un determinado número de teléfono, el CAE (“Switch de PSTN” o centro con autonomía de encaminamiento) dialoga o comparte información con el CTP (centro de transito principal), en el caso de que el número de destino de la llamada pertenezca a otro bucle de abonado asociada a otra central telefónica. ¿Cómo nos damos cuenta de esto? Gracias al sistema de numeración telefónica, que está basado en códigos de área. Si el número de destino no posee código de área, se interpreta que la llamada va dirigida a un usuario dentro del mismo bucle de abonado.

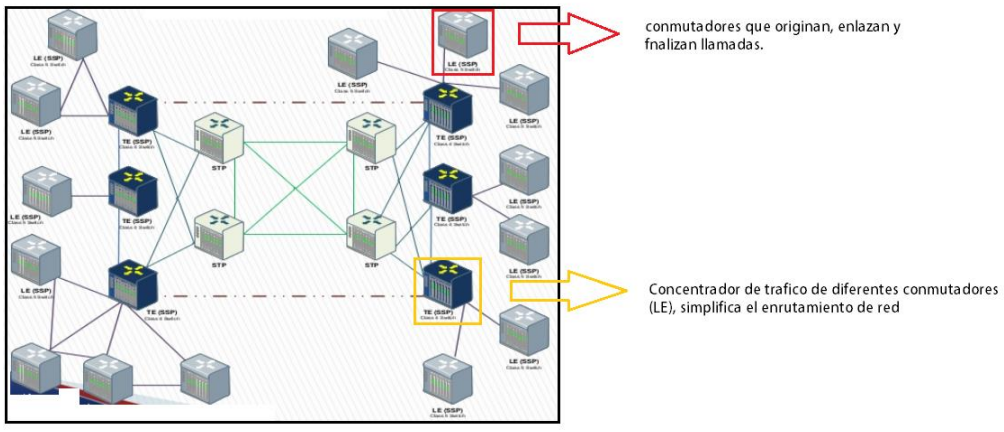


También podemos pensarlo de la siguiente manera:



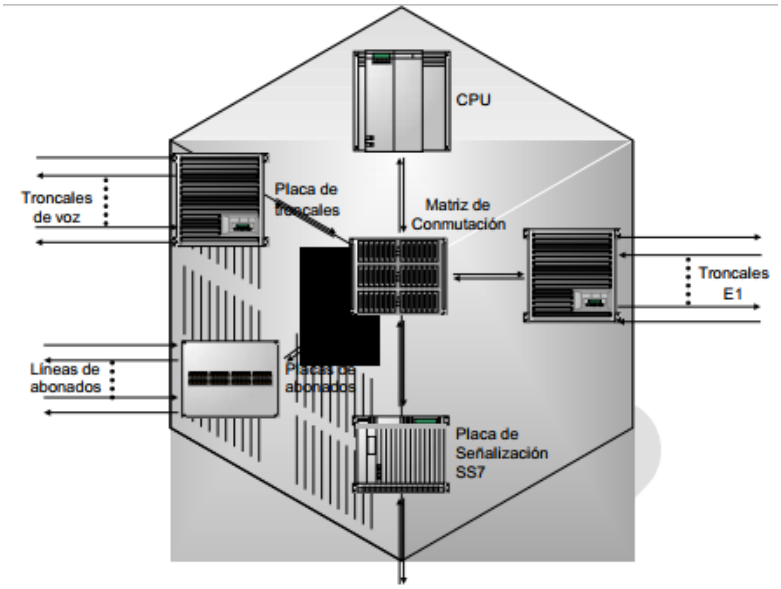
Esta comunicación utiliza por lo general señalización SS7 (*Signaling System N 7*) donde uno o más canales son dedicados puramente a transportar información de señalización de todas las llamadas. SS7 está basado en mensajes. Si el intercambio de mensajes SS7 es el adecuado, entonces la comunicación de voz podrá realizarse sobre los circuitos de voz utilizando los diferentes troncales y enlaces locales. Sin embargo, no es la única forma de señalizar. Existen centrales que utilizan CAS (*Channel Associated signaling*) que por el mismo vinculo donde mandan datos de voz también mandan datos de señalización. El ejemplo típico son los enlaces E1 con 30 canales de voz y 1 canal o time slot de señalización, famoso time slot 16. En las redes que utilizan la señalización SS7 cada entidad que maneja señalización puede constituirse como:

- **SSP (Service Switching Point)** – Modulo de señalización para con otras centrales.
- **STP (Signaling Transfer Point)** – Modulo especializado únicamente en señalización. Su finalidad es optimizar el uso de red, eliminando la necesidad de enlaces directos entre centrales.
- **SCP (Service control Point)** – Constituye un nodo de control dentro de la red SS7, el cual permite el acceso desde todos los conmutadores de la red a servicios implementados en determinadas entidades mediante mensajes de señalización especiales.

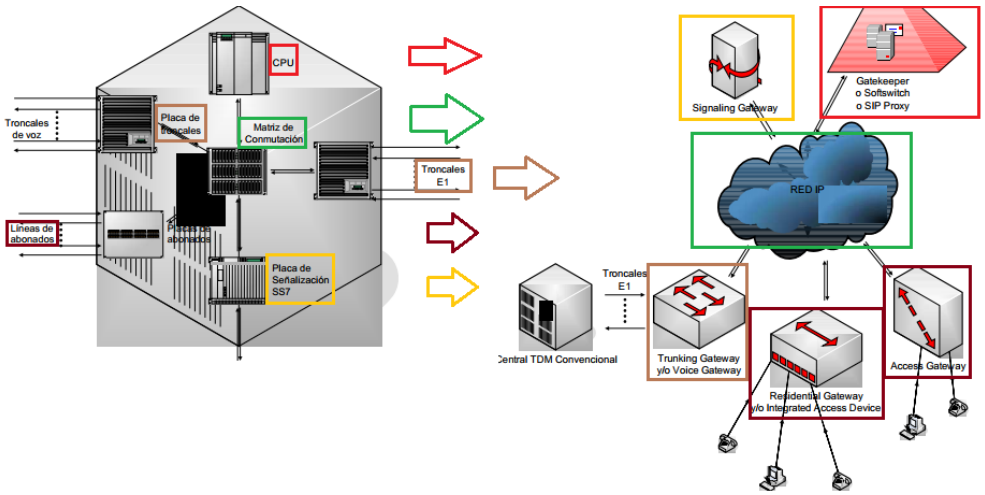


Cada una de las centrales de conmutación está compuesta por los siguientes elementos:

- **Matriz de conmutación**
- **Procesador central (CPU)**
  - Es el administrador y controlador de todo lo que pasa en la central.
- **Módulos de troncal**
  - Brinda interfaces E1 para conectarse con otras centrales.
- **Módulo de abonados**
- **Módulo de señalización**



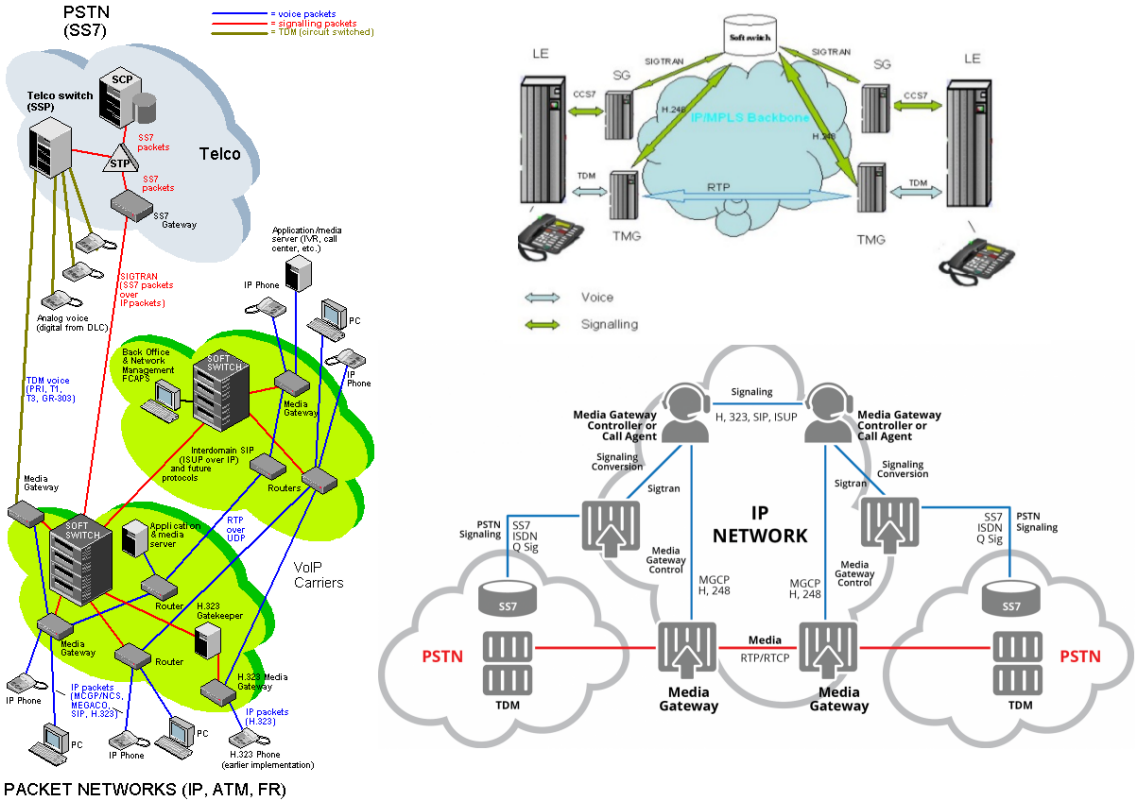
Mientras se da la transformación a **todo IP,** la red de VoIP pretende mantener el esquema anterior de una manera más o menos análoga.



Como puede observarse en la imagen anterior, existen muchas tecnologías y protocolos que permiten ofrecer señalización para el servicio de ToIP (H. 323, SIP), para el tráfico de voz sobre redes IP, se utiliza RTP (*Real time protocol*) junto con protocolo de transporte UDP. También, se hace presente RTPC (*Control RTP*) para el envió de datos de control y datos de medición de las transmisiones realizadas.

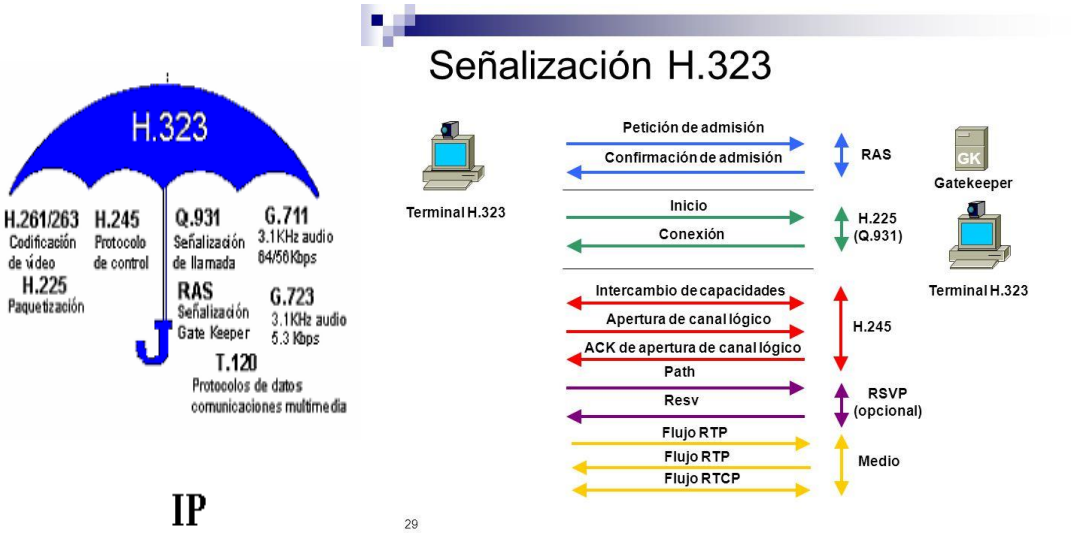
El Softswitch es el principal dispositivo en la capa de control dentro de una arquitectura NGN (Next Generation Network), encargado de proporcionar el control de llamada (señalización y gestión de servicios), procesamiento de llamadas, y otros servicios, sobre una red de conmutación de paquetes (IP). Actúa como gestor en el momento de interconectar las redes de telefonía tradicional, e incluso las redes inalámbricas 3G con las redes de conmutación de paquetes (IP), buscando como objetivo final lograr la confiabilidad y calidad de servicio similar a la que brinda una red de conmutación de circuitos con un menor precio.

Desde el punto de vista de VoIP, se suele considerar al softswitch como el Proxy o elemento de registro en el protocolo SIP o como el Gatekeeper en H.323. También se lo puede asociar cuando se habla de un MGC (Media Gateway Controller) en MGCP y MEGACO.



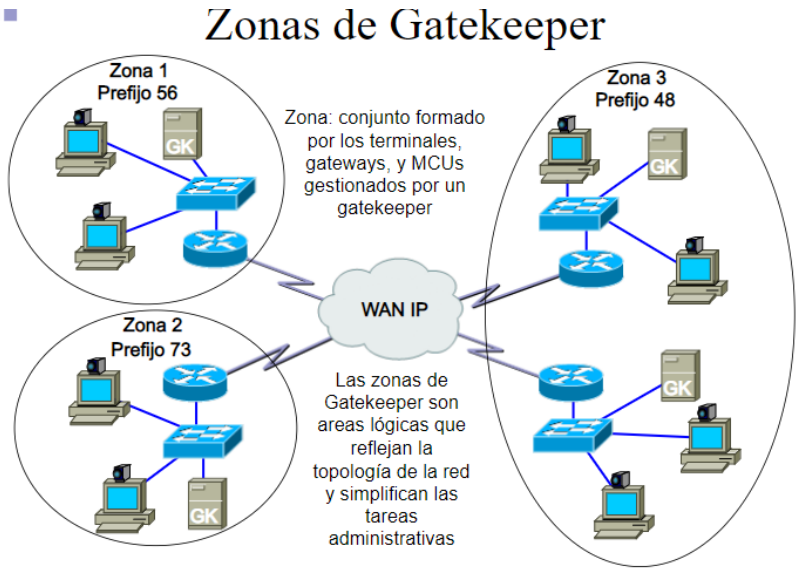
PACKET NETWORKS (IP, ATM, FR)

El protocolo H.323 es un conjunto de normas (recomendaciones de protocolos, por eso se sabe decir que es un paraguas) ITU para **comunicaciones multimedia** que hacen referencia a los protocolos utilizados para la construcción de terminales, equipos y servicios estableciendo una señalización en redes IP.

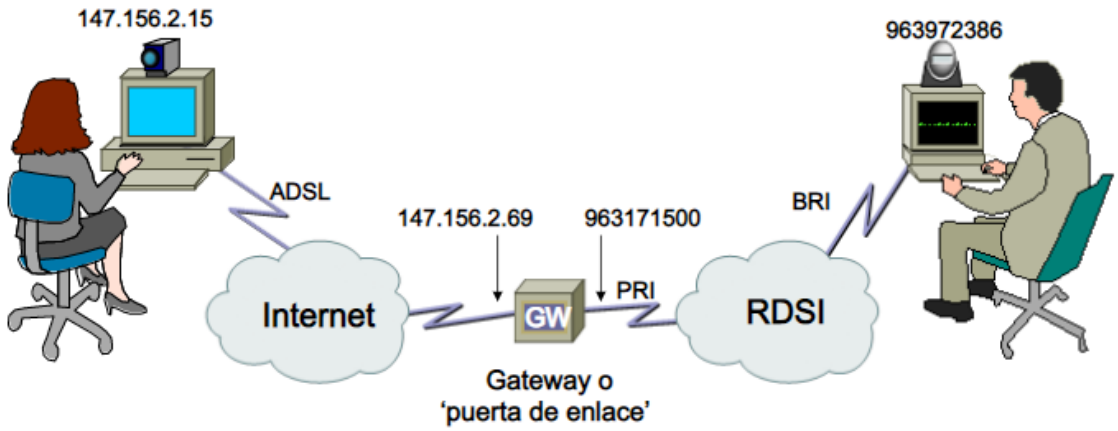


Como podemos observar en las imágenes anteriores, el protocolo **RAS** permite la comunicación entre un dispositivo **terminal H.323** y un **Gatekeeper** para realizar acciones tales como: Registración, control de admisión, control de ancho de banda, estado y desconexión. ¿Qué son los terminal H.323 y Gateekeper? En primer lugar, un terminal H.323 es un extremo de la red

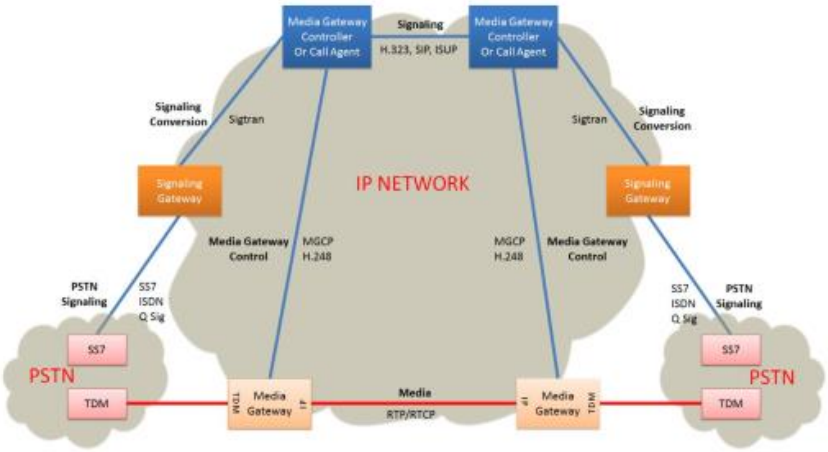
que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, Gateway y Gatekeeper. Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo. Un Gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, Gateways y MCUs (Unidad de control multipunto – llamadas en grupo). El gatekeeper también proporciona otros servicios a las terminales H.323 como por ejemplo la localización de los diferentes Gateways, así como también, controles de ancho de banda para limitar el número de conferencias/llamadas simultaneas que pueden llevarse a cabo, rechazando las nuevas solicitudes. Puede realizar control de admisión, lo que significa que es capaz de rechazar llamadas procedentes de un terminal por ausencia de autorización a diferentes terminales de destino o Gateways particulares de acceso restringido o en determinadas franjas horarias. Además, lleva a cabo el registro y la admisión de los terminales y gateways de su zona. Conoce en cada momento la situación de los Gateways existentes en su zona que encaminan las conexiones hacia terminales RCC.



Hablamos mucho de Gateways ¿Qué es? Un Gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada.



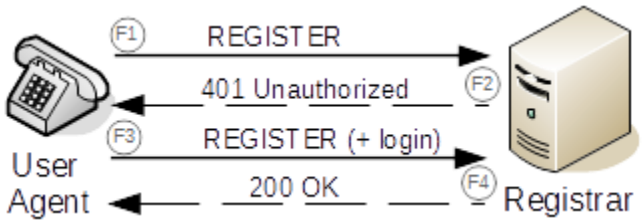
En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. Estos conceptos son generales, porque para constituir un Gateway se necesitan 2 equipos, uno de ellos definido como *Signaling Gateway,* que transforma la información de señalización SS7 en mensajes correspondientes al protocolo H.323 ó protocolo SIP, dependiendo cual se implemente, que permitirá comunicarse con el GateKeeper ó los servers SIP. Además, está presente junto al Signaling Gateway, el *Trunking Gateway* que transforma los enlaces troncales de datos de la PSTN a paquetes RTP direccionados hacia un terminal de destino o Gateway de otra PSTN.



Si seguimos con los procedimientos para el establecimiento de una comunicación, encontramos que posteriormente a la utilización del protocolo RAS entre el terminar H.323 y el Gatekeeper, el terminal H.323 utiliza el protocolo H.225 para invitar al otro extremo terminal a formar parte de la sección multimedia. El protocolo H.225 se utiliza para el establecimiento de la llamada, así como también para su finalización. Posteriormente, el protocolo H.245 se ocupa de negociar las capacidades (ancho de banda) intercambiadas, de la apertura y cierre de los canales lógicos y de los mensajes de control de flujo. En cada llamada, se puede transmitir cualquier número de canales lógicos de cada tipo de medio (audio, video, datos) pero solo existirá un canal lógico de control, el canal lógico 0. Luego, se produce el intercambio de datos utilizando el protocolo RTP.

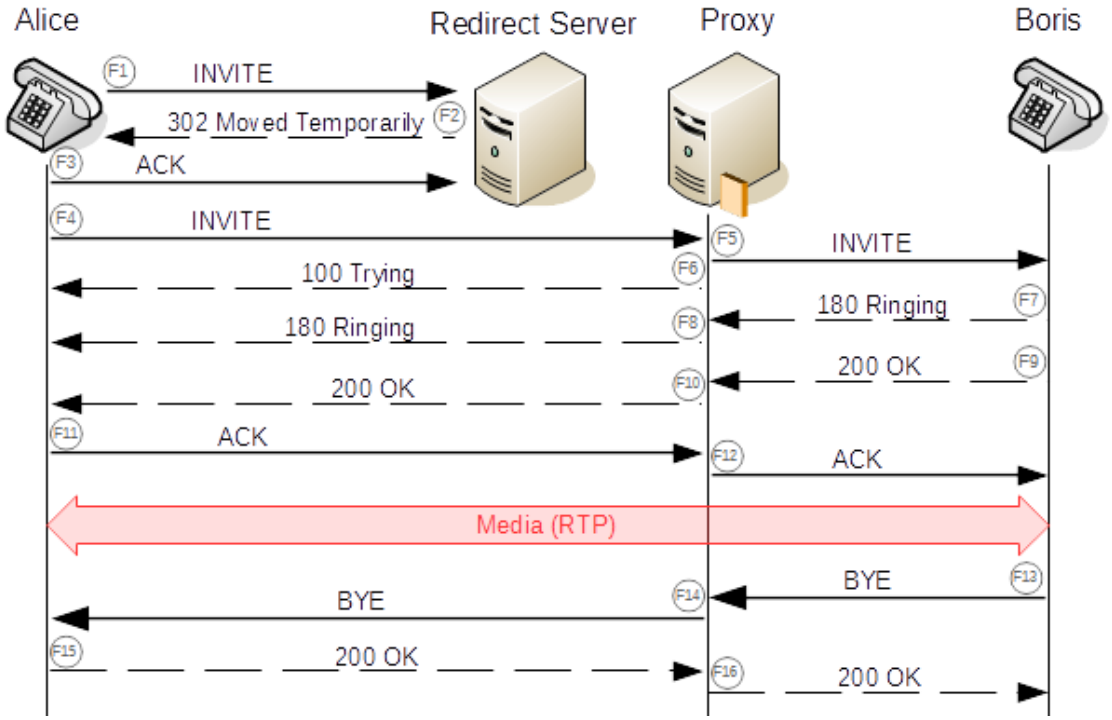
Otros de los protocolos posibles de implementar dentro de lo que resulta la señalización en el mundo de las redes IP es SIP (*Session Initiation Protocol*). Este protocolo se basa en la arquitectura cliente-servidor y es utilizado para generar mensajes de invitación a una sección

multimedia, registración de usuarios y demás. Es un protocolo basado en texto y mensajes, esto significa que para cada acción realizada se utiliza un comando y posteriormente argumentos que permiten al cliente comunicarse con el servidor. Como respuesta el servidor entrega códigos de estado para informar al cliente del resultado de la operación. Como en H.323 se utilizaban Gatekeeper, en SIP se utilizan servidores como: **SIP Server** y **SIP Proxy**. Ambos pueden estar contenidos en un único servidor, pero tienen funciones diferentes. El SIP Server es una aplicación o dispositivo que permite crear y gestionar cuentas SIP y permitir que los Usuarios SIP se «registren» almacenando la dirección IP donde deben acceder para realizar la comunicación con este usuario.



El SIP Proxy es una aplicación que permite que cualquier usuario SIP envíe un comando a otro usuario SIP, obviamente ambos registrados.

La dirección usada en SIP se basa en un localizador URL (Uniform Resource Locater) con formato SIP "roberto@192.190.132.31" (o mediante el dominio Domain: teleinfo.com.ar), de forma que SIP integra su servicio a la Internet. En este modelo se integra un server de resolución de dominio DNS (Domain Name Server). SIP incorpora también funciones de seguridad y autentificación, asi como descripción del medio mediante SDP. Para el proceso de facturación billing se puede recurrir a RADIUS y RSVP.



El Redirect server permite identificar cuando un usuario SIP que se encuentra registrado, ha cambiado su dirección IP y necesita ser atendido por otro servidor Proxy. Luego, el usuario SIP envía mensajes al Proxy SIP necesario para alcanzar el usuario de destino. No hace falta aclarar

de que se tratan los comandos, si por ahí prestar atención a los datos o argumentos que acompañan a dicho comando.

Cambiando un poco de tema, Respecto a IPTV (Televisión por IP), ¿Por qué tiene relevancia dentro de las redes NGN? Porque dicha tecnología constituye el último paso para generar una integración completa de múltiples servicios multimedia interactivos (Voz, TV, Datos) en las redes IP. La tendencia de la que se habla en este momento es que todos los servicios estarán basados en el protocolo IP y el usuario final podrá acceder a ellos a través de una conexión de banda ancha ofrecida por cualquier proveedor de telecomunicaciones. ¿Qué significa esto? Que las redes de acceso, redes PON, redes CATV o redes de par de cobre, solo constituyen el acceso de los usuarios a internet para contratar todo tipo de servicios.

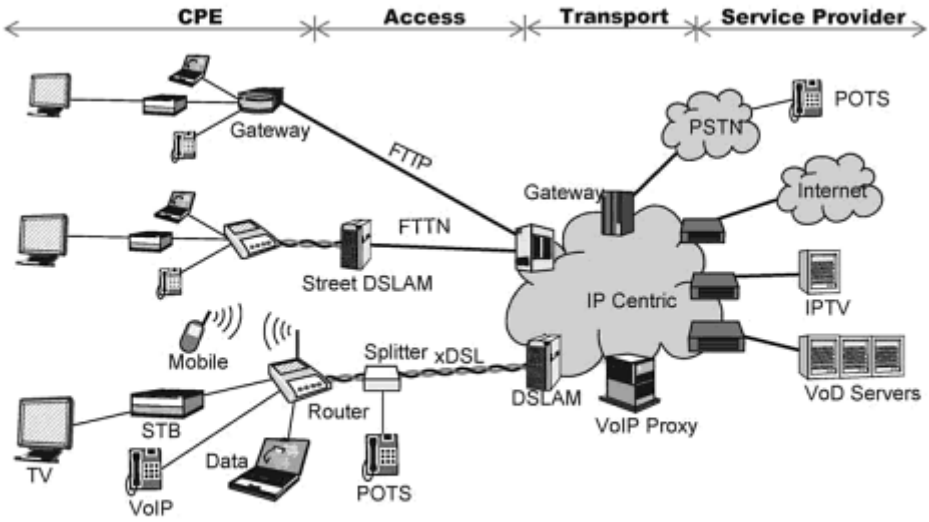


Figure 1-4. Multiple services mean one network, various terminals and many types of access.

Como se comentó inicialmente, en un principio cada tecnología tenía sus propios servicios y arquitecturas de red completas. Hoy en día, las arquitecturas de red solo permiten el acceso de los usuarios con diferentes tecnologías a internet y todos los servicios se encuentran allí. Por lo

tanto, a nivel de servicios no hay diferencias, a menos que la red de acceso no sea capaz de garantizar una conexión de banda. ¿Por qué planteamos este escenario? Porque, por ejemplo, en xDSL las velocidades están sumamente asociadas a la integridad y distancia del bucle de abonado. Esto hace posible que, en ciertas regiones de Europa, se plantee la utilización de tecnología del tipo VDSL2 porque la mayoría de los usuarios se encuentran muy próximos a las diferentes centrales telefónicas. La necesidad de conexiones de banda ancha está asociada a que los servicios requieren altas velocidades de transferencia de información para poder experimentar un buen servicio.

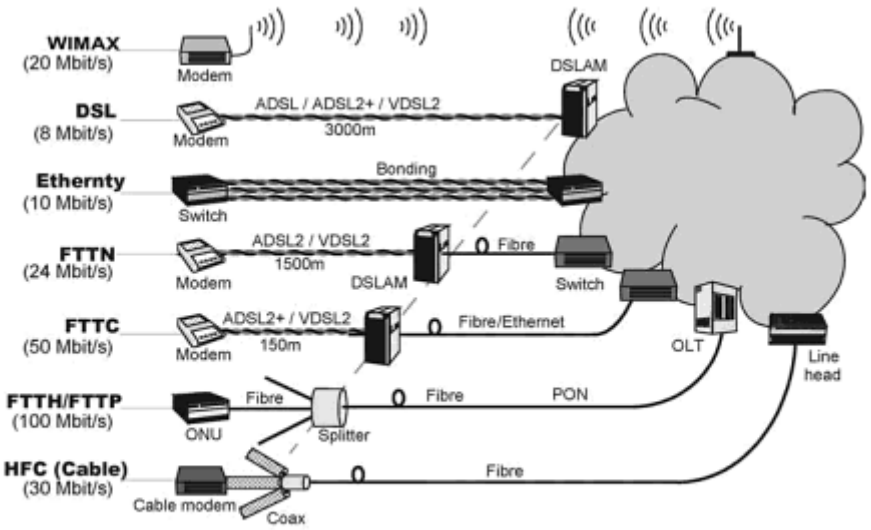
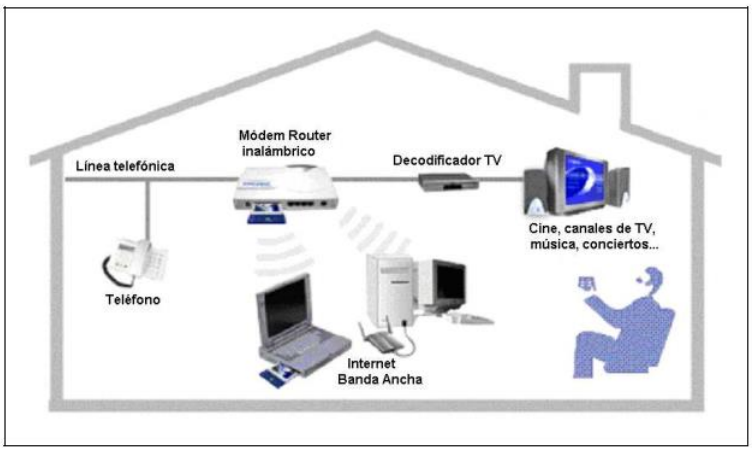
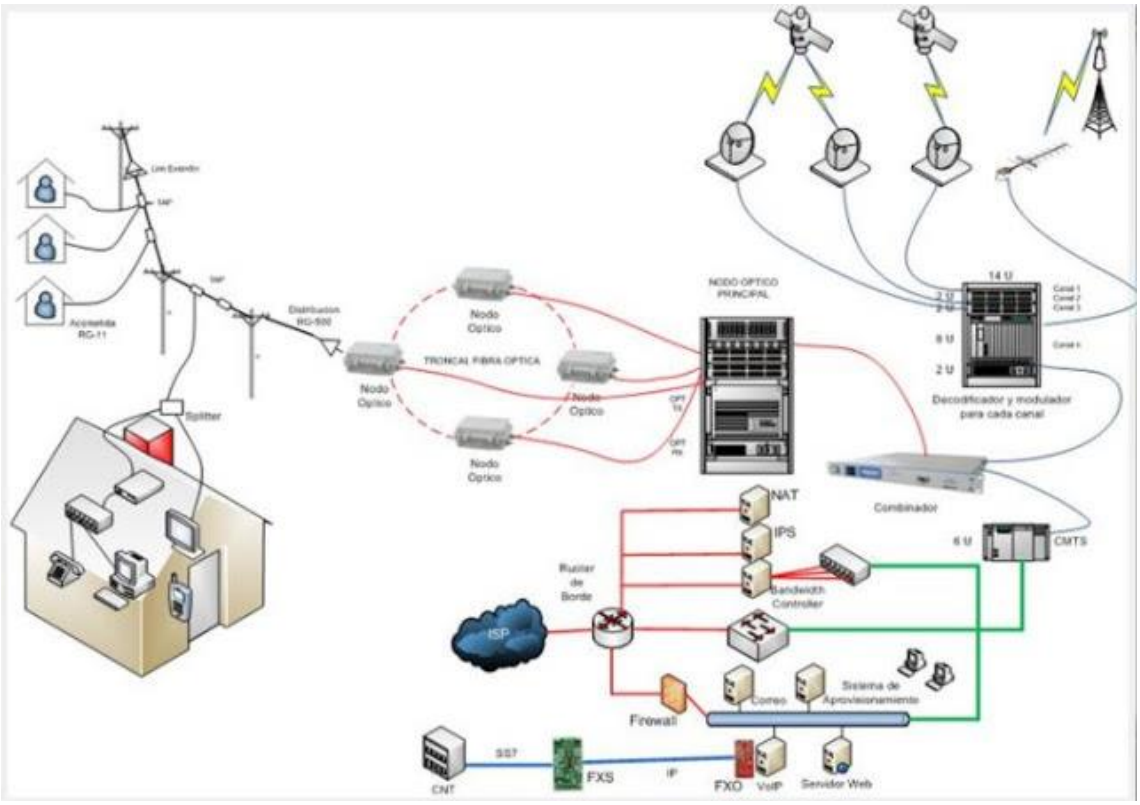


Figure 1-19. Broadband access technologies. Triple Play supports bandwidth hungry applications that require bandwidth of many Mbit/s.

La puesta en marcha de IPTV como una nueva plataforma de servicio de televisión por internet surge de la necesidad de los operadores de telecomunicación, en particular de los de telefonía tradicional, de hacer frente a la convergencia de servicios (TV, Datos, Voz) en redes de internet bajo el nombre de"*triple play*" implementado por las cableras (redes de CATV ó redes de cable coaxil). En esta situación, las redes de par de cobre buscaron alternativas para incorporar junto al servicio de voz, la transmisión y recepción de datos de internet. Con xDSL este objetivo se logró, por lo tanto, fue posible el desarrollo de una infraestructura de red basada en IP. Las empresas de telefonía empezaron a migrar todos sus servicios existentes (telefonía tradicional) e incorporar otros nuevos (Televisión por IP) en internet (red IP), para presentar servicios similares a los de las redes de cable. **Cuestión de pura competencia.**

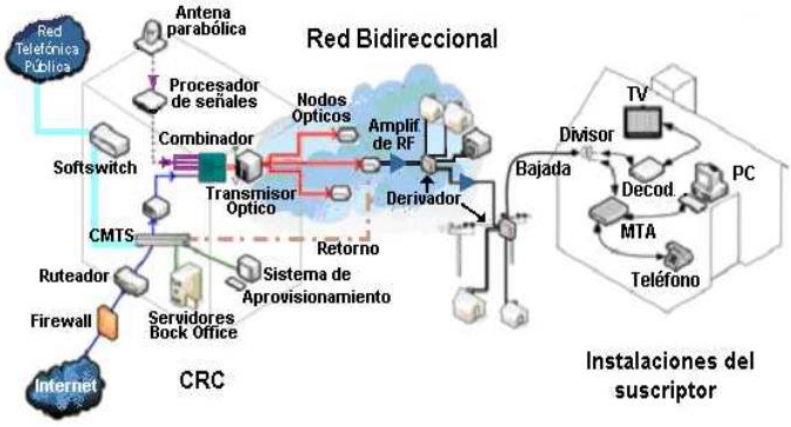


Sin embargo, como mencionamos antes, la implementación de IPTV en redes de par de cobre es diferente en cada país, ya que las velocidades de conexión alcanzadas dependen de la integridad del par de cobre y de la longitud del bucle de abonado. En este sentido, las redes de cable coaxil o redes CATV están mejor posicionadas, ya que son capaces de proporcionar una conexión de banda ancha que permita brindar servicios de televisión, telefonía, internet, de música digital y otros servicios digitales avanzados como video bajo demanda y televisión digital de alta definición.



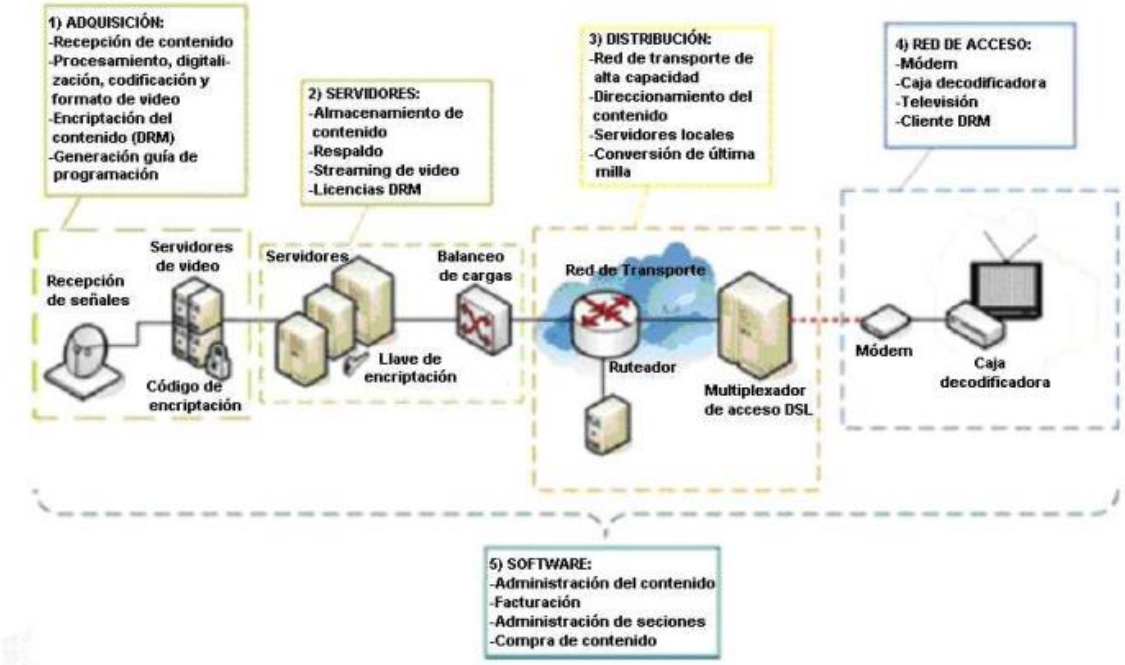
https://repositorio.espe.edu.ec/bitstream/21000/5589/1/AC-TELECOMUNICACIONES-ESPE-033679.pdf

El apunte de clases presenta una imagen muy similar, mencionando cada una de las partes que intervienen.



A nivel general, para lograr la implementación del servicio de televisión en cualquier red basada en IP debe considerarse los siguientes componentes:

- ➔ Adquisición de señales de video
- ➔ Almacenamiento y servidores de video
- ➔ Distribución del contenido
- ➔ Equipo de acceso y de suscriptor
- ➔ Software



Como se observa en la figura, se requiere en primer lugar una etapa en la que se recopila el contenido para integrar la oferta de programas, luego servidores para almacenamiento de video, la distribución de las señales a través de la red de transporte de alta capacidad y, por último, la red de acceso para entregar el contenido al suscriptor.

Las etapas de adquisición y servidores se localizan en la cabecera del sistema, la cual a su vez está compuesta por distintos módulos para realizar diversas funciones. El contenido se puede recibir a través de Internet, de algún proveedor de contenidos o de un distribuidor de señales de televisión digitales y/o analógicas. Independientemente de la fuente, todo el contenido debe ser digitalizar y compatible con el protocolo IP. Por lo tanto, es una función crucial la digitalización del contenido.

Para digitalizar, codificar y comprimir el video analógico, o procesar y convertir el video digital al formato empleado por el codec de video del sistema, se requieren codificadores que además permiten que el flujo de video pueda ser transportado por IP y recibido por la caja decodificadora del suscriptor. El codificador, comúnmente denominado códec (codificador/decodificador) es un dispositivo o módulo de software que habilita la compresión de video digital, típicamente sin pérdidas. La elección del codec de video es de suma importancia porque determina el complejo balance entre la calidad del video, la cantidad de datos necesaria para representarla (tasa de bits), la complejidad de los algoritmos de codificación y decodificación, la robustez ante las pérdidas de datos y los errores, la facilidad de edición, el acceso aleatorio, el tipo de algoritmo de compresión, el retraso por transmisión y otro número de factores.

Los servidores realizan diversas funciones, entre ellas el almacenamiento y respaldo de contenido, la administración del video bajo demanda, del video 'streaming' de alta velocidad y

licencias DRM (Digital Rights Management). Éste último es un servidor de licencias que administra los permisos para desbloquear contenido, autoriza y reporta transacciones y remite el video a los usuarios autorizados. El servidor DRM codifica el contenido y lo encapsula en un contenedor para evitar su uso no autorizado. También proporciona información de facturación para pagos por derecho de autor. Los sistemas 'streaming' requieren más esfuerzo del servidor y también requieren mayor ancho de banda de la red.

¿Qué es el streaming? consiste en un conjunto de estrategias y tecnologías que permiten reproducir una secuencia de vídeo o sonido mientras se descarga con una conexión de Internet. Existen dos formas de realizar streaming: en directo o bajo demanda. En el caso de streaming en directo, la codificación del video y del audio se realiza en tiempo real, los contenidos se retransmiten instantáneamente hacia la red, y son reproducidos en tiempo real por el usuario. Evidentemente, los mecanismos y protocolos utilizados para este tipo de servicio no pueden utilizar protocolos de capa de transporte como TCP. El protocolo más utilizado para realizar transmisiones de video y audio en tiempo real es RTP (*Real time protocol*) que funciona acompañado del protocolo de transporte UDP. Para el caso de streaming bajo demanda, los contenidos son almacenados en un servidor una vez grabados, y se visualizan por el usuario en cualquier instante deseado. Cuando la transmisión de audio y video no se realiza en tiempo real y el cliente es quien controla la recepción de los datos, si se puede utilizar el protocolo de transporte TCP.

¿Qué se necesita para proporcionar servicio de streaming? El núcleo es el servidor de contenido (Audio y Video). Este dispositivo de red se encarga de resolver las solicitudes de los clientes, suministrando el flujo de información solicitado y controlando su transferencia para que la recepción del contenido sea correcta. Para generar la comunicación pueden utilizarse varios protocolos, pero el más empleado es RTSP (Protocolo de transmisión en tiempo real ó *Real Time Streaming Protocol*), el cual se encarga de establecer y controlar uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un mando a distancia mediante la red para servidores multimedia.

Los contenidos han de ser protegidos por mecanismos de cifrado para evitar su reproducción en caso de captura del flujo de datos. Pero ello supone conocer la clave de cifrado para recuperar el contenido original. Al mismo tiempo, se ha de garantizar que la clave sea conocida únicamente por el proceso encargado de descifrar el contenido y no por el propio usuario. Se deben usar algoritmos de última generación para el cifrado, cuidando aquellos puntos que afecten a la carga del proceso de cifrado y descifrado.

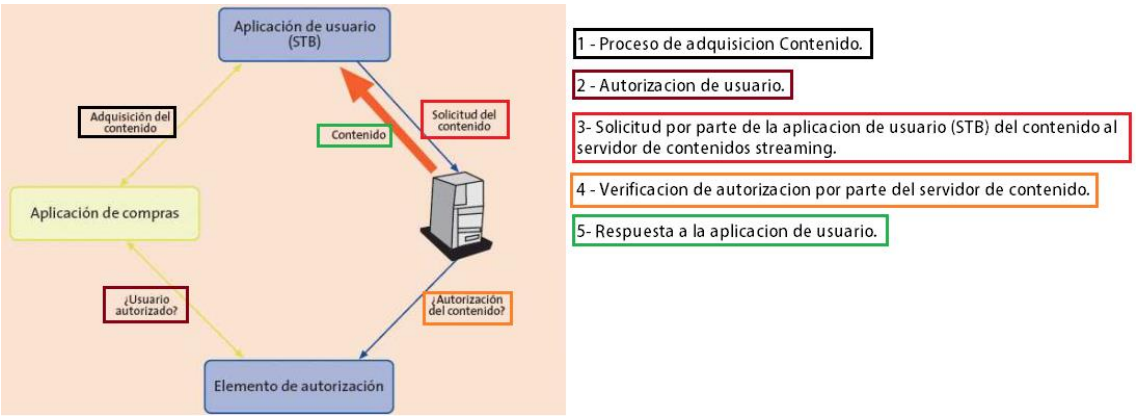
El cifrado del contenido puede realizarse en tiempo real en el momento en que el contenido es transmitido, o bien almacenando el contenido previamente cifrado en el servidor de video. En ambos casos, y como ya se ha apuntado anteriormente, un aspecto fundamental es la forma en la que se hace llegar la clave al proceso del usuario encargado de descifrar el contenido. **La gestión de las claves de cifrado la efectúa otra aplicación.**

Esta aplicación proporciona la clave empleada en el cifrado en el momento de solicitar el contenido. Para la transmisión de la clave de cifrado ha de emplearse a su vez un canal seguro, como por ejemplo una comunicación cifrada. Para cifrar esta comunicación se pueden emplear mecanismos de clave asimétrica, ya que la información transferida en la gestión es pequeña en comparación con el volumen del contenido a transmitir. ¿Se entiende? La idea es la siguiente:

1- Se genera el contenido.

2- Se encripta el contenido y se almacena cifrado o directamente cuando es solicitado se cifra para transmitirlo. **Se necesita generar una clave por parte del servidor. Simétrica o Asimétrica.**
3- Se necesita hacer llegar dicha clave al usuario para que pueda desencriptar el contenido. ¿Cómo hacemos para mandar la clave de forma segura? Utilizamos un canal seguro.
4- Utilizar un canal seguro significa generar un nuevo par de claves para cada usuario registrado y utilizando dichas claves, se manda la primera clave de encriptado del contenido como mensaje cifrado por las generadas para cada usuario. **Quilombo, pero en definitiva una clave cifra a la otra.**

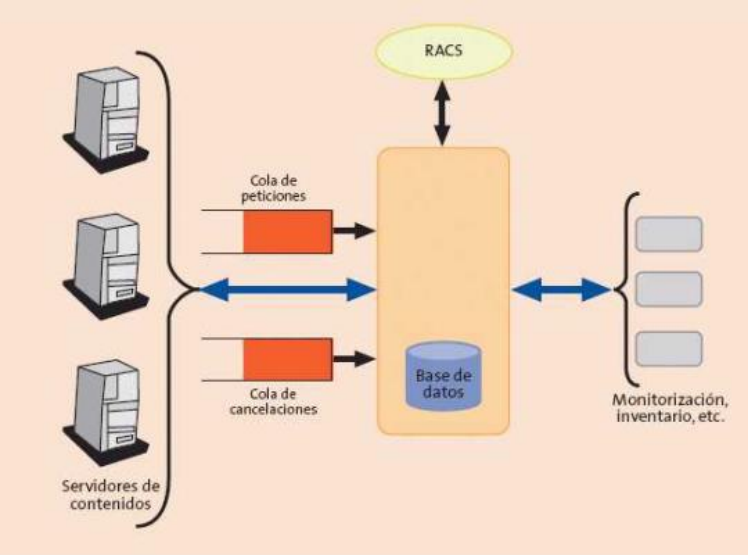
Antes de visualizar un contenido, la petición ha de ser autorizada, y para ello el contenido ha debido ser adquirido previamente a través del sistema de compras, de forma que la compra del contenido quede registrada y pueda ser facturada. La aplicación cliente envía la petición de compra hacia el sistema de compras, y a partir de ese punto se desencadena el proceso de autorización y la adquisición del contenido queda registrada. Al mismo tiempo, la aplicación del cliente le pide al servidor el contenido. En ese instante el servidor comprueba que la petición puede ser servida preguntando al elemento de autorización. En caso de respuesta afirmativa, el servidor proporcionará el flujo solicitado al cliente.



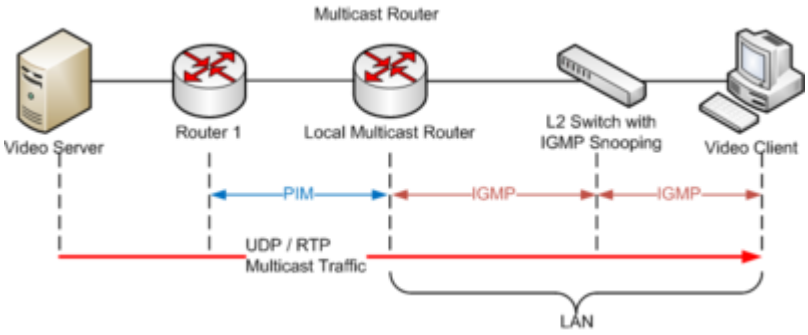
El elemento de autorización no solo basa sus decisiones a partir de la aplicación de compras. Es decir, que no solo controla qué usuario accede al contenido y si éste tiene permiso para visualizarlo. Al mismo tiempo, también toma en cuenta otros factores para autorizar un servicio, como por ejemplo la existencia de recursos suficientes (ancho de banda) para ofrecer un nuevo contenido.

Las peticiones recibidas en el sistema de autorización pueden ser de uno de los siguientes tipos:

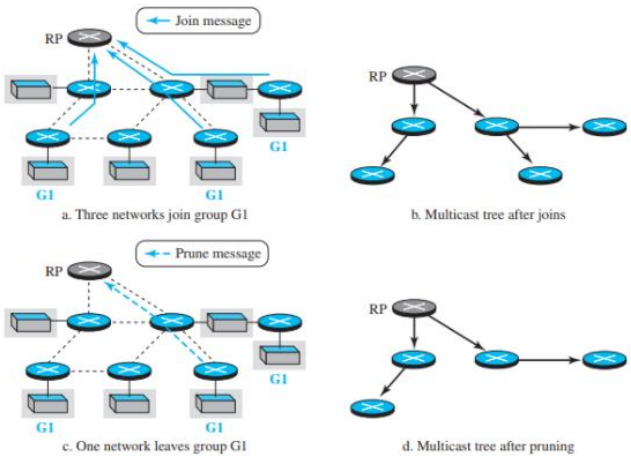
- **Reserva de ancho de banda.** El servidor de contenidos solicita reservar ancho de banda para atender una petición de un contenido. A partir de esa petición el sistema de autorización ha de consultar si hay recursos (ancho de banda disponible) para atender esa petición, y en caso afirmativo, se reserva el ancho de banda correspondiente y se contabiliza como ocupado.
- **Liberación de ancho de banda.** Cuando el servidor cierra una sesión, informa de la liberación al sistema de autorización. De esta forma, al ancho de banda que ocupaba esta sesión se libera y ya no contabiliza en sucesivas peticiones de servicios.



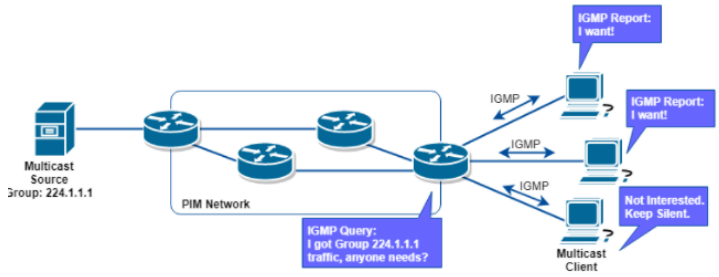
Respecto a la aplicación que maneja el usuario, es necesario mencionar que debe poseer una interfaz amigable y sencilla para que se realice la compra de contenido y su posterior solicitud. Además, dejando a un lado el servicio de streaming bajo demanda o en tiempo real, el servicio de TV tradicional en este tipo de topología de red, se transmite utilizando Multicast. ¿Cómo funciona esto? Los canales de televisión son asignados a direcciones de red Multicast específicas. Para recibir el contenido es necesario que el Set Top Box conozca la dirección IP del grupo en particular y se suscriba. Desde el punto de vista de la red, los diferentes dispositivos deben soportar los protocolos IGMP y PIM.



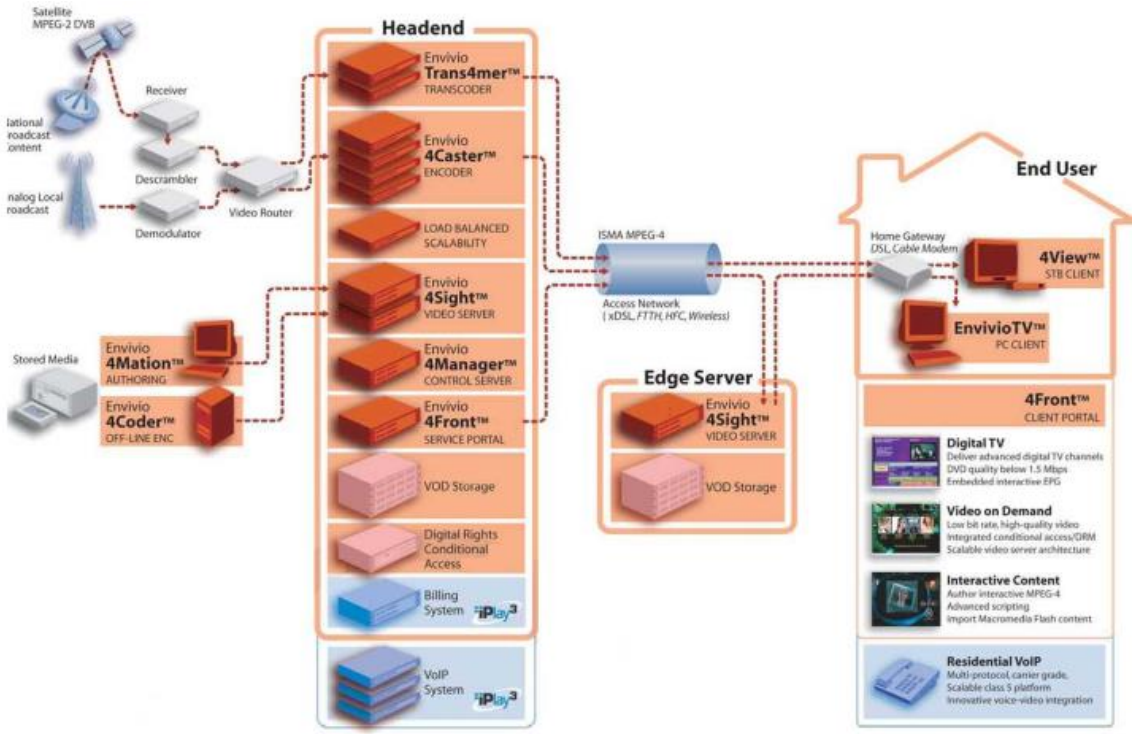
Protocol Independent Multicast (PIM) es un Protocolo de encaminamiento que crea una estructura de árbol de distribución entre los clientes Multicast formando dominios.



El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.



Conclusión, la recepción, generación y manipulación de los datos digitales en cabecera se representa de la siguiente manera:



En esta imagen es interesante ver que Access Network hace referencia a todas las tecnologías de acceso (xDSL, HFC, FTTH) que permiten la transmisión y recepción de información digital y se las presenta como un medio necesario para alcanzar un fin (proporcionar servicios en internet). De esto se trata la convergencia tecnológica.